THE BROOKINGS INSTITUTION

MOVING TO THE CLOUD:
HOW THE PUBLIC SECTOR CAN LEVERAGE THE POWER OF CLOUD COMPUTING

Washington, D.C.
Wednesday, July 21, 2010

PARTICIPANTS:

Featured Speaker and Moderator:

DARRELL WEST
Vice President and Director of Governance Studies
The Brookings Institution

Panelists:

DAVID McCLURE
Associate Administrator of the Office of Citizen
Services and Communications
General Services Administration

DAWN LEAF
Senior Executive for Cloud Computing
National Institute of Standards and Technology

KATIE RATTE
Attorney, Division of Privacy and Identity Protection
Federal Trade Commission

* * * * *

P R O C E E D I N G S

MR. WEST: Good morning. I'm Darrell West, vice president of Governance Studies and director of the Center for Technology Innovation here at Brookings, and I'd like to welcome you to our forum on Cloud Computing in the Public Sector.

And today we are releasing a paper entitled "Steps to Improve Cloud Computing in the Public Sector." Right now the U.S. Federal Government spends nearly $76 billion each year on information technology, with about $20 billion of that devoted to hardware, software and file servers.

But even though cloud computing offers excellent potential for cost savings, very little of current federal IT spending is devoted towards cloud computing. And I think this is problematic because we put out a paper a few months ago on the cloud and we found that government agencies actually can achieve substantial cost savings and efficiency gains through the cloud.

So in the paper that we put out today, I point out several issues that I think we need to think about in terms of our current policy; one is how government often has inconsistent policies across computing platforms. Sometimes there are different rules depending on whether you're talking about desktop computing, laptops, mobile devices or the cloud. We also see differences, not surprising here, across branches of government, Legislative, Executive and Judicial. In Congress, for example, phone conferencing is allowed on mobile and Wi-Fi networks, but not on desktops. So those are the types of inconsistencies where we need to think about making them more uniform.

I think there are also similar issues that arise in regard to privacy rules, although this results more from judicial rulings that have taken place in this area over a period of time.

Some judges have made rulings in which they give consumers greater privacy protections in regard to desktop computing as opposed to cloud computing. Their view is that if you transfer information to a third party, as you would do through cloud computing, that you should have less of an expectation of privacy than if you are using your own machine. But the problem is I’m not sure consumers draw that type of distinction. In an era of multiplatform usage, it’s not clear that consumers know whether they are accessing information, because, you know, if you think about your own usage, people often are shifting from files stored on their desktop hard drive, they may have information on a flash drive or some other mobile storage unit, and they kind of weave in and out of the Internet. So it’s not clear to me that it makes sense to have different standards across different platforms unless it is warranted by the need of a particular application.

I suggest in the paper that it would be helpful to have performance transparency in terms of how reliable the cloud is, how secure the cloud is, data on up time, down time, recover time, archiving, and maintenance schedules. I think it would help build public trust.

When I talk with people about the cloud, I think a lot of people don’t really have a very deep understanding of what cloud computing is, and sometimes that uncertainty creates greater fear and anxiety about privacy and security and the reliability of the platform. So if we had more information on the reliability of the cloud, that would help build public trust.

I talk in the paper about developing more uniform certification processes for federal agencies, which I know the agencies now are in the process of doing, developing a joint authorization board with the power to review management services and certify particular products for use across the government that would help improve the efficiency of the process and create the economies of scale that would be useful. So these are just a few of the suggestions that I make in the paper. The paper is available outside, so if you haven't already gotten one, you can pick one up on your way out. It is also on our web site at www.brookings.edu.

Today we wanted to hear from those who are actually on the front lines of the public sector. These are the individuals who are actually working on cloud computing and seeking to move things forward in the public sector. So we have put together a distinguished set of speakers to help us understand what the government is doing.

With us today, we have Dawn Leaf, who is the senior executive for cloud computing at the National Institute for Standards and Technology, which has become a very powerful agency across a variety of technology issues because of its expertise on standard development, and Dawn will talk with us a little bit about that.

We're also delighted to welcome David McClure. Dave is the associate administrator of the Office of Citizen Services and Communications at the General Services Administration, and he'll talk with us about some of the things that GSA is doing.

And then our last speaker is Katie Ratte. Katie is an attorney in the Division of Privacy and Identity Protection at the Federal Trade Commission and has a wealth of experience and background on issues related to technology.

In terms of our format, we will ask each speaker to give his or her perspective on cloud computing in the public sector. After we hear from each of them, I will start the discussion with a few questions for them and then we will open the floor to questions and comments from you.

So we will start with Dawn Leaf of NIST.

MS. LEAF: First of all, I want to thank the Brookings Institution and Darrell for inviting me today to speak with you and for hosting the event. And I also am really -- I guess I want to make the point that, although there are a lot of advantages to electronic communications and information dissemination, there really is no replacement for a forum like this where we can have an interactive exchange. And I think to set the perspective or to present the perspective for NIST there are just a couple of points I wanted to cover prior to moving into the main agenda for today, the panel and Q&A.

First, I did not want to presume that everyone in here was intimately familiar with the NIST mission. NIST is a bureau within the Department of Commerce, and our role is to support the advancement of technology, particularly related to measurement science and standards. And there is a very complimentary and close correlation with the NIST cloud efforts and in that mission.

If you were to hear our director, Dr. Pat Gallagher speak, or the director of the Information Technology Laboratory, Cita Furlani, you would hear a very strong emphasis on the role of NIST as basically an independent, objective science organization and honest broker, we take that role very seriously, and in particular, we realize that developing and implementing a new technology requires very close collaboration with industry, with academia, with standards development organizations, with consumer organizations, federal, state and local governments, because much of the innovation occurs there, and this really frames our approach to the cloud computing efforts. I wanted to provide you with a very brief overview of the work that NIST is doing in the cloud computing space. I think many people -- most people are familiar with the publicly available NIST definition of cloud computing that was developed by Tim Grance and Peter Mell, two computer scientists at NIST, was initially released in 2008, has now been revised 15 times in its latest 2009 revision.

We produce special publications which are documents that provide recommendations and guidance to federal agencies on how to develop and implement new technologies. In particular interest at this point with respect to cloud is a very recently released special publication, 800125, that talks about security recommendations for full virtualization, basically virtualization of servers and desktops.

We are planning to release a cloud computer special publication in 2010 which will provide guidance and recommendations using the NIST cloud computing definition as a frame of reference, so the five characteristics, the service models, the deployment models.

Our special publications are informed by science and research. We currently have a project underway in the Complex Information Systems Space, which is modeling cloud computing research allocation algorithms.

And the last two points I wanted to make on our general -- over on this cloud computing efforts are that we support the Federal CIO Council, Cloud Computing Advisory Council, Security Working Group, and have worked to define the technical process to support the Fed Ramp Program, which I know Dave McClure can speak to very well in his portion of the program.

The very last subject I wanted to cover is, again, the foundation effort for NIST related to cloud computing, and that is standards, a standards acceleration to jumpstart the adoption of cloud computing project.

Sajak was very intentionally and very explicitly conceived in March of 2010 to address a specific problem, the problem being, how do you support the development and implementation of a new technology like cloud computing during that interim period? You need standards right away.

