THE BROOKINGS INSTITUTION

FALK AUDITORIUM

CLOUD COMPUTING FOR BUSINESS AND SOCIETY

Washington, D.C.

Wednesday, January 20, 2010

PARTICIPANTS:

Keynote Speaker:

BRAD SMITH
Senior Vice President and General Counsel

Moderator:

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

Panelists:

MICHAEL NELSON
Visiting Professor, Georgetown University
Chairman of the Technology Section
American Association for the Advancement of Science

ROB ATKINSON
President and Founder
Information Technology and Innovation Foundation

JONATHAN ROCHELLE
Group Product Manager
Google

* * *

P R O C E E D I N G S

MR. WEST: Good morning, I’m Darrell West. I’m vice president of governance studies at The Brookings Institution and I’d like to welcome you to our forum on Cloud Computing for Business and Society. And I want to start with an audience survey. You know, it’s always interesting to see how an audience feels about things and the question is, how many of you feel like you know what cloud computing is? Raise your hands. Okay, how many of you don’t really know much about cloud computing? And then, how many of you actually served in the military and were taught never to raise your hand for anything? Okay, there are two or three in that category.

Well, this is a surprisingly well-informed audience, I guess no big surprise given the fact that it is an event on cloud computing, but I’m always amazed when I talk with people outside the technology area. Everybody has heard the term “cloud computing,” but there are many people who don't really understand what it is. It's a bit of a mysterious term in terms of what it is and what its impact is going to be on society, business, and government.

So, the simple definition of cloud computing is that it represents a platform for the delivery of software services and other applications through remote file servers. Rather than storing and accessing information from your desktop, data, information, and software are placed on remote servers and are accessible wherever you happen to be. It includes many things that I'm sure people in this room already use -- Facebook, YouTube, Internet e-mail programs, ordering books through Amazon, or paying bills online through your financial institution.

But I think the key thing about cloud computing is not just that it represents a new platform, but how this new approach to data storage and service access affects the entire computing ecosystem. It think it changes how we think about computing, how organizations function, how consumers access information, and how much technology costs.

Mark Foreman, the former e-government guru for the federal government estimates that computing will cost one-tenth of the current money because of the reliance on remote file servers. He suggests that many organizations won’t need those rows and rows of file servers in order to store their own data, that they can move many things to the cloud and only keep really sensitive consumer or company information on their own local file servers.

You don’t have to be at your desktop in order to access e-mail or see what is in your financial account. You can be half way around the world and still have access to your own personal information, and you can get that information through cell phones, PDAs, or other digital devices.

But cloud computing raises a number of questions about security, privacy, data management, and legal jurisdictions. I saw a couple of jolting headlines recently. Mark Zuckerman, the founder of Facebook, recently spoke at an awards ceremony in San

Francisco, and he said that privacy is “no longer a social norm.” The columnist Michael Wolf went even further when he wrote a piece about social media recently entitled, “Privacy is like Virginity, No One Really Wants It.” Now, I’m not endorsing either one of those perspectives, but I think the fact that there are people out there making arguments like that shows the interesting challenges posed by new technologies. Obviously those technologies raise very interesting questions about privacy and security in a digital world and how we need to think about those topics. Is it possible to keep information personal? I mean, despite what Zuckerman and Wolf say, public opinion surveys still indicate people remain very worried about privacy in the Internet era.

Who has legal jurisdiction? If I’m in Washington, D.C., but my Brookings cloud is stored on a file server in Chicago or London or Madrid, who controls the cloud? Is it American, British, or Spanish authorities? What happens to the concept of a cloud if the United States, the European Union, Russia, and

China, have different laws governing that cloud? Are we going to end up with a Tower of Babel version of the cloud where there are different rules in different countries and difficulties navigating across those differing jurisdictions?

To help us develop a better understanding of these kind of issues, we have put together a distinguished set of speakers. Brad Smith is Microsoft’s senior vice president, general counsel, and corporate secretary, and he will deliver our keynote address today. He leads the company’s department of legal and corporate affairs and is responsible for its legal, government industry, and community affairs. He coordinated Microsoft’s antitrust settlement with state attorneys general, data privacy negotiations with the Federal Trade Commission and the European Commission, and intellectual property issues with various companies.

Before joining Microsoft, he was a partner at Covington and Burling and worked in the firm’s D.C. and London offices. He graduated summa cum laude from Princeton University and earned his JD as the Harlan

Fiske Stone Scholar at Colombia University’s law school. He has written numerous articles on intellectual property and electronic commerce issues and has served as a lecturer at the Hague Academy of International Law.

Michael Nelson is a visiting professor of communications culture and technology at Georgetown University. He has a PhD in geophysics from MIT, now teaches courses on the future of the Internet, technology policy, and electronic government at Georgetown. Previously he served as director of Internet technology at IBM, director of technology policy at the Federal Communications Commission, and special assistant for information technology at the White House Office of Science and Technology Policy. He was just elected chairman of the technology section of the American Association for the Advancement of Science.

He’s written extensively about cloud computing and issues affecting technology innovation and last year had an article in *Science* entitled “Building an Open Cloud.”

Rob Atkinson is president and founder of the

Information Technology and Innovation Foundation. He earned his PhD in city and regional planning from the University of North Carolina. He is the author of The State New Economy Index and a book entitled “The Past and Future of America’s Economy: Long Waves of Innovation that Power Cycles of Growth.” He has an extensive background in technology policy and innovation. He previously served as vice president of the Progressive Policy Institute.

And then our last speaker will be Jonathan Rochelle. Jonathan is the group product manager at Google. He has been working on cloud issues for a number of years and supervises the development of collaborative web products. He was instrumental in the launch of Google spreadsheets. Before that he was the co-founder of 2Web Technologies and ITK Solutions and he has a degree in engineering.

So, our format will be Brad will start with the keynote address outlining his thoughts on cloud computing. We then will ask our other speakers to come up on the rostrum and give their perspectives and eventually to answer questions from you. So, we will start with Brad Smith of Microsoft.

MR. SMITH: Well, thank you all for coming this morning. Thank you, Darrell. It’s a real pleasure for me to be here this morning, to be with a really distinguished group of people to talk about what is, I think, a very important issue.

It’s great to see that before I even start virtually the entire audience has a good grasp of what cloud computing is. Hopefully, when I finish you will have at least an equally good grasp and I won’t have taken us all backwards. That’s at least one goal for the morning.

It is a timely topic. It seems like almost every week there is something in the news relating to cloud computing. Last week was obviously no exception. The issues that were raised by Google with respect to China are clearly of great importance, I think, to everyone here and to people all around the world.

The world really needs a safe and open cloud. It needs a cloud that is free and protected from hackers and thieves and that also serves as an open reservoir of information that can serve all people, everywhere in the world. When it comes to security and free expression, neither goal is yet a reality, but they are both goals that we need to continue to work towards achieving over time.

As that reflects, these issues really are important all around the world. But this morning I would like to talk about some of the issues here in the United States.

The computing experience is really undergoing a profound transformation. It really is about the combination of smarter client devices and the use and storage of data and applications in the cloud. People are using computing power in new and different ways. We’re running applications that are in the cloud, we’re storing data and documents in massive data centers, we’re creating and accessing and sharing more information with more people than ever before.

