Transcript: Privacy and Security Initiatives of the U.S. Department of Education

2012 EDUCAUSE Annual Conference

Wednesday, November 7, 2012, 10:30-11:20 a.m.

Denver, Colorado

Presenters: Kathleen Styles, Chief Privacy Officer, and Richard Gordon, Chief Innovation Officer Federal Student Aid, U.S. Department of Education

Moderator: Michael G. Carr, Chief Information Security Officer, University of Kentucky

Note: For a PDF of the presentation slides, including graphics, see the online resources.

Moderator: So, it is my pleasure, Mike Carr, University of Kentucky, to introduce our speakers today. Mr. Richard Gordon is to my right. He's the gentleman with the silver shirt, chief [innovation] officer of Federal Student Aid for the U.S. Department of Education. He's also held numerous IT positions in the Federal Government as well as the Army. I'm sure he could kill us if he wanted to. Kathleen Styles is the Department of Education's chief privacy officer. She's also an attorney and a member of the IAPP [Information Access and Privacy Protection]. She's a certified information privacy professional.

Remember to fill out your evaluations. I do have some that are completed down here already if you want to just take mine. Thank you.

Kathleen Styles: Good morning, everyone. Richard and I do have a fair amount of content, but we both promised we're going to race through our presentations because the part of this that is of great value to us is the interaction with you. We really do want to have some conversation, some questions at the end. We are going to make sure we reserve at least 15 minutes for that.

First, just an outline of what we're going to talk about. I'll talk very briefly about privacy. I will talk a little bit about FERPA — the Family Educational Rights and Privacy Act — and I'll talk about what I'm calling "hot topics in privacy." Richard will discuss data breach, information security, and some FSA initiatives. Then, as promised, we'll leave a lot of room for questions and answers.

So, first, what is privacy? When people talk about privacy, they mean many different things. In the civil liberties context, privacy has one meaning. I talk primarily about information privacy.

When the Supreme Court talks about privacy, they're referring to intimate relationships, to homosexuality, abortion, birth control, those types of things. For the focus of today's discussion, I'm very sorry, we're going to talk about *information* privacy.

Fine. What is security? This is the difference between what Richard does and what I do. Richard does information security, which is keeping the data that we have confidential. Sometimes people talk about privacy versus security. I can say that neither Richard nor I believe that that is the paradigm. We think that it's important that privacy and security work together.

I just thought I'd give you a little bit of an idea of how privacy is structured organizationally at Ed. This is a really poor org chart here [referring to slide 4 on the screen]. We're going to work on that before we do this again, but I wanted to give you an idea that there's a variety of topics that are included in there.

I have a direct report to me of a statistical privacy advisor. We're finding more and more that privacy is encompassing how to publish data, how to anonymize data. One of the first things I did when I got to Ed was to hire a statistician to help me with those issues.

I also do records, records management, information-collection clearance. If you work for the Federal Government, you'll know you have to get approval any time you do an information

collection. We do privacy safeguards, which is privacy compliance within Ed itself. We do the Freedom of Information Act, everyone's favorite.

Under me also is the Family Policy Compliance Office, which is called FPCO. This is the office that administers FERPA as well as the Protection of People's Rights Amendment.

Just a quick background on student privacy. FERPA was passed in 1974. It was part of a blaze of privacy statutes that were passed in the 1970s, sort of along with the advent of computers and government databases.

Since that has happened, we've had a whole lot of change in the way education is done in this country. From records being mostly paper-based and in filing cabinets, now we have online information systems. We have digital information. We have a statute that has been amended, but not amended in a fundamental way in many, many decades.

We now have, at the K12 level, state longitudinal databases and an increasing pressure for accountability and the publishing of data for accountability purposes. This started in the K12 arena, but I'm seeing more and more of it in the postsecondary world as well.

In 2009, Fordham University published their Center for Law and Information Policy analysis [*Children's Educational Rights and Privacy*], a review of privacy protections and state longitudinal databases, and was highly critical of the work that the states have done in that arena as well as the federal government, the Department of Education.

I'm the Department of Education's first executive-level privacy officer. I've been there a year and a half. I actually think they actually established the position in response to the Fordham University report.

The basic picture that I want to get across is that we have a whole lot of new risks and vulnerabilities surrounding privacy and student records.

