THE BROOKINGS INSTITUTION

THE ECONOMIC GAINS OF CLOUD COMPUTING

Washington, D.C.

Wednesday, April 7, 2010

PARTICIPANTS:

VIVEK KUNDRA, Keynote Speaker
Administrator and Federal Chief Information Officer
Office of E-Government and Information Technology
Office of Management and Budget
The White House

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

CONRAD R. CROSS
Chief Information Officer
City of Orlando, Florida

DAVID C. WYLD
Robert Maurin Professor of Management
Southeastern Louisiana University

* * * * *

P R O C E E D I N G S

MR. WEST: Good morning. I'm Darrell West, Vice President of Governance Studies at the Brookings Institution. I'd like to welcome you to our forum on the Economic Advantages of Cloud Computing. There's been a wide range of estimates about the amount of money to be saved through cloud computing.

Mark Forman, the former E-Government guru for the federal government, estimates that cloud computing will save 90 percent of the current money because of the reliance on remote file servers. He suggests that many organizations are not going to need those rows and rows of their own file servers in order to store data and launch different types of applications.

Others offer projections that are not quite that rosy. There was a report by Ted Alford and Gwen Morton of Booz Allen Hamilton, and it concluded that government agencies moving to public or private clouds can save anywhere from 50 to 67 percent.

The most pessimistic of the estimates was a report by McKenzie analyst, William Forrest, who said that there would actually be no cost savings in moving to the cloud, and that actually agencies would end up spending more. So when you look at the range of studies that are out there, you see a wide range of more optimistic versus even pessimistic estimates of what is going on.

So one of the things that we wanted to do at Brookings, given the importance of cloud computing, all the interesting innovations that are taking place at the federal and state and local levels, was to undertake a series of case studies of government agencies in terms of what their actual experiences have been.

So we did a study, the paper was released today, there's a copy available out in the lobby if you've not already picked one up, and we found cost savings between 25 and 50 percent in moving to the cloud depending on the actual migration.

In looking at the experience of various government agencies, we found there were several different variables that affect the extent of the cost savings. One is whether the agency wants to rely on a public versus a private cloud. The offer in Morton report, for example, found that the cost of cloud computing, if the agency was replacing 1,000 file servers, ranged from about 22 million for public clouds, up to 31 million for private clouds. So, clearly, the nature of the migration matters a lot in terms of how much savings there actually is. A second variable concerns the efficiency of the capacity utilization. One of the biggest sources of cost savings that several agencies reported came from being able to use their storage space much more effectively when they move to the cloud.

The problem when agencies rely on local file servers is, they always feel like they need to plan for contingencies where they're going to need a lot more space than they actually can utilize at a current period in time.

Some estimates say that government agencies relying on local file servers often average as low as 12 percent utilization, meaning they're only using 12 percent of their local file storage space. And so when they move to the cloud, if they are able to boost that utilization rate up to 40 percent or 50 percent or 60 percent because of the scalability of the cloud, that is where you can actually achieve pretty substantial cost savings, we found.

The level of security required is another factor that matters a lot. High risk security levels are expensive because of the need for secure facilities, storage in the Continental United States, and having personnel who actually pass security clearances,

so that makes a difference. And then the last factor that is a big variable is the extent of personnel savings, because when you move to the cloud, often times an agency is able to achieve real economies because they often have had a substantial IT staff to keep the hardware running, run the software applications, kind of advise people on various aspects of computing. When you move to the cloud, you're essentially outsourcing that to companies that are able to handle the data storage, the applications and some of the platform issues.

So you can actually save money, but you have to be willing to do something with those IT workers that you used to have, but may no longer need.

And in looking at government agencies, of course, it's always a challenge to actually reassign workers or even to lay off workers if you no longer need them. So the extent to which you are able to achieve cost savings depends a lot on how your agency feels about layoffs and/or staff reassignments.

So I think all those things go into the picture in terms of there being cost savings. So we feel there are going to be very substantial cost savings. The federal government is starting to make a major move into this area. I think we're going to get a very substantial savings out of that, but there are a lot of factors that will go into the exact extent to which we're able to achieve those savings.

So today we are pleased to welcome several distinguished experts on cloud computing who can help us think about some of the issues that effect the migration to the cloud, what the opportunities are, what the innovations that will be made possible, and what are the things we need to think about as we make that move.

We are very pleased to welcome Vivek Kundra. All of you know him as the Federal Chief Information Officer. He will be delivering a keynote address. He leads the office of E-Government Information Technology in the Office of Management and

Budget, and as part of that responsibility, he advises the President on technology innovation in a wide range of issues, including cloud computing.

Prior to joining the federal government, he was the Chief Information Officer for the City of Washington, D.C. He has a distinguished track record of innovation and has been instrumental in developing the federal government's strategic vision in various aspects of technology.

We're also pleased to welcome Conrad Cross. He is the Chief Information Officer for the City of Orlando, Florida. He has been the CIO in Orlando since 1999. And one of the reasons we wanted to invite him here was, as CIO, he led a switch from lotus notes to Gmail that saved 66 percent of IT costs for the City of Orlando. So he'll be talking a little bit about his experiences and his perspective in regard to cloud computing.

And our last speaker is David Wyld, who is the Robert Maurin Professor of Management at Southeastern Louisiana University. At that university, he directs the Strategic E-Commerce and E-Government Initiative. He's been involved in technology innovation at a wide variety of fronts, has written extensively on this issue.

He came to my attention last year because he wrote a report entitled Moving to the Cloud, an Introduction to Cloud Computing in Government. And I've read a lot of things, this is the single best source of information for those of you who want an overview of what the cloud is all about, what the possibilities are, what the issues are in a migration, so I would highly recommend that to you.

Our format will be, Vivek will start with a keynote address outlining his thoughts on cloud computing. He's going to have to run shortly after his talk. We hope that he'll have time to answer a couple of questions. And then following that, we will ask

our other speakers to come up and give their perspective. So I'd like to welcome Vivek Kundra to the Brookings Institution.

MR. KUNDRA: Good morning. Thank you, Darrell, for the kind introduction. And I want to thank the Brookings Institution for hosting this event. As you know, the Obama Administration is committed to changing the way Washington works, and a big part of that is making sure that we're spending taxpayer dollars wisely and intelligently.

When we think about information technology and the potential of cloud computing to lower the cost of government operations, drive innovation, and fundamentally change the way we deliver technology services across the board, we recognize that this is an amazing time in the very early days of cloud computing. We also recognize that the shift to cloud computing is not going to happen overnight. This is a decade-long journey. There are a number of issues that need to be addressed that I want to highlight. But if you look at the case for change, consider this, in the last decade; the United States government went from 432 data centers to over 1,100 data centers.