Standards are inherently constrained by the amount of time that it takes to accomplish certain things to formalize standards. It takes time to build consensus, it takes time to have innovation in a new technology, it takes time to ensure that standards are of a quality and completeness such that they will support industry and requirements in the long term and be broadly adopted. Sajak is a strategy, a process and a portal. And my very last slide, the next one, is going to speak a little bit to the process in the portal, but first I would ask you to really consider the rational of Sajak, big picture, and to think about whether or not it seems reasonable to you, and whether or not you agree with it.

NIST believes that we, the community, we, can support the more rapid adoption, safe and effective adoption of cloud computing if we reduce the uncertainty about the technology, and that one way to do that is to assess the extent to which interim or preliminary specifications which are not yet formalized standards address certain key high priority requirements, specifically interoperability, portability and security requirements, interoperability being the ability, just very general, not a formal definition, for clouds to work together, portability being the ability to move workloads from one environment to another, security being the ability to measure, assess and predict secure operations in the cloud environment.

We believe that by making that information available broadly to the community, that we can again reduce uncertainty and improve the adoption rate of cloud and improve the rate at which standards are developed. The heart of Sajak is really a process, and it is a proven process in technology. And the concept is that there are these certain key requirements -- again, interoperability, portability, security -- and that we can define, refine and interpret those requirements in use case scenarios, methodology, the interaction between computer systems and people; that we can -- an example of the use case, again, very general, might be from a consumer perspective, how do I get my data into a cloud provider environment? Then how do I get my data out?

We believe that we can define test plans, cases and procedures that we can use to assess the extent to which preliminary interface specification candidates, again, those targeted to interoperability, portability and security, meet those requirements, and that the way that we can do this is to execute those test plans and procedures against reference implementations which are cloud implementations that have incorporated the specification, and that, again, we can make the information available publicly to standards development organizations to improve the overall process. So the portal, as is defined in Sajak, will be a NIST hosted portal that will make this information available, will provide documentation of the requirements, the scenarios, documented interfaces, references to the reference implementations, and then the test results, the extent based on the task to which the interface specification satisfied the portability, interoperability, security requirements.

And you hear me use those words over and over together. There’s a lot of focus on the security aspect of cloud, but what we have found so far in just the preliminary development of the use cases is that these are very tightly integrated. You can’t say that a use case only addresses security or interoperability or portability, they really are tightly linked.

And the last point I want to make is that there is many, many relationship between these elements from our view, and again, bottom line, the final goal is to support the safe, secure, effective adoption of cloud computing during that interim period before standards are formalized, and also to aid in the development of standards. So with that, I thank you very much for your kind attention, and I'm looking forward to the rest of the program.

MR. McCLURE: So, Darrell thanks very much for having me here. And I'm happy to be here with Dawn, who we've been working very closely on the both security, as well as the interoperability and portability questions in cloud computing in the federal government, and also a pleasure to be here with Katie this morning, as well.

There's so many things that we could be talking about in the cloud computing area, I just wanted to focus on a few of them this morning and these remarks, and then, you know, turn it into -- make sure we have plenty of time for interactive Q&A.

There's no question why we in the federal government are focusing on cloud computing, lots of reasons that basically boil down to cheaper, faster, greener. We use those terms over and over again in different administrations and in different eras in computing, but that's essentially the power behind cloud computing, is that it can reduce cost, it does allow more agility and flexibility to move faster, and it certainly can provide a more sustainable greener footprint than older technology.

So we're not doing it because -- just for the heck of it or it's a cool thing to do, I think there are some specific reasons in these categories that are compelling for why in government we've got to consider cloud computing options. I wish we, you know, whoever developed the cloud concept, I wish we could almost rename it, popsicle, white box, do something, because we're now so wrapped around the abstraction of cloud computing that it's starting to lose its ability to even communicate with diverse audiences on what cloud computing is.

Dawn mentioned that NIST has done a spectacular job in its 15 revisions of cloud computing. I think getting those models, those concepts down were very important for us to understand the concept of cloud, but it remains an abstraction. We need to get down to the specifics as to what cloud computing really offers for us in the government compared to other computing approaches.

So I like to focus on these characteristics. This, to me, is the acid test, whether somebody's doing cloud computing or not. Is it service based? Is it a service based model rather than a product delivery model? Is it scalable and elastic? Is the solution scalable? Can you increase demand, decrease demand? And is it elastic in nature in terms of resources that can be put in and out of the solution set that you're focused on? Is it shared? Is it a shared resource? That's a critical element. Can we measure the use, can we meter the use of cloud computer whether it's infrastructure use, software use, in such a way that we can track cost to a metered, measured type of approach? And is it Internet- and network-based? If you look at that list, and I've kind of combined a little bit from NIST and a little bit from Gartner just so that words, you know, get it as clear as possible. This is what represents the fundamental shift in the federal environment.

We are moving to a service based computing model, and when you move to a service based computing model, you're dropping a lot of the old tenants of how we run and staff and hold accountabilities in place for our computing environment. That is what's so fundamentally different, it causes us to really I think rankle back and forth on what cloud computing is.

To me, having been in the federal community for many years, this is also not something in which there's a magical want that just simply says go do cloud computing and ye shall be successful.

It's just like any other technology strategy or approach. A lot of the responsibility for figuring out what to do in cloud computing, whether it's infrastructure, or software, or specific platforms that we're creating, the CIO of each agency needs to play a critical role in understanding the value case, the need, the business return, the mission impact from deploying cloud based solutions, and that, to me, is essential.

So if I'm a CIO, I have a portfolio strategy of investments that I'm pursuing to try to get efficiencies, better mission impact, better service delivery, more cost effective in terms of my results, that's what my CEO and my secretary of the agency is going to hold me accountable for.

So that's really I think critical to understand in the cloud space, is getting agreement on why in an agency we want to pursue different kinds of cloud computing solutions, culturally grasp within the agency that this is a fundamentally different model, it's a services model, not buying things and parking them physically and then showing the head of the agency, here's your data center, it's moving to a much more abstract service arrangement than what we're used to, and being, you know, very honest about what this can produce for you by being careful with things like cost estimates, looking at ways in which you can aggregate sourcing in a cloud environment, and focusing on not just cost ROI, returning investment from a financial perspective, but -- in terms of service delivery and efficiencies and mission impact. So I always like, you know, push back to the agencies and CIOs. You need to understand what you're going to get out of this rather than assume it's a magical solution for outdated infrastructure, poor performing applications, or just the fact that I got too many applications, this cloud thing must help me with that.

This has got to be a strategy that agencies actually have in mind. This is a quick list, and it's not encompassing of all of the risk that we encounter in cloud computing, but I think it covers a lot of the big ones that continually come up.

I mean, we're paying a lot of attention, OMB, GSA, NIST, CIO Council, to make sure that cloud is a safe and secure solution for government. If you look at that list and you look at some of the things that can be done to mitigate those risks, this is not terribly different, it's not totally different from the environment we're in now where we have outsourced a lot of our data and infrastructure and even application support to other providers. So we're not crossing a big chasm in terms of the fact that we really already do have these risks confronting us every day in the federal government now with third party providers. It's just the newness of the service in the accountability models that we really have to think through. And we've got to get serious on things like SLAs, and we've got to get serious on things like portability and interoperability. These are essential once we move into a real cloud scenario.

