THE BROOKINGS INSTITUTION

U.S. CAPITOL VISITOR'S CENTER

EVALUATING THE CLOUD COMPUTING ACT OF 2011

Washington, D.C.
Thursday, June 16, 2011

PARTICIPANTS:

Welcoming Remarks & Moderator:

DARRELL WEST
Vice President and Director, Governance Studies
Director, Center for Technology Innovation
The Brookings Institution

Panelists:

CHARLES FIRESTONE
Executive Director, Communications and Society Program
The Aspen Institute

STEVE KOUSEN
Partner and Vice President, Federal Engineering and Cloud Computing Services
Unisys

DAN REED
Corporate Vice President of Technology Policy and Strategy
Leader, eXtreme Computer Group
Microsoft Corp.

PHILIP L. VERVEER
U.S. Coordinator, International Communications and Information Policy
U.S. Department of State

* * * * *

P R O C E E D I N G S

MR. WEST: Good afternoon. I'm Darrel West, vice president of government studies and director of the Center for Technology Innovation at the Brookings Institution and I'd like to welcome you to this forum on cloud computing. This is the latest in a series of forums that we at Brookings have held over the last two years on the cloud.

There clearly are many exciting things taking place in that area so we've undertaken research, we've written a series of papers that are available at brookings.edu, we've made recommendations on ways to make greater use of cloud platforms. And in our work we've found significant efficiencies and cost savings through cloud computing. Rather than storing and accessing information on your desktop computer, it is now possible to store and access data, information, and applications through remote file service so it would be accessible wherever you happen to be, on whatever platform you happen to be using. And I think this is especially advantageous in the public sector where agencies and departments have been slow to embrace the cloud, and I know there are several people here from Capitol Hill who work on congressional staffs, so we're especially pleased to welcome you and we look forward to any questions and comments that you have.

But obviously despite many of the promising features in the cloud, there are many challenges in this area as well. There are concerns over privacy and security, what kind of information government agencies should place on the cloud. There's a question of international jurisdictions, who has legal jurisdiction if information originates in one place but resides on a cloud elsewhere. What happens to the concept of a cloud if the United States, the European Union, Russia, China, or other countries end up with different laws governing data storage and/or privacy? Are we going to end up with a Tower of Babel version of the cloud with different rules in different countries and

difficulties navigating and communicating across jurisdictions?

Many of you know that there are several senators working on a draft of bipartisan legislation designed to address these as well as other issues. The Cloud Computing Act of 2011 is, was introduced and sponsored by Senators Amy Klobuchar of Minnesota and Orrin Hatch of Utah, and the drafts that we've seen so far is proposing to make cloud computing safer and more convenient. Among other provisions, it directs the federal government to negotiate with other countries to establish more consistent laws on security particularly in regard to cloud computing. It also recommends new civil and criminal enforcement tools to investigate and prosecute hackers, and it addresses federal procurement issues and requires all federal agencies to put together cloud computing plans.

So, to help us develop a better understand of this subject, we have put together a distinguished set of speakers. Dan Reed is the corporate vice president of Technology Policy and Strategy and leader of the eXtreme Computing Group at Microsoft. Dan helps to shape the company's long term strategy and vision for technology innovation. He works closely on cloud computing in particular, and ways to advance the state of the art in computing more generally. He also serves as vice chairman of the Tech America Cloud Commission and prior to joining Microsoft he was the Chancellor's Eminent Professor at the University of North Carolina and director of its Renaissance Computing Institute. He's somebody who has had a long and very distinguished career in many aspects of computing.

Ambassador Phillip Verveer is the U.S. coordinator of International Communications and Information Policy at the State Department. He is somebody who has practiced communications and anti-trust law for more than 35 years. He's an expert on many different aspects of communications and information policy, and in his current job he is looking at some of the international aspects of this area.

Charles Firestone is executive director of the Communications and Society Program at The Aspen Institute. In that capacity, among other things, he focuses on the implications of technology for leadership and the impact of new technologies on social institutions and Aspen has been doing some very interesting work on the international aspects of cloud computing so he'll be filling us in on that.

Steve Kousen is partner and vice president of Federal Engineering and Cloud Computing Services at Unisys. In that position he leads a 400-person engineering, operations and technical support practice. He handles the secure cloud computing initiative at the company, and its federal center for excellence, among other things, and so he's worked really closely with a number of federal departments and agencies as a move towards implementation in the cloud computing area. So, in terms of our format, we're going to try to keep this conversational. I'm going to pose some opening questions to our panel and then we will open the floor to any questions or comments that you have. So, we'll look forward to hearing your perspective as well.

I wanted to start with Dan Reed of Microsoft and just ask, what exactly is a cloud? How is it changing how the government and private sector uses information technology? And what do you see as the concerns about moving to the cloud and what are the most important steps that the government can do to address that? I know that's like 15 different questions. But that's my prerogative as a moderator.

MR. REED: And you want me to do that briefly, of course.

MR. WEST: Absolutely.

MR. REED: So, what's a cloud? Fundamentally from an infrastructure perspective a cloud is a massive scale collection of computing and storage, and let me give you a, perhaps, reference benchmark to calibrate scale. The big cloud data centers are somewhere between 10 and 20 X the size of a football field in terms of footprint. They're the largest computing infrastructures by any reasonable measure we've ever built

in the history of computing and that consolidation of network-delivered services is really the fundamental enabler of cloud computing.