Now, when you think about these data centers, one of the most troubling aspects about the data centers is that in a lot of these cases, we're finding that server utilization is actually around seven percent, that's unacceptable when you think about all the resources that we've invested.

And the other thing we're finding is that in terms of energy consumption, that the trajectory, it's a one-way street where we continue to consume more and more energy, and these data centers tend to be energy hogs, and we need to find a fundamentally different strategy as we think about bending this curve as far as data center growth is concerned.

Now, this is a new. If you think about other sectors in the broader economy, whether it was how water is delivered across the board, consider how homes used to have a well to generate or get water, or when it came to electricity, every home used to have to generate its own electricity, but as those markets matured, what ended up happening is that we're able to essentially turn on a tap to get water, and not only get water, but we can control the rate at which we consume water and we're billed accordingly.

The same thing with electricity. As we move towards the electric grid, we're able to consume energy based on our demands, and we're also paying based on that consumption.

Why is it that, when we think about computing power and technology, that we end up over-building, that we end up using seven percent of a server's capacity, and the federal government continues to engage in this multi-million dollar contract where we're using a portion of what's available as far as the needs of the federal government itself.

But a bigger problem we see here, unfortunately, is that the CIOs across every federal agency are spending way too much time on building yet another data center, rolling out more networks, focusing on security, where they could consolidate, and what they're taking their attention off of is actually improving the lives of the American people through delivering better technology. So a perfect example is, a student aid application process, it's so complicated, and by focusing attention on making sure that the CIO at the IRS and the CIO at the Department of Education are thinking about collaborating to ensure that when students apply for student aid, that process is simpler.

Because of that focus, they're able to actually eliminate over 20 questions on this forum and make it a lot easier for people to apply online.

Think about our experience when it comes to filing taxes. Why is it that you can go online, on TurboTax or Tax Gut and have access to three years of your tax records, yet when you go to IRS.gov, you don't have access to the same level of information?

What I would submit to you is that a part of the reason is because we're focused on building data center after data center, procuring server after server, and we need to fundamentally shift our strategy on how we focus on technology across the federal government. We've already begun our shift to cloud computing. We started with a strategy on looking at cloud first policy in terms of figuring out where do we move towards cloud computing in terms of thinking about areas where we're not compromising national security in any way or the privacy of the American people. An example with TSA was that they were going to spend approximately $600,000 to stand up a blog until the CIO came in and said, well, wait a second, why do we need to spend all this money on creating a blog when all the software is available online for free.

Or with the open government directive, part of the requirement of the open government directive was to actually create a platform that would allow the American people to engage and participate in a process which allows us to figure out what we need to do to hardwire a culture of open government.

Instead of going out there and building a platform agency by agency by agency, through ops.gov, GSA was able to provide a single platform that every agency was able to use, and the CIO's weren't focused on standing up that platform, instead, what they're focused on is figuring out how do they open up the operations of their agency.

The other area that we're focused on as we move towards consolidation of data centers, is to think about why it doesn't make sense for the federal government to move to the cloud instead of just weatherfying our brook and mortar institutions. It

makes no sense if consolidation is nothing more than taking 10,000 servers and moving them from ten data centers to one data center. A part of what we're trying to do in the process of consolidating data centers is to figure out where does cloud computing make sense for the federal government.

A third area is around centralizing the process of certification for solutions. If you think about the economics of cloud computing, it doesn't really make sense if every cloud computing solution provider has to go out there and certify their solution with hundreds of agencies. What we need to figure out is an economic model that makes sense both for vendors and also an economic model that makes sense for agencies to be able to leverage the solutions in a way that allows them to ensure that the solution they're providing is secure and shifting away from a culture that focuses on generating paperwork where we're really moving towards continuous monitoring as far as security is concerned.

The State Department, for example, spent $138 million over six years on certification and accreditation, and it was nothing more than generating paperwork. The paperwork they generated was filed away in a room that was far more secure than the very systems they're supposed to protect. So what we're trying to do is, we're trying to make sure that as we move towards a centralized security model, that it also hardwires continuous monitoring so that we don't certify once and come back every three years to figure out whether their solutions are secure or not.

In an environment where we confront threats on a daily basis, we can't afford to move to a culture that's focused on compliance and paperwork.

And lastly, we need to make sure that we're establishing standards around interoperabilities, around data portability, and around security. And part of what's

happening is, as agencies are moving in this direction, the approach to standard setting is going to be very different than the traditional role.

So think about the central certification itself. As I mentioned, the eco system as far as certification is concerned creates an environment where, even with cloud computing, it really won't provide the benefits unless we're able to simplify and also move to an environment where it is actually more secure. So we've charged NIST when making sure that there's a process in place, and we've actually stood up a joint authorization board, and that board is made up of permanent members at Department of Defense, GSA, and Homeland Security, and also at an agency that's going to request a solution is going to be part of this board.

So what will happen is, this board is going to end up certifying solutions, and what NIST is going to do in conjunction with DHS, DOD, and DHS is, it's going to make sure that we've got the appropriate standards in place from a policy perspective, and these agencies are going to continuously test the solutions to make sure that they live up to the security requirements that were agreed to upon certification in the beginning.

But what this moves us away from is every vendor having to go out there and certify agency by agency, bureau by bureau, which is going to drive up the cost, and frankly, it doesn't necessarily move us to a posture that creates better security across the board.

And the benefits are going to be enormous from the federal government perspective. It's going to speed up our time for acquisitions, it's going to allow us to lower the cost of certifications. Instead of spending that $138 million on paperwork, we're actually going to be spending it on real time security instead, and that's a posture we're trying to move the entire federal government toward. And also, we're going to be able to

move to an environment where we're not continuing to build these duplicative solutions across the federal government, because what we don't want to end up with is this environment, but just in the cloud, and that's part of the reason we're moving away in terms of the shift as far as computing is concerned.

The same thing with standards; instead of sitting back and thinking about standards in the concepts of a decade long process, we've charged NIST, and the President's budget reflects an investment of $70 million in standard sitting at NIST, not just for cloud computing, but other areas, but a big focus is going to be on cloud computing.