The cloud really does represent a major extension of the computing power and the computing industry, and in that sense it really has become the next frontier.

The benefits of this transformation really are immense, but I think we also need to address the new challenges that are arising, focus on them clearly, and work together to overcome them. As last week’s issues continue to illustrate, we shouldn’t take the benefits of this technology for granted. We can’t afford to close our eyes to new obstacles and challenges. We need to build confidence in the cloud and that requires a new conversation, a conversation about both the opportunities and the challenges that we need to address. And we need to work together, those of us who work in industry and those of us who work in government and in other parts of civil society.

I’d like to talk a little bit from our perspective about the evolution of the cloud, where it has come from, where it is going, but then really what I’d like to turn to this morning is the new set of issues that I believe it’s important for government to address, especially the U.S. Government.

I will say at the outset that the label cloud computing actually reflects an attribute that is common to information technology. In the early stages of a new technology, those of us in this industry have a tendency to take everyday terms and use them in new ways that most people can’t possibly understand. I mean, after all, we are an industry that completely redefined the use of the windows, the mouse, spam, and viruses. So, perhaps it’s not surprising that as we think about the next big thing, we’re now talking about the weather. It also probably shouldn’t come as a surprise, but an awful lot of people don’t really understand what we’re talking about especially in the early days of a new technology.

Microsoft recently commissioned a poll by Penn, Schoen & Berland, PSB, to take stock of American attitudes about cloud computing. Perhaps not surprisingly the first thing one learns is that 76 percent of Americans either have not yet heard the term or have heard the term, but know little else at this point about what it really means. But interestingly, despite the lack of familiarity with the term cloud computing, most Americans already use technologies that are part of the cloud.

The PSB survey showed that 84 percent of Americans are using online e-mail, 57 percent store or share information through a social media site, 33 percent are already storing their photos online. This will continue to grow. This survey found that 58 percent of consumers and a full 86 percent of senior business decision makers are excited about the potential of cloud computing to change the way they work and use technology. The majority of consumers and business leaders also believe that the cloud has great potential for government as well.

Those are the types of propositions that I think virtually every leader in our industry would embrace. Cloud computing properly implemented really will provide users with greater flexibility, more portability, and more choice in the way they use computing. People can choose to run applications in the cloud or on their own device. They can choose to store their documents and data locally or in a data center.

They can choose to rely on a private cloud that's operated only for one organization or in many instances people will rely on a public cloud that's open to the public and in fact has multiple enterprises, organizations, and individuals using the same infrastructure. There's other alternatives as well.

In essence, given the panoply of alternatives, people will be able to choose to use the cloud for as much or as little as they want, and they'll be able to choose to keep as much or as little of their data in the cloud or on their own computers.

The new benefits from this new technology, I think, are unquestionable. They really will offer new benefits for every part of society. It gives us the opportunity to help improve health care by providing more access to applications and electronic medical records and reducing health care costs. It gives us the opportunity to provide teachers with new tools that can turn classrooms into even more vibrant places. It has potential to contribute to economic growth and job creation, perhaps especially for small and medium sized businesses.

And there’s clear opportunities for the government as well. As the Administration’s Chief Information Officer Vivek Kundra recently said, “With more rapid access to innovative IT solutions, agencies can spend less time and taxpayer dollars on procedural items and focus more on using technology to achieve their missions. That fundamentally enables government to do more of what many in business have been doing, using technology to achieve their fundamental goals.”

These are all among the many reasons that we at Microsoft are excited about the cloud. We’re one of many companies that is investing heavily in it. We’ve already invested literally billions of dollars. Some of our offerings have been around for some time, offerings such as cloud based e-mail and collaboration tools. But we’re also investing in new products and services as well. Already our business online services are being used by 1.5 million users in 36 countries. We’ve built large datacenters around the world and we’ve recently launched our new Windows Azure application platform for the cloud. We're definitely committed to world leading, enterprise class services that are really second to none in reliability, interoperability, and security.

And we're backing this with a strong partner ecosystem. We're working now with over 7,000 business partners around the world including companies such as HP, Excenture, Vodafone, and many, many others. We also recognize that the cloud is different from the past. It creates the opportunity for us to pursue more open and interoperable solutions, it creates the need for us to be more open and interoperable as well.

Needless to say, we are hardly alone. You're going to hear from people from other parts of the industry. Everyone, it seems, is taking new steps, offering new products, and investing in new ways as they approach the cloud. But as we embrace the cloud, one thing we think is important is that we not only tap its new benefits, but that we also preserve the benefits of the present along the way. We should keep in mind that one of the fundamental benefits of the personal computing revolution has been that it has made computing more personal in nature. It’s empowered individuals to use technology in the way they choose. It’s enabled individuals to store their information where they choose. It’s given individuals the freedom to share their information when they choose and with whom they choose.

No technology is perfect, nothing is perfect, but unquestionably the PC revolution has empowered individuals and democratized technology in new and profoundly important ways. So as we increasingly connect smart client devices to the cloud, our challenge is to build on these successes and make them greater still. We shouldn’t sacrifice the personalization of technology in order to benefit from computers in the cloud.

These very issues are in fact on the minds of the American public. The PSB survey found that 75 percent of senior business leaders believe that safety, security, and privacy are top potential risks of cloud computing. And as people think about storing their own data in the cloud, more than 90 percent of the general population and senior business leaders are concerned about the security and privacy issues for their personal information. Not surprisingly, the American public expects us to do something about this. The majority of every audience that PSB surveyed wants us to consider these types of ramifications about the use of the cloud. They want us to be thoughtful as we move forward and they believe the U.S. Government should establish laws, rules, and policies for cloud computing. They're right. In order to make the cloud a success, those of us in the industry need to pursue new initiatives to address issues such as privacy and security. At the same time the private sector cannot meet all of these challenges alone. We need Congress to modernize the laws, adapt them to the cloud, and adopt new measures to protect privacy and promote security. That's why we've concluded that we need a cloud computing advancement act that will promote innovation, protect consumers, and provide the executive branch with the new tools needed for a new technology era.

We need Congress and the Administration to address three issues in particular: privacy, security, and international sovereignty. I'd like to talk about each of these a little bit.

As we think about the future of the cloud, I think it's only fitting that we start by thinking about the future of privacy. Now, one could take the view that privacy is no longer important. I couldn't disagree more. I've been involved in negotiations about privacy with the Federal Trade Commission and with the European Union and neither was nearly as protracted as my negotiation with my 14-year-old daughter about whether I could be her friend on Facebook. People do care about privacy and I think as most parents have learned, teenagers still care about privacy. Privacy is about the ability to determine who gets to see your information. And if people of one generation are more interested in sharing more information with more people, they also care about who doesn't get to see that as well.

The fact of the matter is that privacy is a quintessential American right. The protection of privacy has been fundamental throughout our history. It traces its origins to the Bill of Rights and the Fourth Amendment to the Constitution. More recently a hallmark of the personal computer revolution has been the privacy protection afforded by the PC.