What's driven it is in essence a change in the economics of infrastructure. If you think about the analogy of what a big box retailer has done in terms of logistics and supply chain management, its scale purchasing management, (inaudible) the same kind of economics occur in the cloud computing infrastructure. It allows you to deliver services over the network. I would say as an aside, that's one of the other reasons why broadband penetration wired in wireless is really critical, because the network is the oxygen that allows cloud services really to bring you both consumer, government, and commercial aspects.

Changes in benefits, in some sense, are those economic efficiencies I mentioned that allow the cloud service providers to operate services at efficiency that the analogue or smaller scale might not be possible. It also allows groups to focus on their core competencies. I think the lesson that we learned in many domains is that successful entities are the ones who figure out what they really do better than anybody else and what their core mission is, focus on that aspect, and partner with other entities that have similarly identified that scale base.

From an economics perspective it brings a pay-as-you-go model, that you pay for services and you don't have sunk upfront investments in capital for massive computing. That's part of what has driven and pushed (inaudible) has pursued about consolidation of federal data centers. It also creates some nimbleness because it allows the service providers potentially to adapt rapidly to technology change and amortize those costs across a large number of customers. Those are sort of the operational kinds of things.

The flip side is what is it bringing in terms of some new capabilities? One is the ability to extract insights from data at large scale. We certainly see it in

government circles, private sector and consumers, about the explosion of data poses new challenges for retention, for management, in analytics, and there are certainly a lot of opportunities there. These are tools for collaboration and sharing across disparate groups, both public and private sector, because collocation creates some abilities to correlate data, it brings some challenges as well. It also creates the opportunity for some context-specific services across consumers, across government, and across business. So, if one thinks, for example, about the promise of intelligent transportation systems where we can do better real time traffic management by analyzing sensor datas and providing advice, what that means for the future of greener transportation for hybrid and EVs where we need to do better energy management for batteries, there are opportunities there, and it brings some opportunities for innovation.

One of the things that's true about startup companies is that the ability to launch an enterprise without sunk cost in capital and IT or limited skills brings some changes.

What are some of the challenges? Actually, Darrell touched on many of those. Many of the issues center around concerns about privacy and security. Some of those concerns are real. Some of them are perception. Some of them are sorting through some of the ambiguity about legal and other constraints that exist. There are very practical issues that the Cloud Computing Act attempts to address in terms of penalties for hacking and trying to rationalize those, because it's not clear at the moment whether penetrating 1 account or penetrating 1,000 accounts are, in fact, treated similarly. From a legal perspective they clearly have very different practical consequences.

The transnational data flow issues are ones that, as Darrell said, the cloud commission (inaudible) is wrestling with, how we try to define some rules of the road so that people understand what expected behavior and practices might be, trying to

rationalize those on an international scale.

I think there's some practical social issues with respect to government procurement as well, that in many cases it's easy to rationalize buying a thing, it's much harder to explain buying an intangible, and that's what a service is. It transfers some responsibilities from the group that procures the thing to the management of those who provide the service, and like all technical change, social change is always the biggest hurtle.

All my years in the IT business, I've talked to people about big IT projects can succeed or fail. I've said the top 9 reasons why projects succeed or fail are culture, number 10 is technology, and this cloud transition has all of those similar issues. And then finally there are the issues of standardization and interoperability. The ability to fuse data across different cloud providers and be able to have interoperable services that cross those boundaries.

Despite those challenges, I'm absolutely convinced that this is one of those major sea changes, transitions in technology and computing. We have those -- they happen every decade or so. We're in the midst of one now. There's a huge opportunity. The U.S. is without a doubt the international leader in cloud computing. And what we're here to talk about today is how we continue to take advantage of that and make sure for public and private use that that remains the case.

MR. WEST: Okay, Dan, thank you very much. That leads directly into Ambassador Verveer. So, you work at the State Department, you coordinate international communications and information policy. As Dan was mentioning, these international issues, potential problems in terms of transnational data flows. Can you fill us in on what the Administration is doing in these areas?

MR. VERVEER: I'd be happy to try. As Dan said, there are cultural, legal, regulatory obstacles to the full use of the cloud possibilities, and we're trying to

engage with (inaudible) around the world in terms of seeing if we can't find ways to reduce the obstacles and I think it's very important to understand these obstacles actually are quite formidable.

The essence of the obstacles, I guess, is the transborder data flow issue. There are very significant innovations in terms of moving personal information from one country to another, probably the most significant legal arrangement that governs that is the Data Directive that the European Union instituted in 1995, which makes it very hard to move information from one place to another. And the essence of the cloud opportunity in face is data centers located in more than one place, very often in more than one country, so that if you're going to take full advantage of the opportunity, you've got to be able to move the information as free of legal frictions as possible.

The 1995 Data Directive is now in what the Europeans describe as a consultation. That is to say, the Europeans are looking at whether or not it is going to be important to change, to amend their approaches based upon the realities of present technology, changes in commercial practice, and the changes in the consumer behavior.