But we're going to approach it differently when it comes to looking at cloud computing. We're going to create a model, and under NIST leadership, we're going to actually look at case studies. So looking at a number of case studies and figuring out what are those specifications, testing those specifications so we become smarter solution after solution. And on May 20th, NIST is actually convening the private sector academic institutions to help us think through the specifications, and is going to work closely with the industry in creating and enabling an environment where we can think about and begin the standards processes as far as security is concerned, as far as data portability is concerned, and interoperability.

Now, as we think about the federal government itself, we've actually already begun moving to the cloud. Health and Human Services recently announced it awarded a contract to salesforce.com as it thought about the deployment of electronic health records. And how does HHS stand up a solution in a matter of weeks to make sure that as we deploy electronic health records across the country, that we're managing it effectively?

Rather than spending a year and a half in a process where we're building out servers, going through a process that's going to take forever, they're able to leverage the cloud.

A second example, Department of Interior is in the process right now of moving over 80,000 email address to the cloud. So it's early in the phase as far as the security requirements are concerned, but that's a one way street. And as the Department of Interior moves in this direction, and I'm sure you'll hear about examples at the state and local level of the agencies that are moving in this direction, we're going to see agency after agency over the next decade move in this direction.

Third example is NASA; they are going down the route of a model where they're going to spend up to $1.5 billion in the traditional data center strategy. Now, NASA is stepping back, they halted that contract, to think about what does the next generation computing environment look like and how did they allocate that capital more intelligently in the context of cloud computing.

When we look at what's happening at the Department of Energy, they're investing $32 million in building a Magellan cloud as far as research and development in the science community is concerned.

There are agencies across the federal government that are moving in this direction. At the state and local level, we're seeing moving in this direction. And part of what we're doing is we're working closely with NIST to make sure that, in the context of this movement to the cloud that we ensure an environment where we're got a platform to think about standards and interoperability and security.

This new model, I wanted to illustrate it through an example, why this is so important and why this is not just a theoretical concept. There's a company called Animoto, and think about the old model, if you're starting up a company or if you're going

out there and provisioning services to compete in the global marketplace, the old model was, you would spend probably the first six months just standing up infrastructure, even up to a year, provisioning that infrastructure.

What Animoto did, and this is a company that essentially allows you to create your own MTV channel as you take audio and video and slide presentations and photographs and create an experience that you can share with other people all over the world, they were able to start off with essentially 50 virtual machines and said, hey, this is the business model, we'll see how it scales.

And within a period of just three days, they went from 50,000 virtual machines, because the demand was so high, to 4,000 virtual machines using the cloud. Imagine what would have happened if we were doing this in the physical world as far as standing of the servers.

We are painfully reminded of this when we looked at the cash for clunkers implementation as far as scale was concerned. We couldn't scale fast enough because of the demand. This company was able to go from 25,000 users to 250,000 users in three days without a blink when it came to their delivery of service. Now, imagine how many consumers they were able to gain. But if there's an outage, how many consumers would they have lost as a result of that outage?

Now, they only paid for what they used. They didn't go out there and provision 4,000 servers and were paying for excess capacity. That's the model we're used to today. And what we're trying to do is, shift the government, shift how we procure technology, so in a similar way in our personal lives, we pay for our electricity bill, our water bill based on usage, not necessarily based on buying excess capacity. That will help us drive down inefficiencies across the federal IT space, but more importantly, it will allow us to deliver services in a way we can't even imagine today.

As we think about the potential of cloud computing, there are a couple of things that are happening that are going to fundamentally change the way we deliver services across the board. Think about the movement of open data. We're democratizing data across the board. Today, every agency is going to be releasing their open government plan, and part of those plans are going to involve the release of new data sets across the board. Now, think about terabytes of data being unleashed and how that can drive innovation. The cheaper and more powerful processing power over the last decade, coupled with faster and more ubiquitous networks, enable innovation to happen in ways that were structurally impossible before.

When you couple that with billions of sensors that are being deployed all over the world, and you think about what does this mean to the average person, what does it mean when you think about smart meters and the ability to be able to slice and dice and cube data on a real time basis so you could make an intelligent decision when it comes to energy usage, what does this mean when it comes to help IT, that you end up owning that data and you're able to share it with your providers and people you want to get advice from on a real time basis, what does this mean in terms of shining a light into the performance of government?

Imagine an environment where we're able to look at any given agency, use the data that the government has democratized, and share the performance of that agency the same way we share YouTube videos today. We can't even imagine today the potential of cloud computing as we look forward. But the intersection of higher processing power, cheaper cost, and the ubiquitous access to broadband networks that for the first time are able to deliver content in ways that we couldn't imagine before – transformation that's going to fundamentally change the way we live our lives.

And the federal government is committed to making sure that we lower the cost of government operations, drive innovation, and leverage the economies when it comes to cloud computing. And the President is committed to making sure that we tap into the ingenuity also of the American people.

And by building these platforms across the board, what we're also able to do is create an environment where we can engage with the American people and provide services that are lower cost, help us cut waste, and actually move the government to focus on serving the American people rather than building yet another data center. So with that, I'll be happy to take any questions you have, and thank you very much for having me.

MR. WEST: Thank you very much. That was very helpful in kind of weighing out the issues the federal government faces in migrating to the cloud – how do I turn this on? Okay, that's a little better. Thank you. So thank you for laying out the issues in terms of what the federal government faces as it makes the movement to the cloud and what the opportunities are. I think one of the big things you were talking about was NIST hosting this cloud summit on May 20th and leading efforts to develop standards for security, data portability, and interoperability. So I'm just curious, how would that process work, what's the time table that you envision, do you have any preliminary thoughts on the issue of standards and what you think needs to happen?

MR. KUNDRA: Well, sure; so the first step is actually going to be NIST convening people around the table, and I'd encourage all of you to participate in this activity. And part of what we want to be able to do is test case studies. So looking at implementations, for example, as HHS, and their sales force implementation, and try to understand the issues of specifications, what standards we need in terms of data portability, interoperability and security.

For example, what does authentication look like in the cloud environment as you look at the government and this shift in the last couple of years towards smart cards? How does that interoperate with a cloud base solution? Those are some of the questions we want to address, and what we want to be able to do is, move towards an environment where we're collaboratively, in a consensus driven way, helping to create an environment for standard setting, because what we recognize is, if we don't set those standards, it's going to create an environment where we're doing nothing more than just webifying our current infrastructure, and secondly, we want to make sure that, from a security perspective, we've got the right standards in place so that agencies can continuously monitor the security posture of these solutions.

MR. WEST: And the time table that you envision for this?