In the 1980s, consumers started to move information from their desk drawer to their hard disc. They regarded their PC a bit like the advertising saying about Las Vegas, what happened on their hard disc, stayed on their hard disc.

Now, in contrast, one obvious attribute of the cloud is that information typically is stored on a server computer that’s controlled by a third party. That makes it all the more important for service providers to be thoughtful and clear in communicating what they will do with this information. Equally important, we need government action to ensure that as information moves from the desktop to the cloud, we retain the traditional balance of individual privacy vis-à-vis the State.

I think Americans take for granted that

except in the plots of some popular television shows, the government typically cannot come into their homes without showing them a search warrant. But the courts have cast doubt on whether the Fourth Amendment to the Constitution, which provides this protection, applies to information that is transferred to a third party for storage or use.

The rise of cloud computing should not lead to the demise of the privacy safeguards in the Bill of Rights. The public needs prompt and thoughtful action to ensure that the rights of citizens and government are fairly balanced so that these rights remain protected. Changes in communication technology have often led to this type of issue before. Recognizing a constitutional hole, Congress acted in the 1980s to fill the gap when it enacted the Electronic Communications Privacy Act or ECPA. This law has in fact played a vital role by providing Americans with statutory privacy protection for electronic and stored communications, and it is clarified when and how law enforcement can access that data. But ECPA was enacted before the dawn of the

Internet.

Over the past two decades, technology has moved forward and the law has become increasingly antiquated as a result. We now need new action by Congress to modernize the protection of privacy and fill in these legal gaps. That’s why we at Microsoft support the efforts in this area that are being led by the Center for Democracy and Technology, or CDT. That’s one thing that a cloud computing advancement act should do, modernize privacy law and ensure that privacy remains protected.

There’s a second area where action is needed as well and that’s security. Unfortunately, there are and always will be bad actors interested in stealing digital information. At times this will be because the information is valuable, and at times it will be because individuals or groups are simply malicious or up to no good. You know, the good news is across our industry we’ve been building datacenters with more powerful security safeguards than anything seen before. Cloud computing already has a high level of security and is ready for adoption. That’s good news for consumers and businesses alike.

But at the same time, the cloud also creates bigger targets for hackers and thieves. We can’t close our eyes to that reality. There is no benefit in underestimating the savvy of potential attackers now or in the future. Across the industry we first need to continue to dedicate ourselves both separately and together to strengthening the security of the cloud. This is going to remain a daily fact of life. We also need to take new steps throughout industry to implement new security standards such as those from the International Standards Organization and under the Federal Information Security Management Act.

As the federal government moves data to the cloud, we believe it needs to continue to adhere to procurement policies that ensure that it too implements these types of security standards. But we also need new steps by Congress. Government enforcement will play a critical role in stopping and deterring attacks on the cloud, but only if Congress adapts the law to new security challenges. This is why Congress needs to modernize and strengthen the Computer Fraud and Abuse Act, or CFAA, to help law enforcement officials address security in the cloud.

There are some significant issues that Congress needs to address. Currently it’s sometimes difficult for federal prosecutors to establish the monetary thresholds needed to impose felony penalties. That’s because it’s often unclear how to place a specific monetary value on the theft of content. A photo might be priceless to me, but that is less than clear to a court or to a prosecutor. Rather than asking courts to assign a specific value to things such as photos or documents, it would make more sense for Congress to create statutory amounts or statutory penalties, such as $500 for each individual victim, and give prosecutors the ability to multiply this by the number of victims affected. That would add new teeth to the law to address security.

In addition, we believe Congress needs to increase the level of fines levied against hacking into a data center. Right now the level is the same as for hacking into an individual PC even though the scale couldn’t be more different.

We also need Congress to strengthen the ability of cloud service providers to pursue our own claims against security violators. At Microsoft we have a Digital Crimes Unit. It’s been working for about a decade. We rely on it to help bring not only our own civil cases, but to work closely with law enforcement in appropriate ways.

In some areas of the law, such as under the Canned Spam Act, it’s clear that service providers have their own private right of action. It would be helpful for Congress to amend the law to provide service providers with a similar private right of action for security attacks in the cloud.

Ultimately, stronger laws need to be effective in practice and not just on paper. As security attacks have become more sophisticated, they definitely have become more difficult to investigate. Law enforcement is going to need new technology in order to investigate security offences successfully. Law enforcement is going to need additional resources to procure new technology. Law enforcement agencies are going to need to coordinate more closely in order to connect the dots between different pieces of information. And law enforcement and the private sector are going to need to coordinate more closely in appropriate ways as well. That is what it will take to have successful investigations and protections against security attacks. Congress, in its role as appropriator, needs to provide the resources that are needed for success.

In addition, we believe that both privacy and security will benefit if we as an industry follow principles that ensure clear and complete communication with consumers. We’re familiar with the financial sector’s use of truth in lending principles, principles that were creating in the Truth in Lending Act of 1968.

We now need new truth in cloud computing principles so consumers and businesses have full knowledge of how their information will be accessed and used by service providers and how it will be stored and protected online. These principles should ensure there’s transparency over how data is protected. They should ensure that service providers maintain a comprehensive written information security program. They should disclose whether the service providers architecture, infrastructure, and controls, satisfy well-recognized and verifiable security criteria. They should convey in plain language how their information will be accessed and used by service providers so consumers know what they can do and know whether and how they can reclaim their documents and data in the future.

Simply put, it shouldn’t be enough for service providers simply to say that their services are private and secure. There needs to be some transparency about why that’s the case.

There’s a variety of different approaches one could take to achieve this goal. One would be through industry self regulation and that’s definitely an important option. Alternatively, if there’s going to be new law in this area -- and being realistic, I think there will be -- I think the industry and consumers would be best served if the law were enacted at the federal rather than the state level and administered by an agency such as the Federal Trade Commission. The reality is that cloud computing is national and even global in scope and no one is going to be well served if the law changes every time data or an individual crosses a state line.

Finally, there’s one last issue in addition to privacy and security I’d like to touch upon. This is the issue of international sovereignty.

In recent years we’ve seen emerge a global thicket of competing and sometimes conflicting laws impacting cloud computing. We’ve seen recent cases in Belgium, Brazil, and Italy, for example, where in each instance courts have sought to apply and impose their laws on U.S. service providers even though the data have been stored in the United States. These types of cases increasingly have raised the prospect not only of civil, but even criminal penalties for service providers. This is creating a Catch-22 situation for the cloud where different laws conflict. A decision to comply with a lawful demand for user data in one jurisdiction can place a provider at risk of violating a law somewhere else. It also makes it far more difficult for service providers to provide consumers with accurate information about when and how their personal information might be accessed by law enforcement.

Ultimately cloud computing will benefit the most if governments can establish a multilateral framework that provides legal clarity in the form of a new treaty or similar international agreement. We need a free trade agreement for data and information. While a multilateral framework would require substantial diplomatic, leadership, and resources, it is definitely a cause worth embracing.