We are trying to engage our European friends with respect to that process and with respect to others in the world as well. I think talk about perhaps two specifics. The trans-border data flow limitations are limitations that are grounded principally in concerns about privacy, individual privacy. We, in the United States, are reexamining some of our protections of privacy. The Commerce Department issued what is called a "green paper" that is a set of proposals with respect to protecting individual privacy is thought sometime within the next two or three months to become an Administration proposal, (inaudible) government's proposal with respect to finding new ways to protect privacy. Likewise the Federal Trade Commission is involved in efforts to address questions of behavioral advertising, that involve the accumulation of data (inaudible) personal use is particularly online, but not exclusively online.

We're trying to discuss with the Europeans the ways in which our approaches here and their approaches have a great deal in common. We are not ascribing to (inaudible) completely homogenized or harmonized approach that would be something that I think we believe and the Europeans believe is utterly impossible. But we think if we can bring the approaches close enough together as both sides are making adjustments in terms of their efforts to protect privacy, we may be able to find ways to permit the relatively relaxed transmission of information back and forth without the kinds of (inaudible).

Similarly, we've been talking with the Japanese delegation about its reports and here the recent earthquake and tsunami has created a special center of concerns and insights in Japan. One of them is that the tsunami ended up wiping out the entirety of the personal records in the areas where the tsunami damage was the worst. People's lives as reflected in documentation have essentially been eliminated, and this has caused some reflection on the desirability of geographic redundancy in terms of the maintenance of the kinds of records that all of us rely on to define who we are. And our friends in Japan are now seriously considering the question of the desirability of storing at least copies of records electronically here in North America in addition to Japan, (inaudible) the possibility of future disasters.

That then leads to the last thing probably worth talking about (inaudible), which is the ability of law enforcement and security services to get access to the information that happens to be stored within the national territories of the particular country. This turns out to be a very difficult question and it's a very difficult question for us because, among other things, our law enforcement and security services have some ability to get access to records through administrative subpoenas, that is through efforts that involve third party oversight, and the concerns that our practices raise are magnified with respect to many other administrations around the world where the confidence in rule

of law, the confidence in the legal procedures being conducted fairly, scrupulously, with integrity, are not something that (inaudible).

And so among a whole range of legal and regulatory questions we have to try to put this -- we have to try to provide comfort that there won't be arbitrary access to information that happens to be stored within a particular set of national boundaries.

Now, there are a whole range of additional issues that we could go into and if you're interested in the discussion I'd be glad to do that, things like liability of cloud providers, whether or not they're responsible for consequential damages, the questions about whether or not as small- or medium-sized enterprises begin to make more and more use of the cloud that the take it or leave it terms and conditions under which small- or medium-sized enterprises will, in fact, be honored by local courts. To say it in one word, questions of jurisdiction.

If there's anybody here who's interested, I'd be very happy to talk about this.

MR. WEST: Okay, thank you, Ambassador. Charlie, I know the Aspen Institute has been working very hard on many of these international issues, so can you describe what you're finding and any recommendations that come out of your work?

MR. FIRESTONE: Thanks. Thanks so much for having me here. So, also in reaction to all these issues that Dan and Ambassador Verveer proposed, we've undertaken something called the Aspen IDEA, which is the International Digital Economy Accords Project, which is looking towards a multi stakeholder process to address these issues internationally. Yes, the governments can get together, although it's difficult for bilaterals (inaudible) throughout the world, there is -- legislation points to the OECD. This came up at the G-8 and comes up at various other international fora, but what we undertook was something that would bring together businesses. We have about 35 businesses at this point, NGOs. We're hoping to get more from the global south and

we've been involving government people as well going back and forth, but we don't want it to be a government activity. We want to work with government, because ultimately what we're looking at is fostering an international regime for a single, global, digital market of goods, services, and ideas, one that would create a trusted environment, trusted environment meaning you have to deal with these very issues of privacy, security, and intellectual property, which we haven't touched on, but is also a very significant element of the trust environment, one that would promote a robust ongoing global common medium where you could have not only the exchange of goods and services, but the exchange of ideas. And I know the State Department's very -- has been very instrumental and important in that respect with freedom to connect and so on.

So, what we are -- where we are right now is that we've had a few convenings, most recently in Brussels where, by the way, I should mention that Viviane Reding, who's the DG -- the head of the European Commission group that oversees -- I forget what it's called -- but anyway, it's privacy -- was very encouraged. And if you know Viviane Reding, for her to say that she's encouraged about where the U.S. is moving on privacy and that it looks like it's an opportunity for them to start negotiating with people like Ambassador Verveer is very encouraging.

What we are doing is creating a series of working groups that are looking at first this basically free flow of communications, meaning that basically -- the single market, that basically meaning that we can have free trade in all these services, that you don't have to encounter local laws that are restricting for the purpose of protecting their own -- some company within their borders, especially with borders being so porous.

Second, going to the free flow of communications, what does it mean to have what amount to end-to-end communications across international boundaries, in that robust, common medium that we know of as the internet today, wherein we have some countries that are making moves and indications that they may somehow or another wall

themselves off. Iran being a recent one, China, who knows what's going to happen there, you know, we saw it with Egypt briefly and -- but probably the most controversial area being the area of the trusted environment. That's our three areas of privacy, security, and intellectual property.