Let me mention two things and then I think -- these are two primary things I just wanted to add to the conversation this morning. I'm glad to see these coincide with Darrell's recommendations a bit. I believe what we focused on last, what, Dawn, the last eight months at least in NIST, OMG, GSA is trying to tackle the inefficiencies of the security solutions for cloud computing.

One of the biggest issues we face in general in security in the federal government is it's terribly inefficient how we go about doing it. Each agency does its own independent certification and accreditation and authorizations. These, on average, cost

$150,000 a pop, if not more. And we require the vendors to go through this not only numerous times, but inconsistently. So I think we have to also collect for that, and that's what we've been trying to do with this new what we term "fed ramp centralized CNA process," which we're going to apply to cloud computing first to test it out. We've worked very hard in getting agreement on what the security controls will be in a cloud environment, working closely with NIST, closely with the CIO Council working group on security, working closely with the CIO Council working group on information security and identity management, working closely with industry, and then beating ourselves up in rooms day in and day out.

So we don't claim we've got the solution yet, we think we've got something we can start with, and this is what we want to try to actually put in place. A centralized CNA authorization process will not be used on everything, it's going to be focused on cloud, it's a beta, so we'll have some things that just enter into this pipeline in a test environment, if you will, or a piloting phase, just to make sure we've got this process well defined.

Common agreement on security requirements up front between a cloud service provider and an agency, making sure all the documentation by the provider meets our stringent standards for cloud security, making sure the agency fulfills its requirements in security, because this is not all on the shoulders of the cloud service provider, and then having a joint authorization board comprised of DOD, GSA, and the sponsoring agency authorize the security package. The hope is that once that's done on a product and a service from the cloud community, vendor community that can then be leveraged completely across government.

Another agency can continue to do its own CNA, there's nothing right now that’s prohibiting or forcing this on agencies, but we feel like if we can show the credibility of the process and the stringent nature of the governance process that agencies will feel more comfortable knowing that this has been done with a lot of credibility behind it.

Even if we got into a situation where an agency decided, well, I have unique situations, I need to do additional testing or additional control work, if we cut it to just doing 10 percent more than what’s already been done, we’re already saving money and we’re being much more efficient in the overall process.

So I think there’s great hope that this works out and we can leverage this across government. And we’ll do the piloting beta phase, if you will, for several months, try to understand how we can get kinks out, and then stand this up in a more permanent fashion after that. The second area I just wanted to mention was online cloud procurements. It’s another thing that I think Darrell refers to in his study. We’ve got to figure out how to simplify cloud acquisitions.

GSA is playing a lead role in that by creating the aps.gov site. And this is a site that’s in evolution, it’s not static, it’s not fixed, it’s not what you see today is what you’re going to see three months today. It was launched last year with an aps storefront; these are cloud-based applications that can be procured very easily through a store front process.

We’ve gone back through those service offerings and actually tried to do a little bit better job of mapping the offerings under specific categories to simplify it, so we’ve done some clean up in the last few months. And we’re going to continue to work with our Federal Acquisition Service to make sure this is a simple as it can possibly be and really reflects an accurate market offering.

The second phase of aps.gov is soon to go in place, it's the infrastructure as a service offering, it's virtualization, cloud hosting, and storage. These are big ticket items I think for the federal government. This is where a lot of cloud savings traditionally takes place. So we'll add that to the store front in the coming months, and I think as a result of that, we'll see a lot more interest and usage of cloud computing by the agencies through a more simplified store front acquisition process.

I also want to point to the fact that we've created something called info.aps.gov. It is a knowledge repository of what's going on in the federal government in cloud computing. It has case studies, examples, templates, suggestions, explanations. We're trying to just create a single knowledge repository capturing things as they are occurring so that you have a single entry into government on the cloud computing concept. And I think that will also tremendously help us going forward.

The most common procurements -- common deployments that we see of cloud computing in the government right now I think I'm going to generalize, but it's largely in these areas, prototyping and proof of concept. A lot of agencies are not daring to put mission critical business in the cloud, they want to understand how the cloud computing environment works, whether it's SAS or infrastructure, why web application source serving, public facing data sites, data.gov, agency web sites where they're posting public data for consumption are in cloud environments, a very low security risk. Collaborative environments are very conducive to SAS based collaboration tools. Software development and testing is another big area, forge.mil is a good example of that, where agencies can actually stand up testing for cloud computing solutions in a safe, secure environment, not in their operational environment, and do it with tremendous cost savings because it's being leveraged across multiple entities.

So there is a lot going on. I think we're seeing, as we expected, the evolution of cloud adoption in the federal government going at a pace that's commensurate with the security, the risk, the interoperability questions, and the policy issues being effectively addressed.

Lastly, just some examples of what is actually occurring across federal agencies; on info.aps.gov, you'll find a lot of these case studies formally put up for consumption. It also gives you an idea that cost reduction is not the only advantage or benefit that agencies are getting out of cloud deployments, it's freeing up capital expenditure money, it's certainly allowing better access to information. Some agencies, including my own, that have put things in the cloud have better security than we did before because we have better views into what's actually happening. So there are a multiplicity of benefits that are accruing as we want from cloud computing solutions. And if you look at this last slide, if you can read it, it shows you the specific monetary or efficiency benefits that have been produced across a handful of agencies, both defense and civilian, all the way from ROI savings, movement of people into more high value jobs rather than monitoring infrastructure, infrastructure savings, very clear infrastructure savings, and just the ability to get the solution and be able to change solutions in a much more rapid deployment model has got tremendous business benefits for business owners and the agencies, as well.

So, you know, this is a combination of the SAS, infrastructure, and some miniscule platform offerings that are out in the market now. These are positive signs, these are tangible results that we can say cloud computing is actually helping produce some real outcomes.

So, again, thanks for having me here. I look forward to the Q&A.

MS. RATTE: Good morning. I'm delighted to be here this morning, and I'd like to thank Darrell and the Brookings Institute for putting this together. I'm sure my co-panelists would agree that we spend a lot of time in government in interagency conversations, but I just can't tell you how valuable it is to extend those conversations out to the public and hear from the private sector and the broader policy community on what they're thinking on these critical issues on emerging technology, so this is terrific.

My viewpoint here is slightly different, even from the topic that we're talking about today, which, you know, seems to be government adoption of cloud computing. The FTC actually deals with private sector and commercial uses of information, and I'm on the enforcement and policy side of things.

So I work in the Division of Privacy and Identity Protection. We've looked at the privacy and data security implications of all sorts of new technologies, and I'll talk a little bit about our general approach.

I'd also like to back up, and particularly for the benefit of the press folks in the room, give the general FTC lawyer disclaimer, which is that the views I'm expressing of those of FTC staff and not necessarily the official views of the commission or any individual commissioner. So to start with, I'd like to talk a little bit about the FTC's general approach in the area of emerging technologies. We have a very flexible legal framework. We enforce Section 5 of the FTC Act, which prohibits unfair, deceptive business practices. As more and more commerce is moving online, we have found ourselves kind of in the thick of a lot of these emerging technologies, trying to analyze what their potential impact will be on consumers.

So although cloud computing has been around in some form, you know -- for example, web-based e-mail is not new, so this has been around for a while -- it seems that now more and more of the public conversation is turning back to the cloud, you know. And the first question is why is that?