Experience suggests, however, that a formal multilateral agreement will require first steps to lay the foundation for international consensus. There is a need for both bilateral and multilateral discussions between the U.S. government and other governments on new procedures for resolving conflicts, for addressing data access, and for working through the various jurisdictional issues. This should be complimented by a push for mutual legal assistance treaties and improvements that are badly needed in what is clearly an antiquated set of legal provisions. This, too, would help harmonize domestic legislation relating to data privacy. This is an area where the Executive Branch needs to take the lead, but Congress should ensure that there’s adequate resources for this work and should engage in the type of international discussions with other legislators that help build consensus with other parliamentary bodies.

As we look to the future, we should look at new ways to take steps in all three of these areas: privacy, security, and national sovereignty. Without doubt, those of us in the private sector and in the industry itself need to continue to be proactive. We need not only to develop new technology, but we need to deploy it with a sense of responsibility. We need to identify issues that require broader consideration by others like the ones I’m touching upon this morning, but we also need to recognize that government needs to play a key role, not only in using cloud computing itself to enhance transparency and improve its services, but in moving the law forward to keep pace with this technology.

In short, we need a new conversation about these new issues. It needs to be a broad conversation that includes technologists, legal experts, representatives from industry, consumer groups, and people who speak for all parts of civil society. It’s a conversation that needs to take place here in Washington, D.C., but it needs to include individuals from across the country and in fact with people from around the world. It’s an important topic. It merits an important discussion. Certainly we at Microsoft look forward to taking part.

Thank you.

MR. WEST: Okay, while our panelists are being mic’ed up, I just want to thank Brad for his opening remarks on this. I think he really laid out an interesting call in terms of a need for a new conversation.

This event on cloud computing represents a first step in this effort. We actually have a number of other forums scheduled over the next one to two years on cloud computing technology innovation and other aspects of mobile broadband and telecommunications policy. So, any of you who have particular ideas that you think need to be addressed, feel free to let us know in terms of what you think some of the important issues are in this area, and certainly Brad is very bold in calling for responsible government action. Now, Brad, some people view that as a contradiction in terms, but I like your optimism there and some of the new ideas that you put on the table in terms of amending the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, developing a new free trade agreement. So, I think, there are lots of suggestions here that certainly are worthy of conversation.

What we’re going to do now is engage some of our other speakers. I’ll have a couple questions for each of them and then we want to hear from you as well in terms of your reactions to things that have been said and any questions that you have for our panelists.

So, I'd like to start with Michael Nelson of Georgetown. You write about technology policy and in your recent *Science* magazine article, you recommended building an open cloud with "open standards, open interfaces, and open source software." So, my question for you is, is an open cloud a safe cloud? What, if anything, should the government do to protect privacy and security in the cloud? And do we actually need to update some of the Congressional acts that govern these particular areas?

MR. NELSON: Well, I think Brad has done a wonderful job of outlining the opportunities here with cloud computing and flagging some of the biggest challenges. I think the survey work that they've done to highlight the importance of addressing privacy and security concerns before consumers adopt this technology, is really important work. I hope it will inspire more people in industry to take these concerns seriously.

As Brad said, there’s been a tendency to say, well, the cloud’s going to be better, it’s going to be more secure, it’s going to be cheaper, trust us. We have to really show that that’s going to be the case. And I believe that open standards and open source software, and most importantly, competition in the cloud, are going to help us get there.

On of my big concerns and one of the reasons I’m writing about the open cloud is because I worry that if we don’t do the right things in the next two or three years, we’re going to see the cloud become something that is controlled by just two or three companies. That’s very different than what we did with the net back in the ’80s. We adopted open standards, open source software, and as a result, we built a network of networks, hundreds of thousands of different organizations all building their little piece of the Internet and making it work together.

Then in the ’90s, the web was created, and, again, it was built around open standards. There were companies that tried to create their own special version of web browsers and their own special proprietary web standards, but we as users said we don’t want that. We want to be able to use any browser we want to go to any website we can. And now we’re making similar choices about the cloud.

If we do this right, we’re going to have open source, open standards based technology that all fits together. So, I’ll be able to take something from one piece of the cloud run by one company, and combine it with data and applications in another and combine that and maybe store the results in a third piece of the cloud. That’s what users want. We don’t want to be locked into one company’s solution.

The other nice thing about this model of the future is that it forces companies from a very early point to build in security, security that’s wrapped around the data itself and the software. We know that in the cloud you’re not going to be able to use the fortress model of security, you’re not going to be able to build a firewall around all your data and your systems and be very careful about who goes through that firewall. That doesn’t work in this new world of a totally interoperable global cloud. So we need a new approach. We need to look, very carefully, at what customers are telling us, and, most of all, we have to give them choices and transparency.

And just to finish up, I think the most important word that Brad said, and he said it repeatedly, was transparency. If we’re going to convince people that their data is safe in the cloud, we’re going to have to show them why it’s safe. In some cases there are ways that you’re going to provide built-in auditing capability. There’s technology now called immutable audits, it allows a company to provide an audit trail that will show me, as a customer, every time my data has been accessed, when, how, and why. That’s the kind of technology we need to look at. Encryption is part of it, better passwords, there’s a lot of other things, but the ability to show customers, this is how your data is being treated, this is how it’s encrypted, this is who has access, I think is going to be the key to a successful cloud.

And if we do it right, in 10 years 80 percent of all the computing done in the world could be done in the cloud. This is that big. This is a total transformation if we get it right.

MR. WEST: Michael, I have a question about the doing it right part. Do you think the government needs to do anything beyond what it is currently doing to protect privacy and security? I mean, for example, Brad was suggesting we need some new legislation in terms of electronic communications, consumer fraud, and so on. Do you think that's the way to go?

MR. NELSON: Well, I think Brad's laid out some specific fixes to some legislation that was written long before the cloud and I think some of that makes sense, but I think there are two even higher priorities. The first one is that government, both in the U.S. and globally, has to say what it's not going to do.

I had the privilege of working in the Clinton White House and worked with Ira Magaziner on the Magaziner Report on E-Commerce. That was a unique report because every page of that report announced what government was not going to do. We were not going to specify a certain type of privacy regulation everywhere, we were not going to censor the Internet, we were not going to specify how security systems had to be built. And by providing some certainty in the regulatory system, I think it really spurred the innovation that we saw throughout the ’90s in e-commerce.

Right now there’s a lot of uncertainty about when will governments have access to information in the cloud? Will you need a search warrant? Will it be as well protected as it is on your hard drive? Those are really important questions and government has to clarify what the rules are, but mostly they have to say what they’re not going to do, how they’re not going to regulate this new system, how they’re not going to access data.

The second thing they need to do that’s equally important is they have to be a really smart buyer. The reason we have the Internet today is because back in the late ’80s when we had all these different proprietary networking protocols, the government, and specifically the Defense Department here in the U.S. decided it was going to use TCPIP, an open standards, open source technology, to tie together the military networks, the civilian military networks, so .mil was run on TCPIP rather than an proprietary corporate standard. That tied together the Internet and launched what we have today.

Similarly, government can be a smart buyer of cloud services and avoid being locked into one particular company. Government is a big player in this marketplace and they can demand that when they buy cloud services, they aren’t locked in to one particular solution.

I think all of us need to demand that, and users have a voice here. At this critical point we can speak up and say, this is what we need.