And the aim -- and I'll wrap up with that -- where we hope to go, is to have basically a framework that you would present to the governments to look towards some kind of executive agreement or international treaty or some sort of analogue to what the governments did in 1997 with the telecom annex to the World Trade Organization Agreement. So, in other words, where we -- what we did in telecom in '97, how do you do it in digital in, you know, in the 20-teens? Much more complicated, many more issues, many more technologies, many more countries involved. Secondly would be a series of global norms that we hope people will sign on to that we're working on developing that would be consistent with what the OECD is doing, what the -- there are some other organizations that are coming up with these principles or norms that people can ascribe to, we're working on those and hope that we can have companies and NGOs and ultimately even countries agree that this is the way the internet should work, and finally, maybe either the reference to or the creation of a new NGO that would monitor the situation. Thanks.

MR. WEST: Sounds like you have a very busy agenda.

MR. FIRESTONE: Oh, my god.

MR. WEST: But a fascinating one working with (inaudible).

MR. FIRESTONE: Yeah, I (inaudible) that this was brought in to us by Reed Hunt, who is the former chairman of the FCC under the Clinton Administration. And anyone who knows Reed knows that he's both brilliant, foresighted, and all-consuming, so this has taken up a lot of (inaudible).

MR. WEST: He is somebody who likes to think big, I've noticed.

One other aspect that the proposed legislation addresses is the issue of federal procurement in acquisitions and I do want to clarify Senator Klobuchar has been working with Senator Hatch, they haven't actually worked out all the details in terms of co-sponsorship and so on, so I wanted to clarify that.

But Steven Kousen of Unisys, what do you see as some of the challenges facing cloud service providers in regard to federal procurement and from an industry standpoint, why is it valuable for federal agencies to provide a forecast of their cloud computing needs?

MR. KOUSEN: Okay, thank you, Darrell. Before I answer that I would like to thank the Brookings Institute for hosting this event and would also like to thank Senator Klobuchar and Senator Hatch for their interest in cloud computing, their hard work and leadership in helping to draft the legislation that we're talking about today.

So, regarding the federal procurement and the challenges that the cloud service providers and Unisys, as a systems integrator as well, face involve a few things, the first one being an on ramp acquisition strategy. So, a lot of these solicitations come once a year or twice a year and ask for service providers and systems integrators to offer their services. With the market dynamics driving so fast, it's not unusual to have a lot of new entrants into the marketplace every day. You want that kind of competition to help drive the cost down and you want that to be a regular routine in order to allow those new providers and those new offerings to be able to get on a schedule to be able to offer their services. So, I'd recommend that.

And the second one, there used to be an allowance to address unique requirements. From a service provider perspective we're certainly trying to commoditize services in order to lower the cost and provide the best value to the federal agencies and what we're seeing is (inaudible) the services is it's not unusual for a unique requirement to come up. It's hard to think of a lot of the requirements and address all of them when

you're putting out a solicitation, so the procurement solicitation do allow for specific one off, unique contract line items to be able to address things that come up, change management, communications management, those types of things.

And the third thing, I believe that there needs to be flexibility to allow the cloud service providers to be actual utility providers and by that I mean oftentimes we provide services to the federal agencies, the cost savings can be derived when an agency doesn't need as many services or servers or pieces and they can start to de-provision when they're not in use, thereby saving them money. When you change infrastructure like that, there are a lot of regulations you have to adhere to, operational compliance, security compliance, and so the procurement solicitations need to allow service providers to be able to adjust their services to give back money and give cost savings back to the agencies without having to go through a lot of the compliance requirements after they first get approved. Thereby we can start to keep lowering our costs.

And Darrell, to address the other pieces of the five-year forecast, it's important to the service providers to receive as long a roadmap as possible on the new requirements that the federal agencies are going to have. These are changing every year as you can imagine, so if the service providers are able to craft the right solutions to meet those requirements and know about those requirements ahead of time, it's not unusual to take a year to help piecemeal together a nice and appropriate solution to address the unique requirements, and the further ahead we have it, the better it is.

Also, the services, when the services are first starting to get offered, you want the providers to be able to introduce those services in a very efficient way, a very efficient cost, and the more the providers provide those services, the more efficient they will become. So, the longer lead time we have to be able to prepare the -- to provision and provide those services, the more efficient we will be able to provide and the more

efficient they will be able to past those cost savings on.

And then lastly, while that's just a prioritization of where we feel the federal agencies are going to want to emphasize, whether it be in infrastructure as a service or software as a service, or platform as a service, it's important to know where to invest our own money and funds into providing those services to the federal government.

MR. WEST: Okay, thank you very much. I want to throw out one question for the panel as a whole and any of you can jump in and then I'll open the floor to any questions and comments from our audience.

In our discussion -- I think each of the speakers picked up on points of these -- we talked about security, we talked about the international aspects, Steven just covered the acquisitions, the ambassador mentioned law enforcement, the question of liability. We're sitting here on Capitol Hill so each of you has an opportunity to give advice to members of Congress and we have a number of Congressional staff people here, so I was just wondering if each of you could just make a couple of specific recommendations, like things that you think based on the problems you have identified and actions that you think would really make a difference. Like, what are one or two specific ideas that you think would make the biggest difference in this area? Any of you who want to address that.

Don't everyone speak at once because that is so rude.