And I think one of the answers is a matter of degree. That’s just that more and more data, data of consumers is being collected, consumers are putting their data in the cloud, and it’s being stored for longer periods of time and at lower cost, so that creates slightly different questions than older models that we’ve looked at. But, you know, I think in the end, our analysis remains the same. One of the FTC’s biggest goal in this area is to preserve the ability of companies to innovate and to give some of the benefits of these new technologies to consumers. I love David’s slide showing cheaper, faster, greener, you know, that’s a great, you know, sort of summary way of talking about some of the benefits of cloud computing to consumers. And so, you know, rather than going in with a very heavy legislative or regulatory approach in this area that might impede some of the uptake and delay some benefits to consumers, the FTC really strives to take a flexible approach.

Another reason that we don’t want to legislate or regulate to a specific technology or even a specific threat is that technology is constantly evolving. You know, we could probably spend half a day just talking about what cloud computing means today as opposed to what it may have meant a week ago.

You know, I’m sure if I took a poll of the people in this room, we could come up with 50 different answers on, you know, exactly what the definition of cloud computing is. So, you know, we wouldn’t want to develop standards, even policy standards that would really quickly become outdated.

So a reasonableness approach really means that we try to scale what our expectations are of companies to the sensitivity of the information they’re collecting and storing and using, and also the risk of harm to consumers. So, for example, you know, a company that is collecting sensitive health information and then storing it remotely with a cloud provider, we would expect a very different set of safeguards compared to a company that's collecting something much less sensitive.

So we're not looking for a one size fits all approach, and again, that's consistent with our general approach in the data security area.

So there are two -- I think the FTC's definition of cloud computing is far more basic than the more technical definitions that we've been talking about earlier. Just to put it very broadly, the two major categories of use of cloud that we've been looking at are consumer uses of the cloud, so the situation where a consumer is directly placing their information with a service provider, and that would be like the web mail example, and also enterprise uses of the cloud, and that's where a company is collecting the information of its customers and then storing it with some remote provider.

And as David mentioned, the service provider issue is not new, it's not new in the private sector, it's not new in government. The FTC has always used an accountability model here, and that means that a business will remain accountable for the personal data of its customers, whether they outsource it to another company, and it doesn't matter whether that company is located within the United States or in a foreign jurisdiction.

So, you know, the real responsibility of companies doesn't shift because of the method of the service delivery, you know, it's really a matter of accountability. And, you know, we can see that with the difference of degree that cloud computing can offer. You know, we're not talking about sending backup tapes by mail to a remote service provider. You know, this is a situation where you could have a company's entire IT function outsourced.

So the degree of oversight may have to change, and some of the methodologies may have to change, but I think the analysis is still the same.

So I wanted to speak just briefly about the FTC's current privacy rethink. Last fall the FTC announced that it would hold a series of roundtables to examine the impact of emerging technologies in light of new business practices and developments in technology. So we really took a consumer focused view of how well the current privacy framework in the United States is protecting consumers in light of these developments. We had three roundtables: the first was in D.C. last December, then we had one in Berkley in January, followed by our final roundtable in March. And we had a comment period open until April 14th, and the staff is now reviewing those public comments, and we expect to come out with a report sometime this fall with some proposals on which we will seek further public comment. So this is really an ongoing process and a public process, and we look forward to any input that folks have.

So within our roundtable process, we looked at several specific business models. We really tried to take a broad view of the market, and that included things like online behavioral advertising, which we've been working on for a few years now, mobile technologies, social networking, and, of course, cloud computing.

So I thought, before we get into our Q&A session, I would just talk very briefly about some of the issues, some of the privacy issues that were raised in our cloud computing panel, and, you know, just sort of leave those open for discussion as we move into the Q&A section. So our panel really focused on enterprise uses of cloud computing as opposed to consumers interacting directly with the cloud. And one of the reasons for this is that, you know, the FTC, particularly in the data security area, has already really focused a lot on outsourcing issues, and we wanted to see if there was something new here, something in particular we need to address in our privacy model.

So some of the specific issues we talked about included, well, the first two really relate to the low cost of storage and the increased amount of data we're dealing with here, so that's data minimization. You know, we're in an environment where storage is becoming cheaper and cheaper, and as these resources are scalable, they become more available. So companies have the ability to collect more data and to store it for longer periods of time.

So given that, you know, we explored the question of whether, you know, that might lead us to ask companies to adopt things like data minimization efforts and date retention policies, to make sure that they're not storing consumer data for longer than they need to.

We also talked about the issue of bankruptcy, you know, what happens when you store your customer's data with a cloud provider and that cloud provider becomes insolvent. And that, like many other issues, you know, it seems like that's something that needs to be dealt with in contracts and service level agreements, but we thought that was an important issue to flag for consumers.

Also, transparency issues. We've heard a few references this morning to the question of what do consumers understand about where their data is located. You know, we really aren't an environment where consumers are moving seamlessly between applications on their desktop, applications in the cloud, and it may not be completely transparent to consumers exactly where their data and software is.

And that leads to the next question, which is, what do consumers need to know about that, you know, is it a situation where the consumer has to, you know, sort of seek out and negotiate their privacy settings with each different provider, or, you know, can we rely upon the company that has the relationship with the consumer to enforce some of those agreements.

There's also an issue about secondary uses. If a company is storing consumer data with a cloud provider, we think it's pretty important that the contract specify that the data only be used for specified purposes and not for any secondary uses, but, you know, again, that's something that's kind of a contracting issue.

And finally, I think one of the major consumer issues in this area relates to the location of data. We heard a reference earlier, Darrell mentioned, you know, some of the different legal rights that might attach depending on where your data is located physically.

And, you know, that's an area where we think that we as a U.S. Government agency need to continue some of our efforts to create harmonized standards with other jurisdictions to make sure that, you know, as we're moving into a more globalized environment and different standards may apply in different jurisdictions, it creates compliance issues for companies, but it also creates risk for consumers.

And, you know, one of the things that we want to make sure never happens is that, you know, a consumer would bear the risk that their data is being processed in some other jurisdiction. We think that by developing some harmonized standards, we can prevent that kind of risk, making sure that there are some minimums for transferring data around the world. And the FTC is already engaged in some of these efforts with some of our sister agencies. One of them is underway in the Asia-Pacific region. That's our APEC Cross-Border Rules Project, and that aims at developing a consistent set of voluntary rules. This is a self-regulatory effort that companies can sign up for in order to transfer their data around the APEC region.

There’s also been some work in Europe on binding corporate rules and increasing corporate accountability after data transfers and we think that holds a lot of promise, as well.

So just in sum, you know, I think I’ve probably raised more questions than answers, but, you know, it seems like a lot of the issues here are familiar ones. But, you know, the same questions that we ask with respect to a lot of other technologies I think we need to continue to explore in the cloud computing environment, and I look forward to the conversation.

Thanks very much.

MR. WEST: I want to thank all of our panelists for their insightful comments. They represented kind of different points of views and approached the subject from their different angles. But I think, you know, each of them contributed to our understanding of several of these issues. I’d like to start with a question for each panelist, and I’m going to start with Dave. I noticed the interesting change in slogan here that we see in the technology era, because I remember what the slogan used to be, “cheaper, faster, smarter.” Now it’s “cheaper, faster, greener.” I like that environmental focus, that’s good, but that’s actually not my question.