MR. WEST: Okay, Rob Atkinson, I have a couple questions for you. Is security in the cloud better or worse? And if data are stored in a cloud outside the United States, is the information still safe? And are there legal recourse for consumers if their data are breached?

MR. ATKINSON: Well, first of all, thank you, Darrell, for having me here. I want to start by saying, first of all, I agree with everything -- I think pretty much everything Brad said, I think, is absolutely right, and endorse that. I think he’s absolutely right about the kinds of things we need to do.

I can’t answer your question, Darrell, without responding first to Mike, with all due respect. I think part of the problem with the whole debate on the cloud, as Brad alluded to, you know, calling it the cloud, it’s this sort of magical term that no one understands other than the people in this room. If -- Darrell, if you were to have called this event “Legal and Policy Issues with Regard to Remote Data Storage,” I think you might have had 10 people in the room, but you call it the cloud, and, you know --

MR. WEST: And that’s including the people on the panel.

MR. ATKINSON: Including people on the panel. I might not have even joined.

MR. WEST: Yeah, that’s right.

MR. ATKINSON: But, you know, you call it the cloud and it’s like, oh, my gosh, magical thing. And really the cloud is simply remote data storage. It’s not a magical thing. It’s not transformative. And so I disagree with what Mike is saying, with all due respect, in the sense that if what you’re talking about is an open source, open standard system in the cloud, then you have to also say that that’s what we also want on the desktop. That’s what we want on the entire software ecosystem of the globe because there’s no difference between the software system on the desktop and the software system on the cloud. It’s just a question of where things are stored.

And so we already have an open, interoperable standard to access the cloud. It’s called the Internet. And so I can access any cloud server anywhere in the world that I have permission to access through this regular open source, interoperable standard called the Internet. That’s very different than saying we’re going to transfer that into proprietary software. I just don’t see that as an appropriate call to action or something that would actually be useful.

Going back to this other point about is data secure in the cloud, I think in some ways it is and in some ways it isn’t. Certainly Microsoft or Google, they have much better security than -- and more security people who are more knowledgeable than the company that we use at ITIF. Not to knock the company we use, but it’s somewhere up in Rockville or something and they’ve probably got 20 or 30 people. I’m sure they’re decent. They seem like they’re okay, but I would envision that Microsoft probably has better security people than this little company does. So, is the ITIF data more or less secure? In some ways it’s maybe even more secure if it’s in the cloud because I’m able to rely on these kinds of companies that have a lot of stake in the ground and a lot of expertise.

But I think we also have to remember that people look at the cloud and say, oh, my gosh, it’s not secure. It’s in some ways about as secure as your own remote -- as your own corporate servers or organizational servers. Somebody could -- I could download some keystroke logging by mistake and somebody could easily get into the ITIF server, which isn't in the cloud. So, in some ways I think, again, the difference between the cloud and the non-cloud on security is a little bit misleading.

The last point, I would just respond here, I think what we -- the key to me, threat, of the cloud is as we saw last week or two weeks ago in China, and that's what you could call state-sanctioned Internet lawlessness. And I think that's what we're seeing around the world. There are countries, and I would point to Russia and China being two of the leading ones, but there are certainly other ones that at best turn a blind eye to criminality and, at worst, openly sanction it and possibly participate in it. That, to me, is the big threat to the cloud. It used to be if they wanted to hack into computers they could do it in their own country, they couldn't come here, we wouldn't let them in here. Now, there's a wire that connects hackers, state sanctioned hackers in China, and in Russia -- you know, a wire that connects them into the U.S. And I think unless we come to grips with that reality and say, wait a minute, this is not an acceptable level of behavior, and unless you as a nation crack down on that behavior, we're going to take steps, collectively as a body of nations, I think we're going to have real problems going forward.

And then just to finish, what Brad said, I think the other key threat here is what you would call cloud protectionism. These countries that say, hey, this is a way for us to do what we've always wanted to do which was take -- try to go after U.S. technology leadership. We'll just force them to open up their cloud servers and put them into our country. That's a way we can jobs and other things. That, to me, would be a huge mistake. I think it's a huge threat that's going on, and again, unless I think the U.S. and Europe takes real action and leadership on that point, we're not going to get where we need to go.

MR. WEST: Do you want to respond?

MR. NELSON: I just wanted to clarify

something, Rod. I’m not saying that the whole world is going to be open source and open standards based. My point is that we’re going to have this ecosystem of open source and proprietary technology. If we want the cloud to provide the maximum benefit to the maximum number of people, we’re going to want to have open interfaces; we’re going to want to have ways to move data from one piece of the cloud to another. It may be that there are proprietary applications running in the cloud, but I as a user want to have some way that I can take the data that comes out of that proprietary application and do something else with it.

I fully expect that we’re going to have a very complicated ecosystem with proprietary and open source technology, but we want to have some way to pull the pieces together or else we’re going to end up in a world not of the cloud, we’re going to have clouds, and they’re going to be separate pieces run by separate companies and you’re not going to be able to get the real benefit. And it’s not just about data. It’s about collaboration, it’s about letting people in different places who are using different applications, talk to each other and combine their ideas, not just their data.

But again, let me be very clear, I’m not saying we have this ideal -- this extreme position where everything’s open source. I just want open interfaces, open formats, open standards, so I can move things back and forth. A very good example, to be very specific, is the pen document format. if I’m building the cloud and all these different applications are processing documents, I don’t want to have to buy a bunch of different proprietary technologies to read each of the different documents that I want to bring together in a new application.

MR. WEST: Let me bring Jonathan Rochelle into this conversation. Jonathan, what do you see as the benefits versus the risks of cloud computing? How are you dealing with security issues? And what role will mobile devices play in privacy and security? Does the rising use of cell phones, smart phones, and PDAs actually increase the security risk and the privacy threats?

MR. ROCHELLE: Sure. The -- I mean, I think some of the benefits and risks -- we skipped over a lot of the benefits because I think people in this room feel that, they know the benefits, they understand it, so hopefully that is clear.

The one thing I'd like to just clarify, I think, is the difference between the benefits and the risks of the applications in the cloud and the data in the cloud. They are two distinct things. And it brings me to a point that's -- or at least a terminology thing that I think should be clarified as well which is open standards versus open source, and I think it's too often that people use, well, openness in general, but open source as a synonym to open standards and it's completely different.

Open source, for maybe the two people in this room that don't understand, means that the code, the instructions you give to the computer, can be seen, that a programmer could look at those and say I can see that this program is doing X, Y, or Z. The benefit of open source amongst many things is also part of that whole transparency story, that you can’t hide an instruction that steals a penny from a bank account every time there’s a transaction if it’s open source. A programmer could look at that and say somebody did something wrong here, something evil.

So, open source is very valuable to consumers. And besides that, there’s so many other things, innovation and collaboration and things that are, you know, unmentionable here, it’s just too deep. But open standards, obviously, have to do with doing things in the same way so that there’s some equality amongst access, amongst providers. And for consumers, again, the benefit is portability. So, I think transparency and portability, those two benefits rise to the top easily.