SPEAKER: Well, there are -- there have been suggestions about changing some of our privacy laws in ways that I think would be helpful. The Administration has made some suggestions along those lines. Taking those up in a serious way would be very useful. We also need to look at -- and I say this without any strong sense of exactly how we should address it -- but laws like our Electronic Communications Privacy Act that was passed now on the order of 25 years ago, have obviously been overtaken in serious ways by technology and by the actual practices that

we're all familiar with.

These things have to at least be looked at seriously. There have been some hearings about it. There are going to have to be more -- I think there's going to have to be more examination of it. Things of that nature that bring our important legal activities into line somewhat better with the realities of the technologies and the behaviors that we're all familiar with would be something, I think, that's desirable in terms of eventually getting international support for the kinds of important things we need to see happen for cloud services to operate efficiently.

MR. REED: I would echo that. I completely agree with that. I think there's the more general issue here that clouds and communication expose, which is the rate of technical change in many cases is outstripping the rate that we socially and culturally define frameworks to reason about those things, and I think this is a place where policy frameworks that define guardrails of behavior but allow the unexpected to happen, which I think is part of what Steve was also saying in terms of procurement, is we don't -- none of us have a good enough crystal ball to know what will really happen in some of these domains.

We know some things we don't want to have happen. We want some clear guaranties for privacy and security and the rule of law to be applied when we deal with these issues, but within those constraints there are many unexpected things that can happen as the technology shifts and moves, and one needs only to look backward a few years to see the effects of the unexpected.

I think one corollary of that is being clear about what best practices and standards are and so if you look at the Commerce green paper, you look at the cyber security plan that's been promulgated, those are some of the recommendations there. To be clear, that these are the best practices to be applied and continue to support those mechanisms as we move forward.

I think those will go a long way to help address the uncertainty that I mentioned at the outset because with any new technology, change brings some degree of fear, it challenges existing cultures saying these are the kinds of rules that can be applied, will make a difference.

I should say, finally, on the technical front, I think there's need for continued investment in technology to improve cyber security. There's an R&D component there. It's certainly a place where Microsoft itself is investing a lot of work in trying to advance cryptographic standards and the software support to provide cloud security. That's something that all of us need to continue to work together to support.

SPEAKER: Well, I guess (inaudible). The privacy point that has been made by the other two people, I mentioned at the beginning the interest of the European Union in the privacy movement towards greater protection, I think would be worth taking a look at because it could lead to greater global confidence and in cloud services which are a big -- you know, it's a growing part of the U.S. economy, so this is good -- you know, it's actually good for business.

Secondly, I would say that, you know, the U.S. is a leader in all of these businesses and we're also a leader in our attitude toward governments of this area, particularly the light hand, and we have now -- the United States has not -- well, you know, we've had a little jousting, for example, with the Commerce Department, with ICANN, the International Corporation of Assigned Names and Numbers, which gives domain names and overseas domain names. The point being that the rest of the world is going to be the vast majority of internet users. You know, we're now out to -- you know, at least we have mobile phones in the billions now throughout the world and, you know, we will see a couple of billion, if not more, new people getting onto the global-wide network in the coming few years. We have to allow for other people to be -- have a voice in the governance.

At the same time we at least -- I think we have a healthy skepticism of international governmental organizations running it, so that skepticism, that American skepticism, and a light hand at the same time, you know, dealing responsibly, you know, and fostering trusted environments and (inaudible) communications, I think is very useful and very good to keep in mind as we think about any legislation that comes up.

SPEAKER: Darrell, just a note very quickly, going forward in the future the emphasis to place -- or at least to continue is the cloud first strategy. There will be changes in different members and different leadership, but I think that as Dan said, this business model is here to stay. I think the economics are proving that. I think it's a very impactful model that will save money, and I think that the agencies need to know when, where, how, and actually why, they're asking for cloud computing services. And I think that this continued emphasis to do this cloud first strategy will allow them to think that way, work together with their agencies, and try to foster an environment where it makes sense and why they're provisioning it.

And then lastly, the other piece I'd like to note is around the standards of interoperability. I think as these agencies start to leverage client services you'll have a lot more private clouds, public clouds, and there will be a proliferation of those types of services. It's very important that these clouds be able to talk among each other and with each other and the data as well. You don't want separate islands being built independently. That will help take away some of the cost savings and the benefit synergies that you're able to gain.

MR. WEST: Okay, great suggestions. Let's open the floor to any questions or comments that you have.

Yes, sir? And if you could kind of give your name and if you have an affiliation, that would help, too.

MR. ALEXIS: Alexei Alexis from BNA Computers. I was wondering of

the ambassador if you could elaborate off the discussions with the Europeans about our privacy laws versus theirs and where you see those discussions going.

SPEAKER: The question involved our discussions with the Europeans with respect to their privacy laws and ours and how our discussions are going. I guess the first thing to be said is there are discussions about this that are taking place almost constantly. Now they take place in different contexts. There have been very important discussions that are handled by our law enforcement security agencies with respect to thinks like passenger name records and terrorist finance activities. So, these are discussions that have been going on for some time, they continue as we try to work out ways that are mutually agreeable with respect to providing for law enforcement security services the kinds of information they think they need to combat terrorism without unnecessarily compromising personal privacy.