This is my favorite FERPA quote [referring to slide 6: "You know how sometimes FERPA can tie your brain in a knot trying to think through it all?"]. One of the technical assistance areas that we run is PTAC — the Privacy Technical Assistance Center. We receive many e-mails asking us questions about FERPA compliance and privacy — for data sharing in particular. I just want to say to the author of this message — who, of course, I've anonymized — I feel your pain. FERPA is a very complicated statute, as well as an outdated statute.

I'm just curious: I know I can only interact now with the individuals in this room. How many of you all have worked with FERPA? How many of you all know what it is? [People raise their hands.] OK, wonderful, glad to hear that.

I was going to give a short little background on FERPA. I'm going to make it even shorter, because you all have worked with this before. FERPA 101 is a class in and of itself. In general, what FERPA does is give parents and for most of you all — since you're in postsecondary — eligible students (students who are attending postsecondary institutions) the right to access and seek to amend their education records.

That doesn't mean they get to change their grades if they don't like their grades. It means they get to correct obvious errors. It protects the PII [personally identifiable information] in the education records from unauthorized disclosure.

And [it has] a requirement for consent. "Consent" in the FERPA universe means written and dated consent unless an exception applies. There are, of course, a number of exceptions.

The first exception I want to go over is *directory information*. This is information that many — and, certainly, the authors of the FERPA statute — think is going to be noncontroversial. It includes, however, a number of things that we already recognize clearly as PII and clearly as offering the ability to locate and re-identify students — name, address, telephone number, photograph.

Directory information by regulation cannot include social security number. Students are allowed to opt out of directory information. But if they do not, you are allowed to share their directory information without their consent, but you have to put out an annual notice about the categories of directory information that you're sharing.

Studies. You are allowed to share information about your students without consent in order to conduct studies. That's a fairly limited exception. I'll talk about that in a little bit more detail, as I will about audit and evaluations.

Health and safety emergencies. This was a topic that we discussed a great deal after the tragedies at Virginia Tech. We have tried to be clear. We have tried to issue guidance to say that we're not going to be second-guessing you. If you think you have an emergency on campus, and you need to be releasing information to protect your students on your campus, we are not going to be second-guessing you if you do that.

There are other exceptions in the statute as well. This is very interesting because in the slide, itself [referring to slide 9] there's supposed to be a great big giant circle with the "X" through it to let you know that there is no research exception for FERPA. Somehow, in the putting that together... yeah, beautiful and red.

[laughter]

There are other statutes that have general research exceptions. FERPA's are a little bit more narrow.

We recently amended our regulations for FERPA. Those regulation changes were effective in February and January of this year. They have been challenged in court by EPIC, by the Electronic Privacy Information Center.

We've been going through discovery and records exchange. We have a briefing schedule now that should get us a ruling sometime next spring. We're waiting eagerly to hear the response to that.

The regulation amendments went through a number of topics, but a lot of the changes were intended to facilitate and improve accountability involving data sharing. There's a lot of research about program effectiveness and accountability. We wanted the regulations to be clear about what was and was not permissible under FERPA.

The studies exception. You can share data without consent for or on behalf of schools, school districts, or postsecondary institutions. The exception is not as broad as it sounds on first reading because their studies have to be for one of the purposes here: developing, validating or administering predictive tests, administering student aid programs, or improving instruction.

The exception that is actually the broader one is the audit and evaluation exception. This says that data can be used to audit or evaluate a federal or state-supported education program, or to enforce or comply with legal requirements that relate to that education program. The audit and evaluation exception is the one that is most commonly used to establish state longitudinal databases, by the way.

I just wanted to share with you a couple of key lessons that we've learned since January and answering questions about the new regulations. We get a lot of questions via email, via telephone. We have several centers that you can call. I'll talk to you about those a little bit.

Both of those relate to the audit and evaluation exception. This is my feeble attempt at humor at the bottom [referring to slide 13]: "We're from the government. We're here to help you." We really do like to answer questions about FERPA and to give you advice on the front end as you're thinking about the transactions you want to engage in.

The first is the definition of an education program. You can share information without consent to audit or evaluate an education program. An education program is defined very broadly. It

includes adult education. It includes preschool. It includes vocational education. But it does not include programs that are not educational in nature, like child welfare programs.

The other major limitation that we're finding as we're answering questions is that the proposed use of the shared data is actually for program purposes rather than to evaluate the program itself. The example I want to give you in that context involves community colleges.

There are a lot of community colleges in this country who are doing something, which is a great idea, which is they're trying to follow students who took classes at the community college but did not obtain a degree or certificate there so that they can see whether they've attended other college or educational institutions afterward and obtained credits that would allow them to get a certificate from the initial institution.