My question is, the GSA recently put out a request for proposals for e-mail migration from the desktop to the cloud, so I was just wondering, why that move? What kind of reaction have you gotten from federal employees, from vendors, and from members of Congress?

MR. McCLURE: Sure. Well, it’s still in a sensitive stage, so I have to be careful in terms of what I can actually expose in a public forum. The reason why we’re considering a cloud based solution is they're looking for economy, looking for the advantage of having a cheaper cloud based e-mail system, ability to be more agile in terms of the services that a full cloud-based e-mail system can offer. But we're expecting it to be secure; we're expecting it to meet all of our standards of interoperability, to factor into our existing technology base at GSA. So we're not assuming that it's a magical solution. We also, you know, have to evaluate what's submitted to us from e-mail providers in the cloud space and whether they can, indeed, meet these conditions that we've laid out to be FISMA compliant, to be compliant with all of the policies that we want. So it's an evolution of trying to determine what's out there on the market, what we get in, and determining whether it meets our needs or not, and we'll see what we get. We've had positive response to it.

MR. WEST: I'm curious especially about the reaction from Congress, not just about the e-mail migration, but about cloud computing in general. I know July 1st, a congressional committee held its first hearing on the cloud; you were one of the people who testified there. And I'm just curious in terms of where Congress is and members of Congress in terms of their thinking about the cloud, you know, possible benefits they see, possible risks that they worry about.

MR. McCLURE: I think the risk -- the chief risk that's brought up in any of these conversations is about security. It's understanding that we can deliver solutions in a safe and secure computing environment. I think we've all alluded to the fact that these risks are present now, but we have set up legislation and controls and procedures in place to mitigate them in a slightly different computing environment than what cloud creates. So I think that's the number one question that we always get from the Congress, is this secure, is it safe.

The second is the, as Katie brought up, is the protection of data itself just from a privacy perspective or a usage perspective, what can we do to guarantee that the data is being used for the purpose that it was intended to be used for and it's not being inadvertently shared with other organizations or sold or whatever else the condition might be.

So, again, these are not uncommon, but they're just the speed by which this could happen or the inability without having great transparency into the operation of a cloud provider makes it more difficult, so I think those are the two chief concerns that we always get questions about.

MR. WEST: Okay. Dawn, you mentioned that NIST is in the process of developing these standards, and I'm just curious, what is the timeline that you envision? I mean, you're working on interoperability, on portability, on security. When do you think we will have preliminary standards and then when will we have final standards?

MS. LEAF: Okay. I guess I have a couple of points on that. First, I should make it very clear that NIST does not explicitly develop standards, okay. We facilitate the development broadly with industry and with academia and with just the broad public stakeholders' standards. With that said, I think one paradigm that's very interesting is, there's sometimes a perception that the way standards are developed, regardless of who does it and how many participants there are, is that smart people go off in a room, they start with a list of inventory standards, they figure out which ones apply to cloud, which ones they need, and they write them to fill in the blank. Well, it doesn't really work like that, okay.

The way it actually works is that it's impossible to identify at a top level all the standards that are required. And probably if you tried to do that, you would miss the mark, because standards are only effective when they are addressing real-life problems. That’s the whole point of the scenarios in the Sajak process.

There will be maybe a top 20 percent of interoperability, portability and security problems or issues that we can address with standards and that may address a good portion of our highest priority requirements. Maybe we put 80 percent of the effort in, we address 20 percent of the areas, and we get tremendous payback for that -- we, the community. That’s one point I would make. The other point I would make is that there is not an agreement on what those highest priorities are. It very much depends on your perception, you, in the eye of the beholder, okay.

If you focus on telecommunications, you may look there. If you focus on privacy and security, you may focus there. That’s why it’s a consensus-building process, and that’s why I’m not going to be able to give you a specific timeline.

I will say this; NIST has identified a skeleton set of or a straw man set rather of 25 requirements-based operation scenarios that we believe will address a good portion of the highest priority security, interoperability and portability requirements. We are developing them. We plan to explore those and make those available in the Sajak portal. And the Sajak portal we expect to stand up in 2010.

MR. WEST: Okay, all right. So there you have it within five minutes.

MS. LEAF: Any --

MR. WEST: Well, you did say 2010, and it is almost August.

MS. LEAF: For Sajak, yes.

MR. WEST: Okay. Katie, you mentioned a number of different issues that you have been working on in terms of data retention: what happens if a company goes bankrupt, transparency, secondary uses of information and harmonization across jurisdictions. The question I have with you is a little more general. Who should be deciding these questions?

I mean, we have this -- from Congress, the Electronic Communications Privacy Act that was passed in 1986, obviously a lot of the world has changed since then in the technology area. So who should decide? Should Congress change that law, make amendments, do a fundamental rewrite? Should judges be making the law? Should the FTC be the jurisdiction that makes these decisions?

MS. RATTE: All right. Well, you started off with quite a challenging question. And I think one of the key things you've identified there is that there are a lot of different stakeholders in this space. So, for example, on an issue like the Electronic Communications Privacy Act, which really deals with government access to data, you know, that's really kind of outside of the FTC's current mandate. We really look at the private sector and commercial uses of data. You know, however, you identified at the beginning, a few remarks at the beginning that there's a real issue there with consumer expectations. You know, if a consumer is moving between data that's on their computer and data that's stored remotely in a seamless fashion, they may not realize the different legal rights attached. So as a general consumer protection matter, it does seem like, you know, some of those inconsistencies need to be addressed.

As far as the appropriate agency to do them, you know, we have to work within the jurisdiction that we already have, you know, and that seems to be slightly outside the scope of, you know, what the FTC can do.

I think where the FTC can be helpful is that, you know, we really act as -- we try to be sort of a facilitator and a policy leader in these areas and try to convene public conversations, try to get voices from the public sector, the private sector, consumer advocacy groups, academia, you know, try to understand some of the complexities of these issues, you know, and then to the extent we're able, issue guidance, issue proposals, you know, try to start conversations with Congress, you know, and see where those may lead. I'm not sure what the end point of all of these efforts will be, whether it would be something like legislation or something like principals for self-regulation, but, you know, we're still very much in the process of that conversation.

MR. WEST: Okay. Why don't we move to audience questions now? We have a microphone over here; we'll start with John here in the front row. And, by the way, if you could give your name and the organization you're with, that would be helpful, too.

MR. SEGAL: Good morning. I'm John Segal. I'm the research and policy director of the Administrative Conference of the United States. Possibly I'm the only person in the room with this question, but I am fairly technically sophisticated, so if I have this question. I wouldn't be surprised if a fair percentage of the room does, too. My question is what is cloud computing?

MS. LEAF: Well, I can certainly provide an overview of the NIST definition. There are five key -- well, let me step back. I think there is a general consensus that cloud computing is a model or a paradigm that has evolved based on prerequisite technologies that have not matured. It is not a new single silver bullet technology that has been invented recently.

With that said, the model of cloud computing, as NIST defines it, is that there are five major characteristics: consumer on demand-driven services; broad ability to access those through network mechanisms and through devices that are commonly available; the ability to share the resources, co-tenancy; the ability to monitor or meter the use of the services; and the ability to respond rapidly to elasticity and demand.

In addition to that, there are service delivery models as we characterize the cloud computing model. That would be infrastructure as a service, software as a service, and then platform as a service.