On a separate track, we have conversations going on a -- I think it's fair to say very nearly a continuous basis as well about these kinds of issues. Now, many of them are quite informal. There are a well-known group of officials in Europe who are concerned with the privacy related adjustments (inaudible) for the data-directed consultation (inaudible) activities, so we deal with (inaudible) officials who are responsible for privacy, individual member states, with Peter Hustinx, who is the person who is responsible, in a sense, overall for privacy related doctrines in the European Union, and with the officials at the European Commission who have an important stake in that and there are a good many of them. Their jurisdictional realities overlap very much as ours do here in the United States in terms of our government.

So, we have those discussions on, I think, an ongoing basis. The ones that I've been involved in -- most involved in, we'll have a meeting occurring in Brussels on July 1st that is centered around the issues of cloud computing, the questions of privacy are going to be quite central to that.

Again, my personal hope here is that we get to something that would permit a kind of mutual recognition of one another's requirements with an understanding that the way these requirements are being imposed, the way they're being enforced, should give everyone on both sides of the Atlantic sufficient confidence to permit us to gain the advantages of the cloud without any unnecessary impairments while obviously also protecting the important values of privacy.

MR. WEST: Other questions? Right here on the aisle. And there's a guy with a microphone coming. Yeah, right there.

SPEAKER: (inaudible), Blank Room. We all talk about privacy in general, but if we're talking about implementing like the cloud and pretty much all government agencies, has there been any -- I guess any questions raised about high profile security breeches in the near past, and so what sort of assurances can U.S. companies give to the government if we want to start putting like all of our agencies onto like a singular system that -- like in -- you know, like to a layperson seems like it would be more vulnerable to infiltration as opposed to a physical system.

MR. REED: I think I'm the corporate rep, so I think that means I'm supposed to answer this question. But others should feel free to chime in. That relates to some of the things I was talking about before. I think there are some technical ways and means that are not widely and broadly applied, some fundamental issues about how one can provide the ability for third parties or for consumers or for government agencies to verify that software and the data that are stored on the facilities are, in fact, untouched and unencumbered and ways, in fact, that one can provide privacy guarantees. Because one of the big concerns about privacy, frankly, is not just exterior penetration, but, in fact, that the host of the data and services might slip on those things, and that's one of the transnational issues as well as it is one of the domestic consumer concerns.

That's a place where empowering individuals and agencies with

technology can really help, so I give you -- and this is as close to being a geek as I try to get here -- there's a technology called searchable encryption, which means that data that is stored in the cloud can be stored in an encrypted form. The people who generate the data control the keys for that. The data remains encrypted. They can pose queries against it completely in an encrypted form, and the host of the data does not have those keys.

There are a variety of other mechanisms to verify that the software running on the cloud is, in fact -- has not been penetrated. Those are technical ways and means, and if you look at the Commerce white papers and the cyber security plans, many of what they propose as promulgating clearly what those practices are and the security standards that need to be adopted across the government agencies, and that the cloud services -- service providers need to support and provide. That's a technical aspect.

From an operational aspect, even across government as well as across consumers and business groups, the quality of actual security practice varies widely and one of the things that's true is -- and this goes back to the focusing on what professional skills are -- there are some collateral advantages from cloud consolidation in terms of raising security standards. You're right, that potentially creates a larger target profile, but you also then bring to bear some best practices and professionals whose only job is to think about those kinds of issues, and that's one of the other aspects.

Smaller groups, in fact, if one speaks to the business aspect, for example, if you're a small business odds are your security is not very good because you likely don't have the revenue or, in fact, the IT expertise to procure world class security, and so there's that perception versus reality, but a lot of this is about pushing our best practices, articulating standards, getting those guardrails and agreements that I was talking about, and I suspect Steve probably has something to say about that, too.

MR. KOUSAN: I would agree with everything Dan says. And the only thing I would add to that is there are minimum level of security compliance requirements that cloud providers must adhere to, and the Federal Information and Security Management Act 2002, it's called FISMA, is one of those guidelines, and at least a minimum guideline. There are advancements being made to that Act. I think at a minimum the cloud providers need to show that they're following those security guidelines and that is one way they can, at a bare minimum, make sure their cloud meets those requirements.

MR. WEST: And just one quick thing I'd like to add to your question. When I talk with audiences I often find that people believe that if they have the information and the data in your position and stored on your machine, that that automatically makes it safer because you personally are controlling it and then if you save something on a remote server, some place out there that automatically means it's less safe.

I have visited cloud providers and data storage facilities and I'll tell you, these places are like Ft. Knox. I mean, they have armed guards, they do very detailed background checks on their employees, so my impression is, you know, these people take security very seriously because the industry knows if there's a breach they're the ones who are going to end up having huge problems out of it.

SPEAKER: Thank you. My name is Pat (inaudible). I'd like to ask while we're thinking about the standardization, nowadays we have a lot of various data, not only are they structured data, but also the voices or videos and (inaudible) sensor outputs. And I think the -- it's very necessary to prepare the standardization of format, data format, and also the identification systems. How do you think about this?