On the risk side, clearly there’s other risks besides privacy and security, but those are the two that always come to the top as well and I don’t think that that is -- I agree, I think, wholeheartedly with what Rob was saying, that there’s nothing special, necessarily, about those risks. They don’t exist on the cloud and not on personal and desktop computers. It’s just that I believe that in the cloud those risks become more transparent and more collected and somehow more open so that there’s no quiet crime on a personal computer as much as there could be -- you know, in the cloud you really don’t get that. You have the opportunity to expose some of these risks in a way that affects many people. I believe that individuals on personal computers wouldn’t necessarily have the wherewithal to know when something wrong was going on on their machine and while it feels more comfortable the same as, you know, the money under your mattress feels more comfortable, it might not be the best way to actually manage your information.

So, those risks notwithstanding, I think the other risks that are worth mentioning are access and connectivity, the things that are becoming ubiquitous and were taken for granted already are things that we really are dependent on in a new way. And so I feel this personally and obviously for the company I represent, connectivity is critical. And so with the cloud, that becomes even more critical and much more of a bottleneck potential than it would with a personal computer. Personal computer, I can go and turn it on, but these days a personal computer without connectivity is pretty much a doorstop. You know, nobody’s using that. Nobody looks at a computer and expects it not to be connected anymore. So connectivity, I think, has drawn personal computers into the cloud regardless of whether or not you’re actually using cloud applications and storing your data in the cloud. You have opened your personal computer to the world if you’re connected to the Internet. There are people that know how to get into your machine if you’re connected. Clearly, then, there’s a whole industry around protection: firewalls and hardware and software that protect you in that.

But it’s not like that risk doesn’t exist just because you’re working on a personal computer. So e-mail and some of the technologies that were here when the laws were first passed in 1996 or around that, that was cloud computing. There was already some awareness that your information was going from your local machine or from your fingertips through your keyboard to someone else and there were protections put in place. Clearly that needs to be updated, but I think it wasn’t based on personal computing. I think that was something that was stated. I think it was much more based on e-mail and the transference of data.

MR. WEST: Jonathan, do you think the government should be doing more to protect security? And then, what about the mobile devices part of that? Do they actually make security more of a consideration?

MR. ROCHELLE: I think we do have to update the laws. I don’t think we should necessarily wholeheartedly change the law. I think ECPA’s a good thing. So, the changes would be to even it out and to make it so that data that I have locally, and the way it’s protected locally, would apply in the cloud. There’s no reason that me putting data in the cloud should change my protections as a consumer.

And I do think we have to start even thinking about -- and I think this might be a little bit more forward thinking and it sounds potentially crazy, but I see it in education -- which is that access to information through technology might eventually be considered a human right. I mean, I think that when I talk to a classroom of students, if there are two or three students in that classroom that cannot access information on the Internet, if they do not have a computer at home or a terminal at home that they can access the Internet, that’s immediate inequality. That’s something that really is something that we might have to address eventually, so that access is critical.

And so security, I think there are definitely commercial standards that will arise because consumers will demand it, right, so process to understand what the company that you’re storing your data with is doing to protect your data is important. I think that will happen as part of normal, again, commercial efforts because consumers will demand it. The same with privacy policies became standard. You’re getting so many of these things unfortunately printed in the mail, constant privacy policy changes, and we’re becoming a little bit -- it’s a little diluted. I think the same thing will happen with some of the cloud services in terms of their security policy and to say what are they doing to protect their data.

And then, of course, education and transparency, giving people their data and access to their data when they need it. Mobile, I think, brings up one of the benefits that can be discussed about cloud computing in general, but just portability and the ability to access your data anywhere, mobile has clearly made that more desirable. I can -- this is the first time -- I have to say I think it’s actually the first time I’ve shown up to an event without my laptop and I just discovered earlier that the only disadvantage -- I thought I had everything with me on my phone. I don’t have business cards, so that’s the one thing that I would have had in my bag if I had brought my laptop, but instead of carrying a 20-pound bag around, I’m carrying my phone. And I, as a consumer, almost demand that I can access my information. If I had my information locally on a machine, that would be very difficult, not impossible, but very difficult and it would take a lot of process on my own account.

So, I think mobile will improve and increase the adoption and the demands and actually some of the issues it will arise, that security and transparency and portability will become improved because mobile will make it -- you know, each individual will say it’s critical for me. I need it.

MR. WEST: Brad -- I mean, Jonathan was talking about relying on commercial standards and there’s kind of a sense that, you know, eventually industry security and privacy efforts are going to catch up with the threat and perhaps we don’t need to do as much in that area. Based on your keynote address, you had seemed to disagree with that. You think the government actually needs to be much more proactive, needs to change legislation, needs to amend the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, I take it?

MR. SMITH: Yes, definitely.

MR. WEST: And so, what do you think are the most important things that we need to do in those areas that would actually protect consumers?

MR. SMITH: Well, I think it goes back to two of the points I discussed, I mean, one is the issue around privacy. And the thing I think we should be asking ourselves is whether our privacy rights are different because of the cloud. And arguably they are because of a lack of clarity under the law especially vis-à-vis the state and the specific question of whether the Fourth Amendment applies. To the extent that it doesn’t, I believe that Congress should do what it did in the 1980s and ensure that it does, you know, through amendments to ECPA.

MR. ROCHELLE: And just to clarify, we actually totally agree with that. We’ve joined the CDT as part of that movement.

MR. SMITH: Yeah. And certainly I think that it’s completely appropriate and to be expected that individuals are also going to want to know what those of us in the industry are going to do with data and information and documents as well, which is why I think that having clarity and sort of truth in cloud computing principles is a sensible thing to do. I think it builds confidence in the cloud, which is, I believe, an overarching objective.

On the security side, yeah, I think that it’s not necessarily that constructive to debate, well, which is safer, is it a laptop or a desktop or something in a data center. The reality is that we need to be vigilant in addressing security across the board and the reality is that security attacks or, you know, cyber attacks, have become a daily fact of life and it really crosses a wide range of spectrums. At one end of the spectrum, you know, we have seen some sophisticated attacks from individual teenagers who often are very smart and have no social life and use this as a way to keep themselves entertained. But one of the traits of our industry is we’ve demonstrated that some of the most brilliant thinkers are, you know, below the age of 25. So, if people haven’t found their right path, they end up on the wrong one doing this sometimes.

We’ve definitely seen, especially over the last five or six years, a criminal element that is into the security attacking or consumer fraud business to make money. You know, it’s an opportunity to separate consumers from their wallets, and so they are a threat. And, you know, there are government attacks as well and the use of -- let me just say, the focus on security by governments is not something that is confined to only one or two governments in the world. I mean, it is increasingly something that you see many governments building up resources and so that has become something that we all have to think about.

So, the reality is we need stronger and stronger security protection and, you know, I think those of us in industry are often on the first line of defense. We have to keep investing as we are -- our companies, other companies are investing in building stronger security, but I don’t think that we can expect to do it by ourselves. I mean, if you live in a city you’re going to make sure that you have a stronger door and you’re going to put a stronger lock on your door, but you still want a strong police force, you still want strong laws, you still want strong prosecution. It’s not an either/or proposition. And I think those of us in the industry need to build, you know, stronger doors and better locks, and those in government need to build stronger police forces and have stronger laws and we all need to work together to create a safe and secure environment in the cloud.