And then there are the delivery models: private cloud, public cloud, community cloud, hybrid cloud. And the only point I would add to that given the forum time constraints is that there are certain implications about those service models and delivery models that affect the tradeoff and control between the consumer and the provider.

So in an extreme case, a private cloud implementation is one where the consumer and the provider are the same entity organization. Public is the other, I won't say extreme, but the other end of the scale, where you as a consumer are accessing services that are available to the public at large, and there is a tradeoff. The same with respect to the service models, software is a service versus infrastructure is a service, implies a certain tradeoff in the provider.

So I know that that high level of explanation without providing a clear, detailed explanation of each of those terms that I used is probably not going to satisfy your question in total, but there is, in fact, a concrete set of parameters in terms that we at least at NIST use to characterize a cloud computing model.

MR. WEST: And if I can add to that, I mean, the big shift that is taking place now is really from desktop to cloud computing. Desktop computing is, you have the computer basically sitting on your desk, the file storage is on your desk, the software is on your computer, and so you're basically accessing everything locally. When you go to the Internet, like Facebook or YouTube, you're basically moving from a desktop application to a remote Internet-based application. That is cloud computing.

So as Dawn and others pointed out, it's not new, but what is new is, we're enhancing the data storage capacity. More of the software applications are moving online, and that changes the relationship between the vendor and the consumer, it changes the role of organizations, there are differing judicial rulings that apply. And so it may seem to be just a technical shift in terms of where the information is stored, but it actually has much more serious benefits, as well as ramifications, so that's the reason we've done a series of events on this.

Other questions? Jim, here on the aisle, right there.

MR. SNYDER: Jim Snyder from Isolan. I'm interested in interjection of President Obama's open government directive and cloud computing. So we hear a lot about the implications of cloud computing and the concerns relating to privacy and security. I give all you folks an A in the way you've approached those issues.

We get a little bit on data access, supportability, interoperability, that's great, less sophisticated, careful in its thinking, but one aspect of that has been, as far as I can tell, completely missing from the conversation as it relates to government uses of the cloud, not private sector where it's pervasive, and that's the issue of control and citizen access to information, overcoming the problems of FOIA, that whole model through the cloud. So to give you an example, when Microsoft sells SharePoint, which is perhaps the premier private sector cloud-type application enterprised by document sharing, one of its prime selling points is, this allows companies to keep track of the work of their employees. Instead of the documents residing on the individual desk of the employee, now it's out in the corporate cloud. So that if the employee leaves, the company has control, it can see exactly what the employee is doing.

But when it comes to government, nobody sells the cloud. Now we can bypass FOIA and take control of documents from the individual creating them, giving it to an objective third party to enhance access, because what we know is, whenever government officials have control of their key documents, and they're politically sensitive, it's very hard for the public to get access to them under FOIA, this would largely alleviate that concern.

So just to take a vivid example, the e-mail example that came up, in my county, we have a cloud for e-mail already, it's a county, about 10,000 employees, a half-million people, but they shut down the cloud after 30 days, the e-mail cloud. Now, the way that works is, it allows management to keep track of pornography, personal use of e-mail and what not, but under the Public Information Act, after 30 days, it would be accessible. So by limiting the use of the e-mail cloud for 30 days, you get the management benefits, but you don't have any citizen public accountability through the Public Information Act. It's a very sensitive point when you talk about putting e-mail to the cloud, and that is sort of a metaphor or an analogy with a whole set of issues of putting your documents in the cloud and a whole issue of taking control of public officials who judicially are not excited about making, you know, FOIA more accessible, but it's essential to the open government directive, and that's why I raise the issue.

Is there anything being done on the standards front to create a cloud where the control of information is taken away from the individual who creates the document and makes it available to a third party archives, for example, or making it Google-able under the principle that public equals online? Is that in any way part of the discussion about the cloud in the standard setting, this issue of control and taking it away from the creators and giving it to a third party to make the public's information really public accessible?

MS. LEAF: Well, I think I will start that one, and then you'll see that I defer to my colleagues. Seriously, because standards, technology, policy are not one and the same, although they are closely interrelated. So in developing or supporting the development of standards, it would not be prudent, effective or appropriate to make assumptions about the values that should be infused in the standards.

Now, if a policy decision is made, certainly it is appropriate and effective to define technology and standards to support those decisions. But in defining standards, there's not an objective to define or dictate policy decisions.

And with that, I think I would defer to my colleagues in the other areas of that question.

MR. McCLURE: So I'm trying to get into the question itself. Putting things in -- we have lots and lots of public facing data that have been put into cloud environments already; data.gov, recovery.gov are in cloud environments now. It does not mean that the agency that owns the data has relinquished control of that information, that's not happened. Still things are put through privacy assessments, data categorization schemas, whether it's sensitive, proprietary, national security, all that still underlies posting something to a public cloud or a publicly accessible cloud. So I think the open government directive is not about relinquishing control of agencies of their own information, but turning it over to a third party that then determines access and use simply not there. In fact, if anything, we've tried to make sure that those controls and decisions are being made as accurately as possible.

The power of the cloud in the open government is just the power of accessibility. It is very convenient, it's very fast, it's very cheap in terms of storage, so it offers all those tremendous advantages over storing it individually in 26, 27, 50 different data centers. I think that's -- I mean, I don't know if that answers your question or not, but I don't try to confuse the FOIA or privacy controls policy area with cloud computing.

Cloud computing is what it is. It's a utility service, that's all it is. It's a utility computing service. We're not assuming that it changes the underlying policy issues of government. Now, it creates some challenges for some of those areas, as we mentioned I think in all of our talks. How do you ensure data is actually not being misused in a cloud environment? How do you ensure that access is the way that we have defined it to be? How do we ensure that the data categorizations are not being violated once it's stored in a third party environment? So --

MR. WEST: Okay. We have another question right behind him on the aisle.

MR. HUGHES: Hi, my name is Tom Hughes. I'm with CSC. This is directed towards Dave.

Is there an acknowledgement -- and I'm just thinking for my own personal life. In the last 30 days, I received a notice from the government and then one when my credit card was shut off to tell me that someone had tampered with my credit card and disclosed personally identifiable information, so I have multiple free credit reports that have come to me from the privacy and security issues already being violated.

So at the same time, I'd acknowledge that something like a health care opportunity could be phenomenal for the nation to develop the standards to do that, Dave. So my question is is there an acknowledgement that really privacy and disclosure is -- it's only a matter of time before you have a BP-type incident where there's a flood of information that will occur and people will be very upset, companies will be liable? Do you see that occurring? Do you see us kind of like getting over that hump to develop something like a standardized health care, health-involved type solution, Dave, in government? Because we know it's going to happen. The public is going to hit back at it and, at the same time, you can see the benefit of it. What are some of your thoughts there?

MR. McCLURE: Well, you know, there's already a tremendous amount of progress been made in the health care area, putting health data up and making it publicly accessible. So CMS has done a great deal of work in this area; HHS is putting a publicly accessible health data. Key point here, we're not taking personal EHR records and floating them in cloud environments yet, I think that's the difference.

There's I think an evolution that we have to go through, and one is taking that which is already publicly accessible, but it may be in a very difficult process to get access to it, giving it transparency, and allowing that to be then used for analytics or different views of what's actually happening in the health care space.