SPEAKER: I can give a quick commentary about the standards being (inaudible). So, there are a lot of standards bodies and it's a common topic now amongst

those standard bodies. On one hand, I think, that there's a feeling that let's harden the standards now and make those public and have everybody conform to those early to ensure that people that are collaborating together can collaborate, and I think that's a good thing. On the other hand, I think when a new emerging relation hits the market and it gets patrolled and people are adopting it there's a timing effect of when you start to lock down those standards. If you -- some say that that will stifle some of the imagination and innovation and creativity. I'm not quite sure we're there yet where we can lock those standards down, but I think the bodes -- the standards bodies that are working toward it are doing the right thing, they're talking about them, they're starting to socialize them, and we'll see a natural progression toward the right standards.

Some say that what's in actual practice today, what people are actually using, that should become the standard because that -- you don't want to have a standard sitting on a shelf. So, I think there's a little bit of that logic that's being used within the standards bodies and I think they're doing the right thing now.

MR. WEST: Right here.

MR. RIFKIN: Jared Rifkin with CSS. I was kind of wondering with recent hacks how you see -- especially the international panelists, how you see this playing out in terms of liability and jurisdiction, because let's say there is a cloud -- you know, would the cloud provider be -- if the cloud is in a different country, would the provider be liable or would the country itself be liable for going in and determining what data was taken? And, you know, we currently have problems domestically with the government being involved in the private sector, so how do you see that playing out in a broader international context?

SPEAKER: It's one of the most difficult areas, I think. I think just to start with the question of liability -- despite the very extensive efforts at security that are undertaken and I absolutely agree with the comments about the likelihood that most of

the cloud service members are providing a level of security that vastly exceeds that that at least small- and medium-sized enterprises and, unfortunately, individuals are able to provide.

But despite that, we know that statistically there are going to be some security breaches. We see it happening and the experts that I've spoken with in the government say something that I think is a commonplace which is that these days in the cyber security realm the offensive capabilities vastly exceed the defensive capabilities. It's just kind of a reality at the moment. So that we know that there is exposure here and one of the first questions is going to be whether or not the providers of cloud services are liable for consequential damages. That is the sort of thing that could be absolutely ruinous in terms of the ability to see these cloud services proliferate with what, at least in my view, are the absolutely immeasurable positive externalities that they provide for small and medium sized enterprises or individuals.

So, this is an issue we've got to try to have an adequate handle on.

Now, typically, the terms and conditions of service that are available will disclaim any liability, they will disclaim any indemnification and things of that nature. So the next question is will the courts honor that? And there you have to presumably look at the consumer protection related laws of every conceivable jurisdiction and make predictions about whether or not that might appear to be aggregated circumstances and that the courts would honor contractual provisions that disclaim liability. My guess is that we would discover in many instances as we get to this point, they might not, in fact, they probably will not.

And that then will maybe bring us to the even more complicated question of jurisdiction. These services are being provided on a multinational basis in many, many instances. There are data centers in numerous countries, employees handling that data or tending to the data potentially in even more countries. There are intermediate venders

of one kind or another who are providing the transmission services between and among the data centers, and so you have the possibility of assertions of jurisdiction occurring in numerous national judicial systems.

We don't really have an answer for that yet. I think to be fair, it hasn't really yet become a serious practical problem. It is foreseeable that it easily could become a serious practical problem, and it's one of the things that we have to work at either in terms of developing norms or conventions where one or another jurisdictions will respect the notion that, for example, perhaps the proper place for adjudication of disputes is whatever the contracts happen to specify, assuming that they seem okay and that they're -- there's some learning on this that's available now. But the fact of the matter is, we're at a very early stage in all of this and the possibilities of jurisdictional complications loom large and as time passes, I'm afraid we're going to see them begin to become a real issue, a real problem, and sorting these things out on an international level is going to be no small activity. It's the sort of thing that could potentially take a very long time and an awful lot of good will to come to some set of agreements internationally about who's going to be responsible for adjudicating problems.

SPEAKER: I agree with all that. What I wonder is whether there isn't going to be some massive law case that will be the considered judgment of the -- you know, those gears that are moving towards coming up, you know, rational solutions and, you know, of course abroad where some place will come up with its own resolution probably.

I don't see the liability of a country, if that's what you're -- that's what I inferred you saying at one point. Okay. Yeah, just to clarify that. You weren't saying that a country would be liable.

And one last thing is that we were at a conference last year, grappling with this and, again, I agree, this is a long experimental, you know, there'll be different

attempts, a group came up with some concept of (inaudible) digital embassies, the idea that you would be treated with the way you -- under the law that you came in under throughout the transmission of that data, wherever it went. Well, that would involve countries agreeing, you know, to that in a jurisdictional basis, but some kind of concept where, you know, when you're going to an embassy in a foreign country and you go to the American embassy, you're in American territory, so it would be that kind of concept that hasn't played out fully but was suggested.

SPEAKER: I just want to echo and agree with what was just said, but let me paint a vignette to sort of drive home the complexity, hypothetical. You're a Kenyan working for a German multinational whose data is hosted in a U.S. data center, you're traveling in China. Whose laws apply? That's the complexity of the problem.

MR. WEST: In the front row we have a question.

SPEAKER: While you're doing that, one last thing, which is anybody who went to law school knows that conflicts of laws was like the most complicated course and somewhat difficult -- some of the great thinkers really tried to apply, and this is just going to give them wonderful, not only exam questions, but -- I think I just did, but you know, wonderful attempts to kind of come to grips with this in the digital age.