SPEAKER: Just real quick I want to join the chorus and say that this issue about when can government get access to the cloud and the data that resides there is really fundamental. And if we don’t clarify here in the U.S. what the policy is, other countries are going to go their own way. I think we can be a model if we move quickly. But we have to remember, John Perry Barlow is very fond of saying that the First Amendment is a local ordinance in cyberspace, and what Google has been going through in China is evidence of that.

The Fourth Amendment is a local ordinance in cyberspace as well. We have to make clear as a government that the cloud is not going to be a privacy-free zone that you’re going to need some kind of search warrant that that’s going to be the kind of protection you have. And if we don’t step up in the next two years, really, and show that there’s a clear rule here, other countries are going to start adopting practices that are much more egregious and -- European countries, Asian countries are going to start getting the idea that the cloud is their property, too. They can just go in and get what they need when they want it, they don’t have to deal with search warrants.

A flipside, another piece of this, is liability. What happens if the cloud service provider doesn’t protect data according to the way it was -- it promised to? And this is the other piece of the puzzle. I think we have to make very clear who will be liable for what, whether it’s security, illegal activity. If we hold cloud service providers liable for everything, that’s a great way to kill the cloud. If we don’t hold them liable for anything, that’s a way to have anarchy and have a lot of major problems that destroy trust in the cloud. So we have to get that part right. And again, we don’t have 5 years or 10 years. We’ve got to address these issues quickly.

MR. WEST: Why don’t we open the floor to questions and comments from the audience? I think there’s somebody with a microphone back there, so we have a question up front on the aisle and if you could give us your name and your organization. We have lots of people who want to ask questions, so I’d ask you just to make your questions very brief.

MR. ZUCK: Hello. My name is Jonathan Zuck and I’m from the Association for Competitive Technology. And having gone to graduate school across the street here, I’m very interested in the third component of your speech, which is this international component that you’re just sort of touching on now toward the end. And it seems to me that our track record in this level of cooperation, particularly in the area of intellectual property, for example, is not great. And I wonder is there more we need to be doing? Is there more the Administration needs to be doing to bring about this kind of cooperation or are we really just engaging in fantasy in discussing coordination about privacy practices, government access to data, et cetera, if we can’t really find a way to find that coordination and that common ground with foreign countries?

SPEAKER: I think it’s a real issue and there’s a real need for us to get going, so to speak. If I analogize to -- more to the privacy area. You know, the privacy area is a field legally where the European governments got out on their front foot, in part because of some of the lessons they learned from the 1930s. So they were among the early legislators and regulators of privacy rules.

In the U.S., we tended to say that it was a state issue and we didn’t need as much federal law. We still don’t have a comprehensive federal privacy law and I think we need one. And as a result, the U.S. Government did not play the kind of leadership role in the development of international privacy norms that it has played in a number of other fields. I think we do want and need more U.S. leadership when it comes to working out the jurisdictional understandings and whose law is going to apply in the cloud and the only way to do that is for the U.S. to get going.

I do think that one needs to be realistic. The ultimate goal, I believe, is something like a WTO or other multilateral agreement, as I mentioned, but you just can’t get there in a single step. You’ve got to build a foundation, and the best way to build a foundation typically is through a combination of bilateral steps. One can begin to build certain principles into bilateral trade agreements, other bilateral instruments, and in certain multilateral foray, like the OACD, where you start to build a consensus even before you then have new rules.

And the sooner we get going, the better off we’re going to be.

SPEAKER: Just real quick, I’m glad you brought in intellectual property because when I look at the issues that I’ve been working with for 20 years, the top 3 are always privacy, piracy, and security. You can’t get the first two without the third. But we haven’t talked a lot about piracy, but that’s going to be a major concern in the cloud.

I’d also point you to an excellent conference that OECD had two months ago on cloud computing and its policy implications. And there’s a very nice briefing paper about 15 pages walking through the key policy issues that need to be addressed.

I’m glad the OECD is tackling these issues and informing governments on what needs to be done. But I think at the end, it’s probably going to be more a decentralized approach where each country is going to have to adopt their existing rules and regulations, which vary from nation to nation, to realize this new world. I don’t think we’re going to have the universal cloud treaty anytime soon.

SPEAKER: Can I just add to that real quick?

MR. WEST: Oh, sure.

SPEAKER: I think the federal government, no matter what administration we’re in, has a central approach to this which is along the lines of we’re dealing with reasonable countries who want to do the right thing and, therefore, the right strategy is a collaboration, a coordination strategy, consultative strategy. That’s the right strategy for those countries who want to do the right thing, but there’s a whole set of countries who have no interest in doing the right thing, who have every interest in doing the wrong thing or turning a blind eye to that. Asking them, begging them, collaborating with them, is a failed strategy and the only strategy that will work in that situation is you have to get tough; you have to have real sanctions and penalties. You look at what the Russians are doing or what the Chinese are doing or many other countries where they allow spammers to exist, they allow hackers to be there, they -- in some cases, the governments are involved, as Brad said. You know, we can’t just say please don’t do this. We have to actually work with the Europeans, work with the Canadians, work with other countries who are generally law abiding, want the Internet to be a legal space, and really take tough action. And I don’t see us doing that right now. And I think until we do that, we’re not going to see a lot of change.

MR. WEST: Okay, we have a question there on the aisle.

MS. NEWMAN: My name is Karen Newman. I'm with the law firm St. Ledger-Rooty Newman & Olsen here in D.C. And I'd be interested in the panelists' views about the challenges posed to data security in the cloud by virtualization, whether you think there are currently the tools that exist to address those challenges beyond amending the existing statutes that you mentioned, whether there are approaches that could be taken even at the product design level in terms of embedding approaches at the design phase.

MR. WEST: Virtualization?

MR. NELSON: I'll weigh in a little bit. I mentioned earlier this idea of immutable audit technology. That's just one example of the kind of thing that would make the cloud a lot more secure. If you can actually wrap the software around each individual element of data so that you can track whose got access to it, where has it been moved, how has it been encrypted, you have a lot more information on the security of your overall system, and not only can you be confident it's more secure, you can also convince your customer it's more secure. And that's one of our biggest challenges in the whole space of security.

In the web we've done some pretty cute little things. I mean, SSL is a good security technology and we made it understandable to the customer by putting that little padlock symbol on the bottom of your web browser. That gives people some sense, oh, security is on. My connection is secure.

We've got to think of some things like that that make it transparent and obvious. And we're not doing enough of that yet, but I know Google, Amazon, Microsoft, IBM, all the cloud providers are really throwing a lot of money and a lot of brilliant people at this problem. I think we'll get there. And it will be, as Rob said, a lot more secure because you've got a lot of really talented people building this infrastructure and they know that security is going to be a differentiator. If they can show people their system's a better approach, they're going to get more customers.

I think our biggest challenge right now is convincing people that we don't have to make the cloud

100 percent secure, we just have to make it better than what we’ve got, and that is not very hard.

MR. WEST: Okay, over here in the front row.

MR. SNYDER: Jim Snyder from Isolin. The Federal Trade Communication is the primary --

MR. WEST: Actually, could you speak a little more into the microphone so we hear you?