I mean you now have a view, for example, in Medicare, and to diagnostic codes and charges, which used to be the, you know, domain of CMS and the insurance industry and whoever wanted to pay attention to it. It's out for public consumption. If you want to know what Medicare patients are being charged in your geographic area for a particular diagnostic test, you can go compare that to any hospital that's part of that public database, that's the transparency angle. I think that there's the value case being made, but we're now making a quantum leap of saying, gee, let's put out all personal health data and make it widely accessible. We can't do that, I mean it's against the law to be doing it in the first place, or HIPAA rules prevent it.

So I think the progression is what's going to help us understand as we get these controls and security aspects worked out. And we're confident that cloud environments can be used for more than just the access and the mash-up of the data that's out there, it's just not going to happen overnight, though.

MR. WEST: Katie, do you want to jump in on the secondary use of data since you referenced that generally?

MS. RATTE: Yeah, absolutely. And I think that the scenario that you pause is really a good one for thinking about the cost-benefit analysis that we'd undertake from a consumer perspective. So you can clearly see the benefits of certain types of health analytics, of centralizing health information, of increasing transparency, as Dave said, but once you're talking about the personal health information of an individual consumer, then all of a sudden the risks go sky high. Of course, that's prohibited by HIPAA, you know, depending on who the entity is.

And you might get into a situation where organizations start to see say marketing opportunities arising out of personal health conditions, and I think that's exactly the kind of secondary use that the FTC would be very concerned about, you know, some piece of information that a consumer might consider harmful if it becomes publicly -- made publicly available, something that's not currently publicly available.

So, you know, that's sort of the step that we would take in terms of the secondary use. But if you're talking about aggregate information, de-identified information, and certain types of analytics that provide beneficial information to consumers, certainly the use case is already there for that.

MR. McCLURE: I think one of the, just real quick, too, I think it's an evolving policy area. There already are some countries that are playing around with the idea of allowing citizens to voluntarily, making sure they fully understand what they're doing, to devolve their personal health information, in some cases, for the betterment of science. On the back of your driver's license, I can drop dead and donate an eye and a heart and a kidney like that, but I'm not going to give you access to any of my health care records.

So we've got this dichotomy that we've got to get worked out that we're not going to solve it overnight. There's a great deal of diversity of opinion and rights are right. But if you choose to do that for the betterment of health, you know, why not allow that? So I think we've got some things to think through.

MS. RATTE: I also just want to make a quick note before we move off of this type. You know, I made a quick reference to aggregation and de-identification of information. I just want to note that that's actually sort of a difficult evolving area, you know. We haven't solved denominization in terms of personal information, so I think it's something we have to think about moving forward, you know, how to ensure that the protection of very private consumer information is good from a technical perspective.

MR. WEST: Okay. We have a question here in the front.

MR. TALISON: Yes, thank you. Clark Talison; I'm a principal with the Mitre Corporation. And first I want to applaud the panel for recognizing the policy versus the technology; I thought that was an excellent point.

My question is, after being around mainframe virtualized services worldwide 25 years ago, many of these technology issues are not new, and cloud computing is really not that cutting edge, it's just reapplication of existing things. So the question is, do you see the delay in implementation of cloud computing as being primarily policy related issues and acceptance because of policy driven more than the technology?

MS. LEAF: I guess I can start with that one. I think I agree with your overall point, and the same one has been made, that these are technologies that have matured and evolved, okay. Obviously, virtualization in terms of virtualized operating systems existed in the ’60s and ’70s, and now we’ve evolved to virtual machines.

With that said, I think there is a distinction that the maturation of the technologies really have given us new capabilities. In a sense, it is a new model, in that we really can make services, virtualized services broadly available through the network capacity. We really can address those characteristics in the model, the elasticity, the ability of the end user to initiate their own demand, and in implementing that model, that deployment model, we are really using technologies that are new in the sense that they are -- sure, we have capabilities we didn’t have before, there is a technical aspect to it.

However, the point that you made and that I would support and agree with is that perhaps some of these questions would have been appropriate, and this is Dawn Leaf speaking, not NIST speaking, let me make it clear, could have -- and certainly we could have started to address some of them earlier in the overall technology implementation cycle. Again, I know that’s not a fully satisfactory answer, but it is the honest one I would give you to your question.

MR. WEST: Questions over here.

MS. WALKER: Hi, Molly Walker from FierceGovernmentIT. This question is for Mr. McClure. It seems that a lot of the early procurement around the cloud has been around e-mail, calendar services; in I guess a public cloud through g-mail specifically. Could you talk a little bit about the use of a private cloud, specifically a shared private cloud in agency collaboration, particularly in defense and, you know, information basically?

MR. McCLURE: Yeah, I think that’s probably the growth area in government will be what we call private clouds, or you could say government clouds, where it's really contained within the government, but it's used in a multitenant environment, either across a single department or across multiple agencies.

You can set up "cloud" environments with all the characteristics of a cloud: scalability, elasticity, metered pricing and things like that. In fact, we already have entities in the federal government doing that. NBC -- National Business Center -- has set up cloud-like computing capabilities, USDA, DOD, so it's already occurring.

So I think that's probably going to jumpstart a bit because it still is in a controlled environment as opposed to the Rackspace, Amazon, Google world of wide open public cloud. Quite honestly, there's -- only public facing data that's widely accessible is in those environments right now anyway. So once we get into mission critical systems, transactions, I think the private or hybrid environment is one where we'll see a great deal of escalation.

MR. WEST: Okay, there's a question right back there.

MR. PROCTOR: Hi, I'm Alan Proctor. I work for Formata, also former federal government CIO, actually at the FTC. As a veteran of many E-Gov initiatives over the last 20 years --- Clinton, Gore, Bush -- and I've been involved in some of the current ones, I'm struck both -- I recognize a good idea when I see one. This is obviously great. You laid out a very compelling case.

I also note that just because an application or an approach policy is better, faster, cheaper, smarter, and greener, that that doesn't necessarily ensure adoption. And I think in some ways, you know, when you look at something as smart as say data center consolidation, using what you've already got instead of buying again, in my day-to-day life with e-forms and an ROI of about three days, that doesn't ensure success.

And, you know, when you look at data center consolidation, if anything, the government is moving backward after many years of effort, trying to bring focus and attention on that. And even though many of those agencies are desperate for funds, they're still finding new ways to spend new money that's not necessary to be spent. So what I guess I'm wondering is, adoption, what are you doing? What's the government thinking these days about, you know, bringing what I would think of as kind of radical acceleration of adoption say in the next 5 or 10 years or maybe the next year or 2 years? It's really taking advantage of what you've got here that's going to be distinctly different and more successful than what's happened on a number of these other initiatives.

MR. WEST: Good question, panel.

MR. McCLURE: Thanks, Alan, I really appreciate that question, it's a good one. I think it's a combination. I think, as I tried to say in one of the slides, we don't want to be pursuing cloud-based solutions just because it's a cool technology. There has to be a business case made for cloud computing just like there would be for any software decision or major systems development.

It might be in some cases the decision is easier, but nevertheless, it needs to be put in light of risk, cost, benefit, performance, mission improvement and so forth without getting too complicated. I think that's compelling in of itself to get agencies to move to the adoption of cloud computing, because, quite honestly, in all those examples I gave you, there wasn't somebody going do it, do it. It's an agency saying, this makes sense, let's pursue the solution.