There is a substantial number of students, we're finding out, who have subsequently taken classes then to a degree, and they don't know it. That degree could help them. That's actually not something you can do under the audit and evaluation exception because you're not evaluating the program. You're helping the students.

As a policy matter, if you were writing the statute again, would you write a statute in such a way that it doesn't allow you to share information like this to help children, students — only to evaluate them? I don't know, but that is what our statute says.

If you want to be doing this — some of the community colleges are calling it "reverse transfer" — there are other ways you can potentially do it. Just contact us. We'll talk you through it. It involves the directory information exception.

Coming here today is a great experience for me because it lets me hear and understand the great depth and breadth of innovation and initiative in the postsecondary universe right now. The keynote address this morning was fascinating for me. I loved that. I thought that was really fun.

What we're hearing more and more about and getting more and more questions about are new and novel things that people are doing in the IT sphere, particularly in postsecondary. They're coming to us, and they want to know, "Does this comply with FERPA? Does this comply with privacy?"

I wanted to walk you through the Fair Information Practice Principles so that we could talk a little bit about what's beyond FERPA. In a lot of these, my answer back to you or my staff's answer back to you is going to be, "This doesn't really implicate FERPA." Lots of times people will say it does. Sometimes it does. Sometimes it doesn't.

More often, what you need to be doing when you evaluate your new programs, your proposals, is to think in terms of your fair information practices. These have been around since the 1970s. They are the basis of all major federal privacy legislation, and they still have great meaning today.

I've listed them here. I don't want to go read all five of them here, but think about, for example, the third one — a way to prevent information obtained for one purpose from being used for another purpose without consent; a way to correct records about you.

If you're sharing information, particularly for program purposes, the way to correct a record about you is very important. If you are evaluating new proposals, I want to encourage you to look at the Fair Information Practice Principles.

Data sharing. We answer a lot of questions about data sharing. I just wanted to offer some general thoughts on the process. There's nothing new here. There's many presentations on the agenda today, I noticed, about data sharing, some of them specifically about some of these topics.

First is to develop a data governance process. You shouldn't have to do this again every time you get a data-sharing request. You should have a process in place that allows you to evaluate the incoming requests.

Next is minimization. You share only the information that you need to share to achieve the purpose of what you're trying to do. Use written agreements. That's actually a requirement in our statutes and regulations. Pay attention to disclosure avoidance when publishing results. This is becoming increasingly important. It is very easy to publish tables that have small cell sizes in them and to identify individuals by doing that.

Finally, to be transparent. If you're sharing data and you have results, publish them. We recently completed a review at the K12 level for all of the state education associations on how transparent they're being on their websites about what they're doing with student information. We offered them specific suggestions.

I'd like you guys to think about that as well at your institutions. How much can you tell from looking at your website about what you're doing with student information?

Hot topics. I could have written a whole page on this. I just put a few of the hot ones up here [referring to slide 16]. You all are innovating a whole lot faster than we're responding at this point, so if you have other proposals, I'd love to talk about them. The ones I listed here: analytics, big data, smart disclosure, researcher access, and publishing data. I should have listed MOOCs [massive open online courses], since I've only recently learned what they are.

Analytics and big data. The general rule on this — and the things you need to think about — are (a) whether you've got FERPA compliance, and (b) your fair information practices. There's so much that can be done with analytics with this sort of information, whether it is identifying students who haven't accessed your online learning system recently and who may need a little nudge to get back on track, to identifying which parts of your course curriculum are causing students more difficulty.

When you are thinking about your analytics and your big data proposals there, this is where I say, "Think about whose data this is." If you're doing this and you're thinking about FERPA, most commonly you're going to want to think about the school-official exception.

The school-official exception lets individuals in your school, including volunteers and contractors, see information if they have a legitimate and educational need to see that information. That is most commonly what people are going to be looking at as they consider different types of analytics.

Often, when individuals come to us with questions and they want to use information for analytics, they say, "But wait a minute. It's anonymized." Are you sure about that? Re-identification risk is a very real risk. You can't just take off somebody's name and say that the record is anonymized. With the amount of information that's available online, it's increasingly easy to re-identify individuals.

Again, my final point there is, don't just think about FERPA compliance. FERPA is the floor. The ceiling is something very different. Achieving compliance with FERPA is not the end of the story.

Smart disclosure. These are also called "my data" buttons. FSA is looking into those also at this point. These are things that allow students, individuals to download their own data so that they can easily re-upload it into mobile apps. The privacy issue with that is sometimes it's not only just your data. Sometimes you're entering information about other people as well. Also, sometimes teenagers and adults do not always make smart decisions about their own information.