MR. KUNDRA: Well, this starts on May 20th, and by August 1, we're going to be actually moving forward with initial specifications, and this is also going to launch a portal for cloud standards where we can collaborate online in a cloud environment so that we're not just limited to people who are just within the four walls of Washington that we're opening up this process to the rest of the country.

MR. WEST: Okay. We have time just for a couple questions, right there. There's a microphone coming up. If you can give your name and if you're with an organization.

MR. BALUTIS: Alan Balutis with Cisco Systems. Vivek, I think this may be the fifth or sixth time I've seen your chart on data center growth and it still doesn't fail to disturb me. I mean there wasn't a cloud first initiative during that period of time, but certainly during that decade and before there were initiatives that were called managed services, shared services, IT optimization, infrastructure lines of business. I mean there were things that were intended to bend that curve, and they clearly failed to do so.

What do you plan to do, and this administration, to really make some changes happen so three or four years from now that line doesn't show the same growth in terms of the numbers of data centers? What's going to drive a change in behavior?

MR. KUNDRA: Sure; the first thing we're doing, I've directed the CIO at the Department of Treasury and Department of Homeland Security to help lead this effort, so Richard Spiers and Mike Duffy, and the first thing we want to make sure is, we validate all the data around the number of data centers. So what you're seeing is numbers floating all over as far as how many data centers really are there. And there's a roadmap that we've created where each department is doing an exhaustive inventory of not just the number of data centers, but also processor utilization.

Once we've got that data, what we're planning on doing is taking the data, and each agency is going to create their consolidation/cloud for strategy to allow us to make sure that, from a budgeting perspective, as we think about the fiscal year 2012 budget, that we make decisions that are going to inform that process so that we don't continue on that path.

And part of it is to figure out, you know, what is the utilization pattern across the entire government, and then how do we think about this in the context of energy utilization also.

So with those plans, and also the budgeting process in FY 2012, and commitment from agencies to rethink their strategy, like NASA, so that will be the first step, where you're already seeing movement, but they've backed away from a traditional old school approach to really thinking about what does this new world look like. Now, this is not going to happen overnight, as I've said, we didn't get to 1,100 plus data centers in one day, and we're not going to bend that curve in one day either.

MR. WEST: Okay. I think Vivek has time just for one more question and then he has to leave. We have a question in the front row here.

MR. BURTON: Hi, Vivek, Dan Burton with salesforce.com. And I'm delighted to see your continued push on cloud computing. Turning a battleship is never easy. And do you have any internal metrics just about two, three, five years out, you would like to see five percent of the federal IT budget on cloud applications or ten percent? Are there any internal metrics like that you're thinking about?

MR. KUNDRA: Well, a lot of that work is actually grounded on the data that we get as far as what's going on across the federal government. So this process as far as the federal data center initiative is vital to our migration to the cloud also, because what that information is going to do is, it's going to give us a real picture of what our utilization patterns are. And also, when we think about modernizations, a lot of the IT initiatives that are being initiated, part of what we're doing is, we're going back and saying, well, if this is not vital when it comes to national security or in no way has a huge impact on privacy of the American people, why aren't we considering these options? And you're going to see more and more solutions, but at the end of this process, which is going to be towards the end of October of this year, we're going to come out with very specific metrics around what we want to move toward and what that path looks like.

And any of the activities that NIST is engaged in, and that's why I want to encourage as many people as possible to be actively – to actively participate as NIST convince people on May 20th that is going to be vital to our strategy as we think about what are some of the barriers.

Security is clearly the biggest barrier. Data portability is another barrier, because we don't want to lock the federal government to one vendor, and if we want to switch to another vendor, that we're locked into a proprietary system. And third is going

to be interoperability. We want to make sure that in the same way, you know, personalize, we can go anywhere in the country and have access to whether it's water or whether it's electricity in a consistent form, that we don't go out there and create an environment where everything is proprietary and the government ends up spending billions of dollars trying to integrate these various systems.

MR. WEST: Okay. Vivek has to take off, but we're all looking forward to May 20th and seeing the start of this process. And we want to thank you very much for all of your leadership on this issue.

MR. KUNDRA: Great; thank you very much for having me.

MR. WEST: Okay. The next stage of our event will be an expert panel. As I mentioned earlier, we have invited two leading authorities on the issue of cloud computing to share their perspective with us in a minute. We will hear from Conrad Cross, the CIO of the City of Orlando, who will talk about his experiences and his perspective; and then we'll also hear from David Wyld of Southeastern Louisiana University.

So I think I'd like to start with Conrad. And if you can just give us your thoughts on cloud computing, what your experience has been, and what you think the possibilities are.

MR. CROSS: Ten years ago when I became CIO of the City of Orlando, I prided myself I think on being grounded. Ten years later, I think I'm still grounded, but my head is in the clouds. And I say that because my experience has been one that has been a forced experience. Now, I have been following cloud technology for quite a while, I could say maybe two years, but from a theoretical level, but it was when our budgets got sliced significantly just last year, a 12 percent cut, and I lost a substantial amount of my

staff, that it really forced me into looking at the cloud as something that would make a difference.

We did that by moving our email system to the cloud and were able to realize at least a six percent savings. Now, it wasn't an easy process, it was a process wherein we had to, first of all, figure out if that was viable, because there are inherent dangers in going into the cloud, like we were told by a different department.

Being a city government, of course, once of the first things that came to mind was security. The police department wanted to know was their data safe. Now, in the cuts, my organization, my data processing, or IT organization, I'm sorry, I dated myself with data processing here, we have three security officers, and we have well over 200 applications that we provide for our city government. One of my security officers got cut. So when we started talking about moving our email to the cloud, it was kind of interesting because with two security officers, I was still supposed to be providing security for all my apps, as well as making sure that my email, which was going out to the cloud, was secure. And then the thought occurred to me, my email is going to an organization, and we did Google apps, who has way more security potential or way more security assets than I have, more people who do this every day for a living, in other words, they have data sent and they have people who monitor 7/24.

In my organization, we are a 7/24 operation because we support public safety, but I don't have a security officer on guard 7/24. So when we started looking at the reality, there is an organization out there, several organizations, many organizations out there who could do security better than we could. So it was a kind of innocent argument when we started looking at it.

And this is a macro view, because, of course, when we get down to the fine points, it may not be as simple as saying, okay, I give my security to Google and they

take care of my mail, I'm safe, but it was a reality check. They could do email security better than I could. So that wasn't an argument not to go to the cloud. And so we put that to our organization, and we sat down, we thought about it long and hard, we asked questions of our provider, Google, and they gave us answers, and were good answers to us. That was one area.