MR. WEST: It will be a great exam question, but no one will know how to grade it.

SPEAKER: Well, that's a good exam question.

MS. DOCTOR: Hi. Roz Doctor with IBM and my question's for the ambassador. A lot of these issues we're discussing are going to be handled contractually, as you mentioned. Do you think as you look towards policy and mutual recognition with the EU there's an advantage to making a distinction if you're talking about public clouds or private clouds? Can you comment on that, please?

MR. VERVEER: Surely, this is a very important distinction between

public clouds and private clouds. The private clouds are presumably going to be arrangements that have been negotiated between and among a vender and a customer and I think that where you have negotiated arrangements, the courts are very likely to honor whatever the ultimate outcome is in a contact.

The place where I think the largest complications arise are with respect to so-called public clouds where numerous customers are bringing their activities to a vender, the vender is dealing with these in some ways in common. These are typically not going to be negotiated arrangements but rather arrangements that have been secured on the kind of standard terms and conditions, take it or leave it, and it's in those circumstances that I think the kinds of jurisdictional problems we've been talking about are likely to be most acute.

MR. WEST: Other questions? Right here.

SPEAKER: Yes, on the -- (inaudible) with Government Computer News. On the subject of security, whether you're in the cloud or outside of the cloud, you know, infrastructure, protecting the infrastructure seems to be very important. We hear a lot about the -- in this world of multi type of environment with cloud computing that there's more a need for data centric security and controlling who has access to data, and make sure they only have access to the data they're authorized to have access to. So I'm wondering about this sort of data rights management, enterprise rights management. Are the tools or technology there to -- for the cloud with regards to, you know, data rights management?

MR. REED: So, that's an excellent question and I completely agree with the premise. I think that's a place where the continuing cat and mouse game goes on. It's why I was talking about some of the technical advances. If you think about -- to the ambassador's point about public clouds where you have -- and your point about co-tenancy, if you think about mainly the ways that many groups work, there's both

collaboration and competition. So, there's limited sharing of information that people might choose, again, you can construct hypotheticals, a couple of pharmaceutical companies who are collaborating on a particular project, but otherwise are strong competitors in their marketplace. There are lots of analogues of that, and so you'd want limited data sharing and that really speaks to the notion of claims-based access, that you have access to data for a certain purpose, for a bounded period of time, and limited ability to transfer that data to any other parties. And that's a technology development that we see moving forward, so-called claims-based identity. It also speaks to the issues of public cryptography and key management and the ability to advance things, like searchable encryption.

And one of the hot topics in cryptographic research -- and now my academic roots are going to show here again -- there's something called fully homomorphic encryption. That is the ability to do computations on the data that's never decrypted. Because if you think about the standard model that exists now, data that's stored in the cloud is either stored in the clear, that is, it's not encrypted at all and anyone has access to it, that's the data that your web search engine goes after. There's data that's stored encrypted, but any time you want to apply any computation to it to extract material, you have to decrypt it, it is in the clear at that point and is potentially vulnerable to any other intrusion or malicious behavior.

The Holy Grail, in some sense, of public key cryptography is to be able to apply those computations to the data while it remains fully encrypted and only the owner of the data controls that. That's an active area of research in cryptography now. There have been some phenomenal advances made over the last few years. It's certainly not something that's deployable now, but that goes back to this issue of the continuing improvement and the ambassador's point about trying to improve the defense capabilities that we have in response to offensive capabilities.

So, that's why I was saying at the outset to continue to invest in the R&D, both in the private sector and the research sector and in government to drive these things forward is one of the places where NIST is playing an important role, promulgating and pushing standards and verifying the integrity of current technologies.

MR. WEST: You're doing better. It actually wasn't too geeky.

MR. REED: Okay, I tried.

MR. WEST: Although at Brookings it's okay to be a geek, so we don't mind that.

SPEAKER: I think I would just add, as systems innovators are working with cloud providers to integrate those solutions in, we are seeing the advancements out on the marketplace today, much more so than ever before. In addition to what Dan said about the encryption of the data and we have to remember, it's at rest and it's in motion too as well, so you have to think about it as it gets transported, making sure that it's encrypted.

Other technologies that we're seeing and integrating today revolve around the single sign-on principles to make sure that you are who you say you are and verification and something called a dual factor authentication system, it's not enough just to have a password. But we have rather similar technologies to verify, okay, here's your password, but let's take some unique credential about yourself. Check with the federal agency's directory, make sure you're in there first and if you are, in fact, in there, then we'll allow you through. And that technology exists today.

Cloud providers are providing that second factor to your cell phone in verifying -- or a text PIN message that you can also type in addition to your password and they can verify that. And other technologies are springing up to integrate it right into the federal agencies.

So, we're seeing terrific advancements and we're integrating those

today.

MR. WEST: Other questions? Comments? Okay, if not, I'm going to thank all of you for coming up to join us. And those of you who work for members of Congress, please take these ideas back to your members so that they have a better understanding of these issues, and I do want to thank Dan Reed of Microsoft, Ambassador Phil Verveer, Charlie Firestone with Aspen, and Steven Kousen of Unisys, so I thank you all very much for coming out. (Applause)

And I believe we have some food for you out in the hallway as well, so please help yourself.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

/s/Carleton J. Anderson, III

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2012