Researcher access. The National Center for Education Statistics has been licensing confidential data for several decades. We're working to expand this now to include Ed program data. We're putting in additional data sets. The civil rights data collection and the school-level accountability data, if they're not already available, should be available very soon.

I don't know how many of your all's institutions are interested or are now engaging in sharing student information with outside researchers. If you're doing so...the document that I cited up

here [referring to slide 20] actually was developed for K12 by the National Forum for Education Statistics. It's not an official Ed publication, but it's got some very good information about best practices for establishing a program to share with external researchers.

Publishing data. We've mentioned this before. One of my first acts was to hire someone with a background in statistics. We are in the process of trying to publish school-level accountability data right now or school-level assessment data at Ed. The states have been doing this for a while. As we're doing it ourselves, I have to tell you it is a humbling experience. It's very complicated to do the kind of suppression and blurring that you need to do in order to protect student identities in small cell sizes.

I wanted to close by just offering you the site, www.ptac.ed.gov. There is a whole lot of resources up there. My contact information [Kathleen.styles@ed.gov] is at the end of this. But really, the best place for you to start if you have a question about data sharing or analytics or a novel idea is going to be PTAC. I say that because I get 200 or more e-mails a day, and I don't log them in, and I don't track them. You are going to get a response quicker if you send your questions to PTAC.

They're also available. They make site visits. We put up guidance documents on their website. We have done case studies. We have released our first FERPA 101 video for the FERPA junkies among you. That one is geared toward the K12 universe, but we have a FERPA 101 for postsecondary that we hope to have up in about a month. [Editor's note: both videos are now available at http://ptac.ed.gov]

With that, when we close, one of the things I always ask at these conferences is, [given] the guidance that we've put up, are there additional topics that we are missing? I've got a long list. We have a year's worth of priorities, but if we're missing something, we want to hear it. With that, let me turn it over to Richard.

Richard Gordon: Thank you, Kathleen. Every time I have to do these, I have to ask myself the question, why me? Why did Rodney [Petersen] and Valerie [Vogel] call me and say, "Guess what you're doing in a couple of weeks"? I'm a nervous wreck every time I present, so bear with me.

I'm an operations guy at Federal Student Aid. As many of you know, Federal Student Aid is not a big staff of folks. We have about 1,200 staff. We have about 10,000 contractors.

We do the movement and protection of a lot of big data. One of our systems alone, FAFSA [Free Application for Federal Student Aid], has over 1.2 billion page views per year. It has 113 million unique users. We operate with partners in 35 countries around the world, and we have students in over 225 countries around the world. That's just one system.

We have a need to protect data. We have a need to make sure that the facilities are there, they're doing the things that they need to do, and they're compliant with the laws and regulations.

My start point is, what is a breach? It is the unauthorized extraction of data or the manipulation of data. It's either coming from the outside or coming from the inside. Whatever it is, we have to make sure that it doesn't happen.

When you have systems that are processing so much data, it's very easy to say that a breach is something that includes millions of records. No, no. We have to be responsible for every single record, for every single student, for all 70 million accounts that are on our system. We have to be accountable for all 90,000 folks that have privileged access — the ability to see data, more than just their own, data for every student that's going to that institution.

What does this thing really look like? You're going to have a lot of presentations on what these breaches look like, but I just wanted to point out a few things. According to one report, 98 percent of the breaches come from external entities.

What really got me is that 96 percent of them are not difficult things. They involve servers, so your centralized data access. They weren't discovered by you 92 percent of the time. They were discovered by somebody else. A lot of them were very, very easy things that occurred.

So when you have this problem, this is not something where we have to figure out the world. We don't have to articulate or define "love." We just have to do the basics. We have to make sure that we have processes in place that are protecting the assets that we have. We have to make sure that we sequester data that is highly sensitive. We have to make sure that every single person that's associated with the systems has the right skills and is doing the right thing each and every day.

I was talking yesterday to a couple of folks about a phone call that I got from our data center provider recently. Whenever I get a phone call on the weekends — especially on a Saturday morning — from my data center provider, it's never good. This call came from Hal. Hal said, "Richard."

I said, "Hal, how are you?"

"I got this problem."

"Well, what's the problem, Hal?"

"A patch got loose."

"What do you mean a patch got loose, Hal?"

"Well, one of the patches that wasn't supposed to go in for another week or so just cut loose and started to patch 130 servers."