Storage, another area that we considered. And I'm kind of giving you the process which we made our decision on. My users were always complaining, I need more storage. I go to the budget people, and we thought we bought more storage a few months ago, why are you coming back to us.

The reality is we gave on average our users 100 megs and they had to clean up their mailbox. That wasn't acceptable. What was happening is that they had private mailbox on the outside, and in an effort not to lose their mail, they were sending their mail to their outside mailbox, and we started seeing some trends towards that.

Now, the solution that we bought when we went to Google apps, we got 25 gigs per person. Isn't that an overriding reason not to go cloud? So these were some of the things and just some of the few things that we considered. Personal, I lost one and a half administrator in my mail prior to going to the cloud. And there were things like back-ups and updates and so on that were not my headache, again. And I report to the CFO of the organization, and it was interesting to see her take on it. Her bottom line was, I'm spending less, they're having the headaches, and you're thinking twice about this move.

MR. WEST: Sounds like a good deal to me.

MR. CROSS: And so it – in us, and we made our move, and we haven't looked back since. Now, one of the things that has come into vogue within the organization ever since we did that is that whatever application we undertake or we think

about replacing new application, one of the first questions that we ask, is this a cloud or did our cloud provide an ap.

And if the answer is no, we still pursue the conversation, we still want to know what you're all about, but we think our future is in the cloud, and primarily because in local governments, you get to spend once every so often, whether it's once every four years, once every ten years, once every 20 years. We have apps, ERP apps or HR apps that's 20 years old.

Now, if I should replace that app and it's not a future technology that I'm going into like cloud technology, then I really have lost an opportunity. Now, I could go on, I know David has the chance – and I guess it will come back over to me, so I'll turn it over to David.

MR. WEST: Okay. David, we've been hearing several stunning scenarios here in terms of possible cost savings, opportunity to innovate scalability and so on. I mean you're an academic expert, you've written extensively on this, you know the opportunities, but are there risks here, as well, are there things that we should worry about, especially in the public sector as agencies are thinking about doing this migration?

MR. WYLD: Okay. Well, I want to first thank Brookings and Darrell for the invite and making it possible for me to be here and join you today. And I do want to borrow your video of the event so I can play the one minute endorsement of the cloud report. And the best news is this is free and downloadable from the web site with IBM.

The risk of all this is inherent to the lack of control, or the feeling that if I have my servers, if I have my control over the data on site, that that's better and more secure than using an outside provider and the data being somewhere in the cloud.

And I think one of the things that the cloud vendors and integrators have to overcome is, every time you can't access your Gmail for an hour or two and it makes

tremendous headlines when there is an outage that becomes an issue that becomes a reliability and a security concern. Government at all levels has unique considerations, at the U.S. federal, and certainly at the city and state and local level, we have concerns about the data residing within the U.S. borders and not being at a cloud center somewhere around the world, and so that differentiates the public sector from private sector use of the cloud.

But when you look at the potential downsides of security, reliability, the fear of not just data security from a hacking standpoint, but physical security, as Conrad pointed out, you know, his data centers are not guarded – data center.

MR. CROSS: Center.

MR. WYLD: Center, okay, are not guarded physically 24/7, whereas, you know, Google and other providers go to great lengths to demonstrate physical security, not just data network security, but, you know, guards and boats and all kinds of – alligators, I believe, you know, to guard the data.

So in some ways we have to get over that mindset that if we have internal control, that it's going to be better and more secure than using an expert outside provider who this is their business, this is their reputation on the line 24/7 to provide government with better, faster, and in many cases, cheaper security and data access than what we can do internally.

MR. WEST: If I could ask one question of each of you and then we'll open the floor to questions from the audience. The liability issue, I mean let's say there's a data breach or a hacker or something gets compromised, what are the liability issues now associated with cloud computing? Either one of you.

MR. CROSS: In my case, it depends where that breach is. We are the sunshine state, in other words, sunshine state literally.

MR. WEST: You are the sunshine state.

MR. CROSS: We are the sunshine state. But we operate in the sunshine, and so just about everything at some point in time is available for public consumption. I mean I guess it depends on when it's released. And I did mention that because we're a city government, we have certain things in the police department that hold there, rape information maybe something that you'd secure and so on. If there is a case where something was transmitted or something was – regarding the case and it got exposed, there could be potential loss – so on and so forth. So it definitely depends on what the nature of the breach is, and that would determine what the consequence was. But –

MR. WEST: Whose level, the city, the vendor?

MR. CROSS: In the case, it could be ultimately the city. I guess we would try to figure out – maybe the vendor would cushion a part of that, but ultimately, it would be the city.

MR. WYLD: I might add that one of the choices that you have to make strategically from a CIO perspective, from an IT perspective, is data that is viable to be shifted to an outside cloud provider versus data that has to be internally housed and protected.

And so the liability question that is really joint liability between the governmental entity and the cloud provider, and then if there is a third party contractor, that certainly is brought into force, as well.

But you have to, first off, make decisions about what data can we shift to the cloud, what data has to be housed internally, or if we're going to shift to using the cloud, it's not just a generic shift to a cloud; it's what kind of cloud. Are we going to have

a private cloud environment that is strictly managed for us or are we going to open this up to a public cloud, which in government's case, is going to be less common.

MR. CROSS: Let me just follow for that, because the way we operate right now, the way we operated prior to going to the cloud is that we transmitted stuff through ether all the time, which could have been hijacked in a similar manner. It resides in the cloud, going through the cloud, could have been hijacked. And the caution or the precaution that we give to our law enforcement agencies, particular if this is so confidential and so protected, that maybe you should think about an alternate way of transported from A to B as opposed to sending it truly ether or having it reside in the cloud.

So this is one of the discussions we had with our internal police department, especially our security organization, that maybe encryption, and if encryption isn't good enough, put it in the car, drive it up to Tallahassee or wherever it needs to go. If you don't think it needs to be there, don't put it there. And the same thing would have applied before going to the cloud, all the precautions are there.

MR. WEST: Okay. Why don't we open the floor to questions and comments from the audience? So we have a question over here?

MR. DOROBEK: (off mic) Chris Dorobek, Federal News Radio. One of the challenges is giving –

MR. WEST: Hey, how you doing, Chris?

MR. DOROBEK: (off mic) one of the real challenges is, you have real impetus because you didn't have money, so you had to go this direction, but in federal agencies where that is not always the case – won't talk quite so loud.

In federal agencies where agencies really want their server, often in closet some place, and the CIO doesn't really have authority to drive folks to a unified enterprise

approach, I'm wondering if you've seen how folks deal with that issue across government agencies.