We also -- in government, you have to have many times a lever, so those levers are being applied. OMB is asking federal CIOs or federal agencies to demonstrate cost savings in the area of 10 percent from cloud computing adoption in the next fiscal year.

So while some may say that's a compliance drill or a push drill, you know, you have to pull different levers to get what you're talking about, an acceleration in the adoption of something, without pushing ridiculous things out, you're trying to do it in a cautious manner.

MR. WEST: I mean, the best accelerator may be the fact that the federal government has a $1.4 trillion budget deficit, you know. The cost savings argument is just so compelling, like everybody has to figure out ways to do more with less, and this becomes part of that answer.

MR. McCLURE: Yeah, definitely.

MR. WEST: Paul, here in the front row, we have a question.

MR. VERKUIL: Paul Verkuil, Administrative Conference. So, all right, it falls on the very important question, I'm restarting an agency, right, we're in the hands of GSA's Agency Liaison Division. Cloud computing has not been mentioned as an option. We're back to servers and we're investing in hardware. How do we get with the program?

MR. McCLURE: Well, I think it's, again, approaching it from -- administrative courts is an area where there's sensitive legal information, so, you know, there are caveats in terms of what business you're in and how fast the adoption might take place.

MR. VERKUIL: But no one has even -- it's not on the table, that's what I'm saying.

MR. McCLURE: I would ask why it's not on the table and have somebody come and make that -- have that discussion occur.

MR. VERKUIL: And he would talk to them?

MR. McCLURE: Yes, absolutely.

MR. WEST: There you go, you just speeded adoption by one possibly. Right behind you, there's a question.

MR. BROWN: Hello, Dave Brown. I'm with the National Council for International Visitors. I direct IT, and we do work with the State Department, and we're actually looking right now at a system that was based on the individual server, workstation, software aggregating information and that sort of thing. I won't go into specifics, but ultimately looking at the opportunity of using cloud computing to bring all the players and all of the different members of this process together and to enable new things.

And that's one of the things that I think people can think about as they move forward, is that the information that's normally aggregated and reported and moved upstream is all immediately available to folks within the network, so that you can have snapshots and reports on a minute-by-minute basis. And I just think that that might be helpful as far as a pitch.

And I also find what you had today that was available that I can help point people to because it's an educational process, and understanding this is a new way of doing business and actually will enable greater efficiencies, better strategic thinking possibilities based on the fact that the information is more real-time than after-the-fact reporting, so any comments on that would be helpful.

MR. McCLURE: Not really. I think it's a good point. I don't want to confuse the people. You know, the chart that we have up that points to the impact of cloud based solutions, without being overly complicated, if you're technical, you'll know that the success of any cloud based solution is still dependent upon if you're doing a software based solution, the quality of the software, and whether it's actually accomplishing the business need that you want.

How it's performing and where it's performing adds into the cost and efficiency equation, but I still want a good product. So I just don't want to confuse accessibility and efficiency of cloud with still there's got to be rigor and how the infrastructure is configured. If you're buying infrastructure space, there still has to be rigor in the development of the code behind the software that's producing the business result, and none of that goes away in this environment. That's why I don't want to confuse this concept. When Dawn was describing, or got asked the question, what is cloud computing, it's utility computing in a simple form. There are many different models of it, but it's utility, and it's like power or electricity. You move into scalable, consumable, elastic, demand-driven supply of a computing power, whether it's software or infrastructure. You still have to do the basic punt, pass and kick of IT.

MR. WEST: Okay. I think we have time just for one or two more questions. We have two questions right here, so we'll take both those questions and give our panel a chance to respond.

SPEAKER: My name is Holi. I'm a Ph.D. student at George Mason, and my research is in sustainability in cloud computing.

And my question is, what lessons can be learned from the financial sector crisis, where the too big to fail kind of -- how can we avoid this while the cloud computing is evolving and there are policies and regulations and consumer protection type of effort is being done to, first, avoid having two, three big dominant companies let's say within the cloud, and also protecting small business providers in the cloud? So what lessons can be learned?

MR. WEST: Okay. Hold onto that question and we'll take the question right next to you, as well, and then we'll answer both of them.

MS. SARIF: This is (inaudible) Sarif. I'm a senior IT consultant.

And kind of -- a lot of the clients that I work with is the portability centers in cloud computing, and from the platform point of view. Infrastructure and applications is a little bit simpler, but portability from the platform, the clients feel that they're going to be locked in. So how are you identifying portability standards so that this way you're not locked into one provider in case that provider, whether it's Amazon or Microsoft, change direction or not available?

MR. WEST: Okay. So we have two questions, a financial sector crisis and what we can learn from that, and portability and vendor lock-in.

MS. RATTE: I'll start with the first question a little bit. I think that's a really interesting analogy, and you've identified sort of the flipside of some of the pro-cloud security arguments that we've heard, you know, and that's that when you have all the information kind of under the control of a cloud provider, they may have better security protections in some cases, they may do security better than, you know, in a more distributed environment, but, at the same time, you can get into a situation where there's a single point of failure, and a single mass of data breached could result in a real loss of consumer trust in this sort of environment. So I think as these data centers become more consolidated and more and more data is stored in a smaller number of places, we have to think really hard about how to do security right and how to avoid, you know, these sort of big incidents that will effect consumer trust.

I also think another analogy to the financial crisis has to do with transparency. I mean, one of the big issues there is that consumers didn't really understand these really complex financial instruments, they didn't understand the market. And so as we're moving into a cloud environment, you know, we at the FTC are seeing a real challenge in just making consumers understand how this environment works, where their information is, where their software is, you know, how things work at a very basic level so that, you know, they can make the decisions with full knowledge of what's going on. So I think those are the two, you know, kind of lessons learned that we could move forward in this environment.

MR. WEST: Portability and vendor lock-in?

MS. LEAF: Yes, I'm actually glad you asked that. It gives me a chance to circle back a little bit to one of the points earlier.

The concept behind the standards acceleration is to jumpstart cloud computing and focusing on specifications before they are formalized and making those available really broadly and allowing a broad participative group -- industry, academia, small and large -- to propose candidate specifications, and to have an independent process that assesses the extent to which they -- real-life scenarios, like getting your data into a cloud provider and out.

The purpose of that is to drive innovation and to level the playing field, to make sure that the focus is really on the technology solutions. Now, with that said, it's natural that industry, technical sources of excellence are going to provide innovative methods to address those requirements, that's what they do, but that isn't an exclusive promise of large providers.

And one of, I think, the really important aspects of making this information broadly available is that the consumer can assess the extent to which these solutions satisfy the requirements, again, using these real-life scenarios. And this is not a short process that is accomplished in a few months, okay. On October 1, we are not going to stand up Sajak with the answers to all of these questions. It's a new technology; there's going to be trial and error. This candidate assessment is going to occur over a long time period, but the hope is that the process will provide not the only, but some of the solution to address the concerns you raised: making sure that it's open, making sure that it's level, that it's not driven by a particular stakeholder, and to make sure that we make really informed decisions.

MR. WEST: Okay. I think we will close our forum on that pro-consumer benediction. So I want to thank David, Dawn and Katie for their contributions, and thank you very much for coming out.

* * * * *

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