"Well, Hal, can you shut this down?"

"No, I cannot." All of [a] sudden, my entire Wintel footprint just went south.

We had another situation where we had a piece of application code that went into production. We had a vendor who has been with us for quite a long time, that's done a lot of great stuff, but they missed one statement in the code, one little bitty statement. All of the sudden, a lot of people were able to access stuff that they weren't supposed to be able to access.

Again, it's not the Huns coming over the wall. It's not that we have to feed in the alligators in the moat. It's to make sure that every single process that you've already defined is actually executing the way you think it's supposed to.

It's when you're dealing with these partners and you outsource to the latest cloud, or you've got a bunch of folks that just show up, that you actually go down and say, "Are you patching the servers? Are you monitoring the performance? Are you doing the things that are necessary?" In a meeting that I was in yesterday, I said, "I am so afraid of this basic kind of thing that I fear that we're facing a tsunami."

I'm assuming that everybody in the room has an iOS device. Is that fair? Everybody's got one? I believe that the greatest privacy release that we've ever experienced is going to happen in just a few months. Why? Because Christmas is coming, and everybody is going to update from i4 to i5.

When they do it, they're not going to go in and say, "OK, let's trade this device out. I want you to shred the hard drive." No, no. They're going to walk in and say, "I want my i5. Move my contact list over," and they're going to walk out just as happy as can be. When you think about what we've done leading up to this point, you realize that we've put a lot of data out there.

Let me pause for a second. I get to say "MOOC" one time. I have no idea what it is, but I get it. When you think about needing to protect assets and needing to protect data, it's a big deal. When you realize there are so many of the assets that we really don't control, you realize that we have to change the strategy that we use to protect these.

We have to get people like my 13-year-old son to realize that that phone that he has is a real big deal. Just losing it or loaning it out is troublesome. We have to realize that we have to write

policies that are not generic and not broad, but that speak to the heart of each and every person that's got access to our data and their data.

One of the big debates we have in the department is, whose data is it? Your customers, your students, log into our system. What do they give us? All of their tax information. They give all of the tax information for mom and dad at the same time, every time they fill out the FAFSA. We transmit that data down to you all. For some of your institutions, that may be 20, 30, 50 thousand records, and you do it several times a year.

It's on computers that you are responsible for. I venture to guess that if we actually started an audit and started walking through and said, "What's your control policy for those financial aid administrator computers?" you'd probably say, "Well, it's what we do for everything else."

Really? You're telling me that when you upgraded from Windows 95 to Windows 2000 or whatever the case may be, that you actually went in, realized that there are probably hundreds of thousands of IRS records on that hard drive, you pulled that hard drive out, and you drilled it or you degaussed it, or you did whatever?

You're probably, hopefully, going to tell me that your policy with those financial aid administrators is to say that, we really don't care how busy you are. That student labor that's in the room cannot — *cannot* — use your account to log on to any of the systems and act on your behalf, because once you hand that off, it's a done deal.

We struggle with 110, 113 million users that log on to our systems each and every year. What scares us are organizations like LoanLook and all these big data aggregators. Why? Because in order to get into [their] systems as a student, you have to hand off your user ID, your PIN. The problem is, once that's handed off, that organization has access to your data. There's really no way to revoke it other than changing your password.

This is not a hard problem, it's just big. But it is something that I firmly believe that we can start to move through. We can start to change the curve. We can start to get rid of some of the rough edges, but it's going to take each and every one of us taking this seriously.

I tell you, we have your data at Federal Student Aid. If you got a direct loan or a FFEL loan or a Perkins loan, you got a Pell grant, your data is one our systems, as well. You have a vested interest in making sure that your four, five, six, seven years of IRS information is not leaked. You have a vested interest to make sure that all those kids that are working with you that are attending your institutions understand that they have to take this serious. We have to move the dime on this.

We can go through the normal stuff. There are breaches. There are breaches that occur each and every day. There are tens of thousands of records that are leaked out into the community. But many of you may or may not know, what's the cost of a breach?

Only those who have gone through one and have had to start spending money to tune of about $200 per record realize that this is something that you probably want to get ahead of because if the breach occurs, that wasn't one of your budget line items. All of the sudden, someone's research is about to get stripped. Someone's administrative budget is about to get stripped.

You leak 25-, 50- 100-thousand records, and you're starting to buy data protection, you're starting to bring in external legal resources, this is troublesome. But again, there are things that you can do to start to reduce the risk, to start to reduce the potential for those kinds of leaks.