MR. CROSS: I can't speak for the federal agency, we're a local government, but some of those kinds of situations does exist within our local government. And I think, like you captioned or you cautioned, my case was a financial situation, and the CFO will not allow, if we can make the case, that this is not cost effective the way they're doing it, we're better served by going to the cloud, that's quashed right there. I'll defer to David, and he may have knowledge of the federal space.

MR. WYLD: Well, I think in the federal space, it's a real shift from, as Kundra said, that you're shifting away from adding capacity that is in federally funded sponsored controlled data centers to using cloud services, and if that message is being translated from a budget standpoint, then certainly you have to work within those constraints.

At the state and local level, with IT, we're certainly getting that message, and we are shifting toward a cloud first strategy, yes, because of the technology, but it is a convergence of the technology, the budget issues, and also the demand for ubiquitous anywhere, anytime, any device access to computing power. And so we're seeing a tremendous shift, and yes, it's being driven by budgets, but there's other factors at play.

MR. WEST: Okay. Other questions? Back there is a question.

SPEAKER: David, following up on what you just said, then could you – and you talk about this in your excellent paper a little bit, but you talk a little bit more about where you see some of the different entities in terms of who's on the forefront or not. Obviously, small and medium sized businesses, every new one created now goes immediately to the cloud, so they're ahead of everyone else, but then when you look at

large private companies, and then there's federal agencies, state and local governments, how do you see them kind of matching up in terms of the trajectory?

And then the other thing you mentioned in your paper which I'm interested in after just spending a couple of weeks in Africa, is, what do you see from a developing country standpoint, do you see them leapfrogging a lot and do you see them providing, you know, Africa, places in Asia, you know, tremendous opportunities, are the cloud providers going over there?

MR. WYLD: Okay. Darrell, do I have about 30 minutes? Okay.

MR. WEST: As long as you can hold the audience.

MR. WYLD: As long as I can hold the audience. I'm just impressed so many didn't leave after Kundra left. I think the – there's some common themes here. When Kundra focused on the Animoto example of how a company can scale up so quickly without having internal IT resources, and we see that again and again demonstrated by the private sector, we see in China examples of cities and regions specifically focusing on developing cloud computing resources for small or medium sized enterprises so that a start-up company is not focused on having to build up IT capabilities, IT staff, IT infrastructure, but can worry about their business model and grow from there.

And so if we look across government around the world, and there are some very good examples, and I touch on those in the paper and have followed up with specific case studies dealing with what's going on in Japan, what's going on in the United Kingdom which have uniform across their national government drives and initiatives that rival our own in terms of the focus on cloud first strategies, what's going on in Thailand and in New Zealand and across other developed nations to where there is a focus on cloud resources.

What I think is interesting is, as you mentioned, in the developing world, to where we could see this take much the same trajectory as say in telephone, in internet connections, to where you almost leapfrog from maybe not having a wired infrastructure in place to moving – skipping that phase entirely and moving to a wireless access structure. And so you have the ability of government, nationally, on the province level and on the local levels to be able to increase their capabilities rapidly and scale up, much the same as done in the private sector, but being able to leverage those cloud resources, pay only for what they need, and quickly and continuously upgrade their technology.

And I know in our pre-show conversation, Conrad expressed, you know, I have one shot to buy technology, and with the current budget situation, that may be our last shot ever at buying technology on the state and local level, but what's interesting is, as cloud develops and iterates and goes through generations, and as we see what will develop, you know, might change rapidly every six or 12 months, my investment in technology, in hardware, is not going to go out of date as quickly as Microsoft used to make it go out of date, because as long as I have a web browser, as long as I have web capability, I'm going to be able to use the latest and greatest cloud technologies because it's all going to be delivered on a web platform or on my mobile platform or on my iPad. And so, you know, we're not going to see that sunk cost and lost cost that frustrates many from an IT budgetary perspective, and that is a real powerful message for government around the world.

MR. WEST: Okay. Here we have a question.

MS. KENNEDY: Hi, Jeannette Kennedy from Nokia. So, obviously, because you come from – both of you come from the budgetary point of view and you're looking at reducing cost, have you noticed or has there been a parallel discussion of how call computing or managed services, what have you, will transform the way you work,

have you looked at telecommuting or having people alter schedules, and is this something that is maybe not primarily in the discussion, but as also, you know, maybe budgetary over the long term, how could this transform the way people become more productive?

MR. CROSS: I'll take a first go at that because we are in our infancy in terms of our entering into the cloud, but we already start seeing more people. It's changing the devices that people – people are always on the go, people are mobile, and one of the – I had one commissioner who, one of the first concern was, now, can I use my non-supported city device to get to it, well, commissioner, you could before, but we didn't allow that, but that's in – in the cloud means I should be able to get to it everywhere, everybody can look up and see the cloud.

So we have more and more people saying, well, can I work from home, yes, you could before. There is an expectation because it's up there somewhere, that – everybody can see it and get to it, whereas before it was in your data center, you could have gotten to it before, but the expectation now has increased.

So we now see more and more people asking for more mobility, the ability to work from home and things that you eluded to more. I guess with time we will see, as we put more applications on the cloud that things like telecommuting and so on will be – it's just a matter of the organization trying to keep up with the challenges or the gains that technology has given us.

MR. WYLD: Let me follow up. The changes – it does change the way we work, not just the location of where we work, and not being tied to our PC at work, it doesn't tie us to our laptop, it ties us to whatever device we can access, and so that does promote remarkable levels of change in terms of our ability to work remotely.

It also changes the budgetary picture in terms of – and I'm speaking from the college and university standpoint, that our university and hundreds of other universities have migrated to Google apps and hosted email, because not only does that increase the capacity, and as you said, here's the proposition, unlimited capacity versus your hosting it internally, it really does change the way we work, it changes also the nature of IT work, and I think a lot of this coming – having done federal IT work for a number of years, you know, we're always concerned with the nature of the federal IT workforce, and that's true at the state and local level, as well.

This changes IT work from – there's going to be less need for the technical support, the hands in boxes type of IT work to more value added IT work, to more training, more developmental work.

And so it's very interesting in terms of how this not only will change probably – and that's why, you know, one of the things that Darrell focused on was the controversy that occurred in Los Angeles as their city changed to hosted services.