This is really a bad slide [referring to slide 27]. I'm just going to pass through. Malicious attacks are on the rise.

This slide [28], what it's supposed to say, and the point I want to make... This top one where it says "CISO." The next one actually says "external consulting support." What this slide is trying to say is that, if you formalize your processes, if you have a CISO that actually understands what they're doing, what will happen is the basics of making sure that you're doing the right thing will be there.

You're going to have the policies. You're going to have the procedures. You're going to have the audit. If it is something that is an "oh, by the way" job, then it's probably not going to get done because patching is boring. Securing those routers is boring. Monitoring is boring. But if you don't have someone doing it, then your potential risk is going up exponentially. When the lawyers show up, they're going to say, "How did we get here?"

"Well, I know we still have Windows 2000 servers, but we just couldn't get there from here." OK, well, get out your checkbook because there's really nothing more you can say.

This was not something that was insurmountable, something that you couldn't take care of — it was something that you had the responsibility [for]. You've been briefed on it again and again and again. All you had to do was the basics: getting your policies and procedures in place, auditing your processes to make sure the right things were indeed being done. And then, if a breach occurred, no harm, no foul. The risk should have been a lot smaller. The circle of leak should have been a lot smaller.

This slide [referring to slide 29]. is supposed to say that there is a customer impact. I apologize. We'll make sure it's uploaded to the EDUCAUSE website. What it says is, that if you do experience a leak, there is going to be a negative impact on your customer population. On the financial sector, if you're a financial organization and you have a leak, there's a higher potential that you're going to start to leak customers.

The typical activities that occur around a breach. You start doing investigations. You start doing auditing. You start doing outbound contacts. You bring on legal services. You do identity protection and customer retention practices, anything you can do to try to seal this up.

What you also do, the column on the right is, you increase training. You do additional manual processes. You do encryption. You do identity and access management control. You do endpoint security. You do all that stuff when the breach occurs that you probably should have been doing before the breach occurred, so that the potential for this to happen would have been less.

It is said in many venues that the biggest place for a possible breach is in the higher-education community. The reason is because of our kids. It's not because of your core activities. It's that our kids don't necessarily take this serious. I wish I had a great answer for how we're going to solve that problem, but I know it's a problem that we're going to have to solve, because it's getting bigger and bigger and bigger.

Our kids are showing up with high concentrations of data. Many times, that includes the parents' data, the guardian data, and all of the rest.

What are the basics? Configuration control, making sure that your assets are configured and protected in a way that you think is appropriate, making sure that you do appropriate testing.

If an incident happens, have a reaction plan. Make sure that you get up there and seal the leak. That's the first thing you've got to go. That's a team working on that. Get help, because chances are, you're going to go into panic mode, and you're probably not going to be thinking out of the box the way you should.

Document everything. Start creating that root cause analysis document at the moment you know there's a problem. Have a single voice to outside parties. Get to the root cause and execute the fix.

This is something that you need to put in place long before you start to leak records, and it's something that you need to practice.

Our organization has gone through a couple of system failures, which feel like a breach.

If FASFA goes down around February or March, we actually have to start calling all 50 state governors. Then we have to call leaders from other countries.

We practice our incident response a lot. It is not something that you want to just wing it. You want to have a plan. You want to know who you're going to call. You want to know what your responsibilities are, especially if you're operating in multiple states or in multiple countries.

That's it on the scary stuff. Some of the easy stuff that we're doing in federal student aid? I am one of the principal officers that's been assigned to a project called F6, working with the IRS, Social Security, Health and Human Services, and a bunch of other folks.

F6 is an effort by the federal government to create a federal identity exchange. The whole goal is to set up a bridge whereby a third-party AL2- and AL3-level credentials — trusted credentials, many times having two-factor [authentication] — are allowed to come into this bridge and be translated into accounts that we have on our local systems.

You might be able to use that very secure Verizon account that you have to log on to complete your FAFSA or to look up your benefits over at Social Security. It's a big deal. Why? Because all of us at the agencies, not just the Department of Education, have a responsibility to provide view access to data.

The problem is, especially at Federal Student Aid, your identity changes. You enter our system typically at around 16, 17 years old. For many folks, it goes all the way through to the time that they die. All through that, you're identity continues to morph.

So, having just our local Federal Student Aid account is probably not the best use of time. When you back up and look at the aperture, open the aperture on the Title IV ecosystem, those same folks are traversing many of your institutions.