But what's going to be interesting is that the nature of IT work will change, and with that, it will be a more highly desirable, less back room, with computers spread all over the place, to working with individuals and working with vendors and managing the vendor interface. And so it's really going to change, not just the user perspective is interesting because from that – from a user perspective, I just want to know what's going to be on my screen. How it gets there is a mystery, it's a cloud. But from the IT perspective, from a management perspective, and also a hands on perspective, it really does change the game.

MR. WEST: And I think it also helps government in terms of weather related issues. I mean, you know, having just gone through a winter where Washington got 60 inches of snow, and there was one week where the city was paralyzed, you know,

the opportunities of cloud computing to promote telework went up enormously, and that's another potential cost savings for agencies.

MR. WYLD: As long as a tree is not across the utility line.

MR. WEST: Yes, there are limits on that. Near the back, there's a hand up.

MR. HASSINE: Hello, I'm – Hassine with Government Computer News. I can see applications like email services seems to be a low hanging fruit, you know, moving those types of applications to the cloud. Are there applications at this point that are not ready or not suited for the cloud? Because when I talk to people, I hear about, you know, legacy systems, for instance, mission critical legacy systems are much harder, a much more complex type of, you know, maneuver, maneuver those to the cloud, it's just a lot more complex. So are there applications right now that are better suited for the cloud?

MR. WYLD: That are better suited or not suited?

MR. HUSSINE: Either way, because – or not suited, because – well, for instance, moving data base applications, you know, it just seems to me those are much more complex types of, you know, applications to move to the cloud.

MR. CROSS: Speaking for my organization, I'd say no. I think just about – you can find a vendor out there who can provide – and this goes to – we may have legacy applications, but we may need to get rid of the legacy application and start looking forward. And public safety, I like beating up on them because that's what we're all about, first and foremost as a city, we need to protect our citizens, and the conversation got to where, first of all, I saw Steve Bama speaking to a group of CIO's a few weeks ago when he said public safety acts are ready for the cloud, and we started pondering that statement, and we started thinking that there is a company right now On

Star that could pretty much tell you if you have a problem, wherever you are, how to get a resolution to that problem, and we started – if On Star can do that, if we have got satellites up there, maybe there is a company out there who could dispatch our police locally.

It's a communication call. Right now the data bases that we have, when we have an incident, we have a police officer and place a call – citizens place a call to 911 or wherever, and it goes somewhere, and then somebody looking at something determines, okay, my nearest office is here, why couldn't that be done from a satellite up there and so on.

And I would think that would be one of my most, not necessarily complex in terms of hard to do, but one of the most challenging. And where we started thinking through, we sat around, we were having this discussion, our dispatch for local police officers could very well be done by a remote company somewhere with the ability to look using satellite technology or something, or GPS technology and all that put into the mix.

So to go back to your question, we may have legacy applications within the organization that are not cloud ready, but that doesn't mean that there aren't applications out there that we could buy into or buy that are ready and could replace the legacy applications that we had.

So if there are data bases that need to be converted over to the new apps and all of that stuff that goes on, we may need to do that, but I don't know if I can see any one application today within my city government that would not be able to go to the cloud. I may be overly optimistic, but that's just the way I see it.

MR. WYLD: I would say at the – the federal level, of course, the hardest area is going to be in the defense and security areas, and I think those are a different animal than the rest of the federal sector.

If you're talking about legacy data bases, legacy systems, I think the question becomes the value of transferring those to the cloud over, you know, are they going to be used that widely. I think the push for openness and transparency, and citizen access, user creativity is going to push a lot of that onto the cloud even if it comes at a significant cost for data migration. I think the really ultimate test is going to be electronic medical records, because it is the ultimate value add of this and also the ultimate information security nightmare scenario. And being able to come up with protocols and access, because basically this inevitably will be a cloud based system in order for authorized users to be able to access to it, but think of the improvement.

I mean there's going to be billions and billions of dollars spent at the federal level, at the state and local levels in terms of electronic medical records, and what's going to be the value is, you talk about legacy systems, we all have a legacy paper trail sitting in a series of manila folders in various offices around our area, around the country, and being able to combine those and take the paperwork aspect out of this, and again, transform what was a data cumbersome system into a fast access system, but it's going to have to go through specific protocol, specific verifications in order to gain access.

And again, the fear would be that a data breach that's well publicized is going to really shake confidence in these systems, but we're going to have to build in the security up front and make wise decisions on the protocols and information security angles so that when this comes into wide spread practice, that we'll gain buy in from all constituencies in electronic medical records.

MR. WEST: Back there in the –

MR. PEARSON: Thank you. I'm Steve Pearson, Director of Science Policy for the American Statistical Association. And I think this goes to Professor Wyld.

In terms of the federal statistical agencies, I'm wondering what you've been hearing in terms of how they fit into this, where the situation, you know, as you know, the departments – there are dozens of statistical agencies, and there's a national academist report called Principals of Practice, Practices for a Federal Statistical Agency, where one of the principles is making sure the agency had the autonomy over its IT resources, and the issue, and we've been hearing security, but the issue is also perception of making sure that their data is, you know, any data provided is confidential so that they can ensure that they have a high response rate to their surveys.

So how does ensuring the perception of confidentiality make sure there's a firewall between where the status is stored, how does that fit into the discussions of cloud computing?

MR. WYLD: Well, I think it's ultimately a matter of confidence. And, you know, I think it's incumbent that it's both an IT policy decision and a public relations matter, as well. And so you have to instill that confidence. If you're talking about survey respondence, if you're talking about researchers to be able to feel comfortable with those data bases being secure, that's going to be a tremendous challenge.

At the same time, the open access nature of all this is at one point making the matter more complex, because you're going to have, you know, accessibility issues combined with security issues, and so it's going to be very interesting to see how those agencies go about managing that risk.

MR. WEST: I would agree with that, because I think one of the issues particularly for sensitive federal data and statistical information of the sort that you're talking about is, I know that currently with sensitive federal data, you have to have a secured facility. Like at a university, you often have a specific room that's locked, you know, it's not a public access computer, in order to access that type of information. And

so I think what your question implies is the federal government is going to have to think about its own definition of security and privacy for the cloud. And it's going to be a two-step process of, one, securing the security of the cloud, and then secondly, persuading the people that's data base that is in the cloud is as secure as a data base that is on a local data center.

I think we're kind of not at that point yet in terms of public perceptions in the scholarly community about data bases, but that's the process we're going to have to go through in order to address the question that you raised. Do you have a question?

MS. NESS: Susan Ness; it sounded as though the federal government was going to be applying border bumpers to the cloud to keep it over the United States, so to speak. My question is, so often the regulatory and judicial ramifications bumble along long after technology has been implemented. I was wondering if you could comment on any of the policy or legal ramifications of cloud computing, particularly cross border cloud computing.