What the F6 project team has been trying to do — and they're moving ahead quite rapidly on it — is to get this bridge up and running in a prototype mode that will allow a couple of organizations to federate to Federal Student Aid, SSA, and others.

We're also working on a case management system. Our program compliance group is working on that. We've been working on it for a couple of years. It's going to go well. We are, hopefully, going to reduce the burden associated with Federal Student Aid coming down to do an audit on your financial aid office. Instead of shipping us boxes of paper, boy, wouldn't it be great to auto-upload some things?

We've got the integrated student experience, where we're trying to reduce the number of entry points into Federal Student Aid, so if you as a student, or you as one of our partners, wants to get into our systems, instead of going through 10 or 15 systems, you go through a single portal and get access to the information that you need.

Then, of course, we've got the bread and butter technologies — Arena, K2, SharePoint, things that everybody's been doing for years. We're trying to catch up. It looks promising. I think it's going to make a huge difference. Hopefully, it will allow us to have more flexible access to our systems for many of you.

That's all I got. Now I can sit down and have a panic attack. [chuckles] Thanks.

Kathleen: Anyone have any questions?

Audience Member: I'll step in. You had mentioned, on the privacy area, about the school experience, if I remember correctly. It was talking about our school exceptions so that when we have contractors who are gaining access to this information as being agents for our institutions. Do you have any suggestions on how we engage these external contractors so that they understand what their responsibilities are, and then how we should make sure we integrate with them? In particular, what I'm thinking of is, we have a lot of online learning going on, and we have a lot of agents out there who want to help us engage the students and recruit the students. Exactly what is our obligation as institutions in sharing that information with these agents of ours?

Kathleen: The first thing I'd say is that the thing to concentrate on is understanding, yourself, what it is...I have to [inaudible]. Oh, that's great — hold it closer [referring to microphone]. Sorry. [laughs] I'd suggest the first thing to think about is understanding, yourself, what it is that you're trying to achieve, first of all, in terms of FERPA compliance, but in terms of privacy and security in general on that.

The answer of how to get your contractors to understand it? I hate to be simplistic, but this is what you ought to be writing into your contracts. The school-official exception is pretty broad. I probably should include that in my standard presentation in a little bit more detail.

Basically, if this is something you all are doing as part of the core business of educating children... Hah, children. *Students*, in this case. Sorry, I speak to a lot of K12. ...it's going to fit within that exception. The question is, who has the need to know which particular pieces of information? The trick is to just think about it beforehand and be clear about what the access rights are and those sorts of things.

Anyone else? We're kind of blinded here, so you may have to wave at us. [laughs]

Audience Member: Hi, Richard. I was really very interested in what FSA is doing right now in terms of identity management. I'm interested, though, in having you kind of vision for us down a little farther timeline on that issue. I think about the example you used of your son and a cell phone, and how we may not really be inculcating the culture of responsibility on our own digital exhaust that is just everywhere. If you were to look — let's say, down a 10-year timeline for us — what might you vision identity management or identity to look like?

Richard: The way I think this is going to go — I'm an engineer, so I have to give you the technical response — is that within the next five years, you are going to be responsible for bringing to the table your own electronic credential. It would not be unrealistic for someone like me to believe that you're going to go down to your local post office and take your passport, your driver's license, and a couple of others to say, "I need an electronic credential, an electronic cert issued to me that I plan to use as I go forward."

You may also have a couple of commercial ones that you get. If you're a researcher, you may have a couple of those. It's clear, at least to me, that there are going to be several bridges that are going to have to be set up.

When you look at the dynamic of the way that data is moving and the synergies that [are] coming together, at the end of the day, we always need to know it's you. That's going to be the tough thing. It's always got to be, and it has to be, you in a way that is nonrefutable.

I see it as being almost scary. I actually see the entry point being around kindergarten. That will probably be the first time that your real identity stands up and we start to figure out who you are.

I got a briefing recently from an organization that talked about these little iOS devices and everybody's having fun with them. That's most likely going to be the scanning tool. It was really cool. This happened, I guess, about a month ago. They came in. They had an iOS device and those look-back cameras. I always wondered, "Why in the world would we do that?"

Well, the security folks that I talked to are using that look-back camera to do facial recognition, to do your iris recognition. It becomes your scanning device. So, it won't be unrealistic to say that if you're trying to get into a secure place, it just says, "Dial this number or stand within this network. Point your phone at yourself." Your face will come up, and then you'll see all that recognition occur, and then they will allow you to pass through.

So, a little nervous, but I don't see any other way for us to get through the next big wave of data integration and the next wave of specific use of data.