MR. WEST: I think that's one of the biggest challenges of cloud computing right now. In my paper, I use the metaphor of a tower of babble emerging in the area of cloud computing, because what's happening internationally is, each country is worried about cloud computing and essentially starting to impose differing standards on what cloud computing means in their particular area. And so you could easily end up in a situation where there are five, ten, 100 or more differing standards based on national sovereignty, and so that, obviously, undermines the principle of the cloud, it undermines possible cost savings associated with it, and so legally that whole area is very much up in the air.

Some people have suggested, you know, just as we had a treaty of the sea and we have various other international treaties, that we need an international treaty

of the cloud that would essentially work out some of these international legal issues, ensure that countries have at least some common sense of what the standards should be so that you don't have, you know, one cloud for Switzerland and then another for Germany and the United States.

MR. WYLD: Just to follow up on what Darrell said, I think, from a U.S. perspective, storing governmental data abroad is going to be an onstoger and should be, and so I think that works in a number of ways to benefit us economically. And I think what you will see is, and we're already seeing it with Google, in that, you know, the competition for locating data centers is going to be intense, much as we had ten years ago locating the next auto plant.

I think we're going to see areas of the country really develop as has happened in Washington and Oregon already. If you have access to cheap electricity, you could have access to cheap water; you're going to be a leader in terms of providing this storage capacity.

And as more and more government IT is shipped to the cloud, unlike private sector companies, governmental use of the cloud is going to be generally country specific, and so we're going to see that.

I thought Darrell did a very good job in his paper of highlighting the legal issues. And we deal with the cloud as a metaphor anyway, because in programming terms, it's just trying to explain something you can't explain.

And so the tower of babble is a reference we've used repeatedly in computing, but it's true, and I think as we work across borders, I think it's going to be very important to have standardization of legal requirements so that there is not this splintering of the cloud marketplace. Even though the data may need to reside in a country specific

location, at least the standards will make it easier for not just providers, but also buyers of cloud services to work together on this.

MR. CROSS: I was just going to say, prime real estate for good data center, Orlando.

MR. WEST: Orlando.

MR. CROSS: A lot of cheap energy, sunshine, and a lot of water, not very far in the ocean.

MR. WEST: And there's some good places to visit and play golf after you –

MR. CROSS: Well, and there be the occasional hurricane.

MR. WEST: Okay.

MR. BURTON: Dan Burton from salesforce. There's a fundamental contradiction in the government debate about cloud computing that you don't see in the private sector, and I'd really appreciate your comments on it. And one of the big advantages of cloud computing is, there's no IT infrastructure, you know, your experience, you don't have to build a data center, you don't have to maintain it, operate it, update the applications or the data bases or the mainframe computers, you just pay a monthly fee and it all works for you. And if you look at the way the private sector is embracing the cloud, you know, when companies like Cisco, and Dell, and Symantec decide to put their sales and marketing on the cloud, they don't go out and build a data center, they use commercially cloud secular systems to do that.

And yet when the government talks about cloud computing, whether it's U.S. government agencies, we heard some of that today, or foreign governments, often the first reaction is, I love cloud computing, it's cheaper, faster, better, I'm going to go build a data, you know, a cloud data center.

So digital Britain says I'm going to build a 500 million pound G cloud, and Japan talks about the Kasumigaseki cloud, and yet that sort of misses the benefit. Now, granted, there are security concerns, everybody talks about cross border daniflows but I'll just give you, again, the experience of salesforce. We have government agencies in Japan, New Zealand, Australia, UK, Germany, France, Canada, Denmark; I mean you name it, all these government agencies are running government applications on commercial clouds. So I'd really be interested in just commentary about that contradiction in a focus on IT infrastructure which governments seem to really be hypnotized with, and the private sector is like, hey, I don't have to do this, that's the reason I'm going to the cloud.

MR. WEST: I would say it's getting – I mean there's a mindset issue and then there's a regulatory issue, and the mindset issue I think is being overcome rather rapidly, because those in government IT, and Conrad can speak to this, you know, recognize that the private sector is perhaps a better provider from a security, from the reliability, from a cost standpoint than government can ever be, and yet we're having to overcome the mindset of -- the engineering mentality of IT that I control more boxes, more capacity, more people, and the natural tendency is to grow.

That is being constrained now by certainly budgetary forces, and so perhaps that's why the technology is coming on at a very opportune time. I think from a regulatory standpoint, the IT providers need to be very aggressive with regulators and with policy-makers in terms of convincing them that their security, their reliability is as good, if not better, and in many cases far better than what has existed previously. And so it is a matter of informing the debate and overcoming some of the natural hesitancy toward using an outside provider with various forms of data, and certainly more secure data.

You mentioned, and I deal extensively with the digital Britain project and the Japan, and I'll go with your pronunciation on the Japanese project, but it is that – overcoming the thought that, okay, I'm bought in, I'm sold on cloud computing, but I'm going to sit at my own cloud rather than allowing the outside provider to do it and contract for those services.

And I think that's going to be a central obstacle to overcome, because there's – the feeling is in government that I have to control the resources, and if you can shift that to a contracted model, then that's going to really advance government IT in ways that we can't see.

And I appreciate Mr. Kundra's perception that, you know, this is going to produce unintended consequences, very positive, perhaps some negative, but over the next five or ten years as we see this evolve.

MR. CROSS: I think he sums it up best, just real quickly, budgetary mindset regulator. We see when the money says this makes sense, that's what we do, and I think any government today – and I go back to the point of security, if the Chinese hacked the City of Orlando, we would throw our hands up in the air and say, I'm sorry, I'm busted, because I have no Chinese developers in-house who could help me track, so I may end up going back to a private firm and say help me with this, or it could very – it could be one or – law enforcement agencies with that expertise, but I doubt very much that we would find that kind of expertise there.

So it could very well be that we would engage a Google ultimately or some other company with that international flavor to help with that kind of stuff. So when the debate starts and when the debate ends, we may find that we just did it this way because we were used to doing it this way, so we build data centers because that's the way we used to do it. But the more we look at the reasons why it's a different world, and

the finances say you may be best served by just going this way, go to salesforce.com or whoever it is at outset, then that may be the thing to do. I think we're being driven.

MR. WEST: Okay. Unfortunately, we are out of time, but I want to thank Conrad Cross and David Wyld for joining us and sharing your thoughts on cloud computing. And thank you all 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