Kathleen: Can I chime in on that one?

Richard: She's probably terrified.

Kathleen: No, no, no. But I'm not sure I'm your typical privacy officer, either. I just want to say I agree with what Richard just said, but you have to understand: in the privacy community, that is a very frightening prospect. The idea that everyone has an irrefutable identity and it can be used to track you to a certain place — there are people who think that government in particular should not know that about you. I just want to point that out here. It's an ongoing discussion.

My focus as a privacy officer is on information management, but those whose focus is more on the civil-liberties aspect find that alarming. Next question?

Online Audience Facilitator: There's a question from the online audience. It's regarding F6. How are you going to get applicants to sign up for another government ID versus using their campus ID to access their accounts in government systems? There's a follow-up question, as well.

Richard: One of the things we're doing in addition to working with the F6 project team is working with InCommon to address that very issue. I'm a firm believer that there won't be one or two places that participate in the federal bridge. I think it's going to be a lot of organizations. We get a lot of questions about, "I've got 5,000 freshmen that are supposed to show up on my doorstep. I don't want to privilege 5,000 accounts because only 2,000 may actually appear. Can we use something like a bridge in order that the Federal Student Aid account that they used for FAFSA be the account that they use for semester one?"

We're trying very desperately to set it up so that if you are an Ohio State user or you are a Penn State user and you've got that Penn State account, as long as it's privileged at the appropriate level, that's fine. Go ahead and pass through. We will work with you on matching that to the Federal Student Aid version of that account, and we'll take that token.

Online Audience Facilitator: The follow-up question was, wasn't there an earlier attempt by the federal government to have a similar bridge project in the mid-2000s that didn't work?

Richard: Yes, there was. Actually, I think there were a number of runs added. There are several examples of it going well. You go out to the NIH community, the researchers figured this out quite a long time ago. We're fortunate that they're at the table with us. I think some of the problems had to do with understanding the dynamic of what the bridge technology is going to take. Even the Fed right now is struggling. We actually are architecting a solution that says that you can use any of your appropriately privileged accounts to get into a federal system.

It just may happen that — especially with federal student aid — we have the majority of accounts. Wouldn't it be cool, I think, to say that, "Federal Student Aid, you're a consumer of F6, but you're also a provider of identity on F6."

So that when the student pops up and gets a Federal Student Aid account or however, they get in there, they can use that same account to go over to Social Security or go over to the Department of Labor or go over to some other place or to go into one of the institutions that's a consumer.

Right now, the bridge is being set up as unidirectional, but I think at the end of the day, it's going to be bidirectional in the way that allows folks to use their electronic credentials.

Online Audience Facilitator: Okay, thanks.

Kathleen: I think we're actually at [inaudible]. Oh, one more?

Audience Member: There were other reasons that I think the bridge failed, too, having to do with just being early as far as technology is concerned. I want to ask one question, though, having to do [with] HIPAA [Health Insurance Portability and Accountability Act]. The HIPAA privacy thing is fairly similar to the FERPA privacy thing, which a long time ago I wrote an article on in *EDUCAUSE Review*.

The point being, if we're going to have PII for students and PHI [Protected Health Information] for patients, and we're going to expect employees — particularly lower-level employees — to react correctly with that data, we need one set of rules. I don't see here a tying together of the privacy aspect of HIPAA with the privacy aspect of FERPA.

Kathleen: Yeah, I agree. What you suggest makes a lot of sense, but it's also something that would clearly require congressional action, because they're two separate statutes. We have a whole host of privacy statutes, and there's a host of privacy statutes at the state level, as well. Getting that next bridge there... Privacy is an odd thing in terms of where it falls on the political spectrum. It's something that the right and the left actually agree with on the far ends of either spectrum.

Audience Member: [laughs] Yes, right. But the HIPAA thing, it's very interesting because... I lost my train of thought, I guess. We tried to do some of this, and I've done some of it with some of the Texas schools. Health and Human Services ruled that all student medical records are education records. That allowed them not to say anything about them. Yet if you have a medical student that's being treated by a doctor in the medical school, then when that student graduates and still wants to be treated by that doctor, they can't transfer the records to them.

Kathleen: I think we're out of time, but just again, I do agree with you that there's a lot that needs to be normalized between them. One of the most complicated things when we start analyzing which privacy laws apply is figuring out which privacy laws apply. Whether it's because you've had a breach and you need to figure out what protected them, or because you have something new and novel you want to do, it gets very complex. Thank you guys very much.

[session ends]