MR. SNYDER: The Federal Trade Commission is the primary federal agency with jurisdiction over privacy issues. They’ve been doing a series of workshops on the Internet and privacy and, in the last few weeks, they introduced an initiative on cloud computing and privacy, exactly the subject of much of this discussions.

My question to you, most of the discussion has been on what Congress or various international bodies should do to deal with these agencies. If you assume that Congress does nothing and the FTC’s jurisdiction does not change, what can and should the STC do as part of its cloud computing and privacy initiative do to deal with this issue?

SPEAKER: I was here last January 20th and everybody was optimistic about what all parts of government would do, and a year later everybody's very pessimistic. So you assume that Congress will do nothing and it just reflects a little bit of the changing mood.

I think the question will first turn on what the FTC believes it has the jurisdictional authority to do, and certainly there are additional steps that the FTC can take. I think that the FTC can help the situation in general by contributing to a new consensus around, you know, sort of what truth in cloud computing principles might look like. The FTC can play a role in encouraging those in industry to sort of get on a similar or same page. The FTC might be even able to take certain steps within its legal authority already to make some of that binding. But it won't be able to do, in my view, the number one thing that also needs to be done, which is to have this law created and applied at the federal level rather than the state level.

I think that it's not really going to serve consumers or our industry well to have a new patchwork of laws where we have a federal law and, you know, 50 states and the District of Columbia having laws all being applied at the same time. I think we'd be better served if this really got elevated to the federal level.

One reason I think it's important for Congress to act quickly is because if Congress acts first, I think you can preempt the creation of conflicting state laws. But once states start to enact laws, it just becomes a more complicated and difficult political proposition for people on Capitol Hill to be prepared to preempt state law. And I think this is where we need leadership at the federal or national level.

SPEAKER: If I could just add, I'm a technologist, not a lawyer, but I do think the FTC can have a major role in pushing companies to be more transparent and making sure that the privacy policies, the security policies that they promise are actually abided by.

MR. WEST: I have one question on this

transparency issue which several of you have raised. How do we improve transparency without letting the bad guys know what we're actually doing?

SPEAKER: I think you are going to let the bad guys know some of the things you're doing and they're going to be very discouraged when they start seeing what kind of security provisions are put in place. I don't think that the answer is security through obscurity. We've tried that for 30 or 40 years and often the threat is not the outside hacker, the 14-year-old, it's the disgruntled employee who decides he's going to do an inside job. So, if you build the system right, you're protected from the outside and the inside. The transparency allows a company like Google or Microsoft to see into their own systems better, to see where data's being accessed when it's not supposed to be accessed. That, I think, is -- that's what I think of first when I think of this transparency.

There is a balance. I mean, clearly you don't give people passwords, but you can tell them how the system works and the outside hacker will, I think, start to understand that they should go looking elsewhere, steal credit card bills from peoples' mailboxes rather than try to hack into the Google cloud or the Microsoft cloud.

SPEAKER: I don't think it means 100 percent transparency, I think -- so giving away passwords would be the ultimate test. But the algorithm for those passwords or the algorithm for second-level checks or double authorization or things like that, those can be unique and they can be intellectual property. And I also think that practices, things like -- and it becomes a little bit more capable with things like cell phones so that every time your account is accessed, you know, send me a message, call my home phone, call my cell phone, tell me that my account was accessed. And if it becomes annoying I can turn it off, but at least I know that when I feel like I'm at risk, I can turn that on. Those are the things that are pretty, you know, easy practices, but not very technical. It doesn't have anything to do with the transparency of the code.

MR. WEST: Okay, in the very back there's a question -- actually, right here on the aisle.

MR. ALEXANDER: I’m Jeff Alexander. I’m policy analyst with SRI, and I would like to know your reactions to two proposals I’ve heard thrown around about how to improve innovation and security. One is actually something Mike had mentioned about holding cloud service providers liable for security breaches. I mean, when my Visa card gets stolen, I know my liability’s capped at $50 and I don’t have to wait for the attacker to be charged for me to get reimbursement. So why not hold the service providers somehow financially liable when they say that their system is secure?

The second proposal is to have the equivalent of a National Transportation Safety Board for security forensics so when there’s a large breach, like in the case of Heartland Payment Systems, you would have a government agency go in and investigate what happened and publicize the investigation results so that companies can’t hide behind some kind of proprietary shield and we would actually know the details of what went wrong.

MR. ROCHELLE: The second proposal’s a new one. I’ve never heard -- that’s interesting, it’s actually intriguing. I haven’t thought through it enough, especially not to represent Google’s view on it, but my own view, it sounds very interesting.

The liability concern, I think, you know, Brad mentioned, I think the toughest part of that is putting value on what was stolen, exposed, you know, lost. But it’s also very clear that that would raise a whole new cycle of insurance, which I expect -- maybe it already exists, but certainly, you know -- and court proceedings and all kinds of things. It’s a tough one to say, no, we can’t be liable. That’s virtually impossible. It’s just whether you need new laws to make that liability clear. It’s not very clear to me, but certainly the value side has to be raised to the top and say, well, how do we value lost, stolen, exposed information?

SPEAKER: You have to make the standard very sharp and clear. I mean, you can’t hold all cloud providers liable if they're all part of some interconnected cloud of clouds and one of them does something not quite right.

On the other hand, if somebody does something blatantly obviously wrong and gross ineptitude, I think they should be held liable. They'll certainly be pilloried in the marketplace if there's transparency and people know what happened, but I think we have to get this question right. If we get it right, we'll see the benefits we've seen in e-commerce, in the credit card industry, the example you gave; if we get it wrong, we could close down this incredibly exciting opportunity very quickly.

SPEAKER: And it's very connected to what was spoken about in terms of -- I wouldn't necessarily call it truth in cloud computing, but truth in advertising. It goes back to any product which is if it was promised that when I put something there that it's safe, literally, and there was some description of what that means, you know, 100 percent guarantee that you can get to it again, then that would be something that would be, I think, a little easier for a court to say, yes, this is what was promised, this is what was delivered.

But there are so many instances now of small companies delivering very valuable service that it’s so unclear what the expectation would be, so if I, you know, go to some new drawing product on the web and I create a new schematic of something that I think is the most brilliant invention and I hit Save, I quick save, I don’t know who’s liable if I clicked Save and I can’t get to it again. Was it my connection? Was it that provider? Did that provider promise that I could get to it again? Is there something in the fine print in terms of service that I just clicked and said, yes, I agree, whatever, click, done? There’s so many steps along that process, there’s a continuum, so it does depend what was promised.

SPEAKER: And it is a cloud of clouds, so it could be that the defect isn’t with the company you thought you were getting your cloud service from, it was a subcontractor who was providing some other cloud service that they rely on. So the way to think about this is the issues are now 10 times more important and at least 5 times more complicated.

MR. WEST: Brad?

MR. SMITH: Well, you raise two very interesting questions and they’re quite different and I’ll just pick up on what Jonathan and Michael are saying. Taking your second question first, I mean, I’d probably say, you know, there’s virtue in the right people in the federal government understanding what has happened with respect to particular security attacks and the like, but I’d also say that there’s probably a need for judgment to be applied as to how much information is then shared publicly about individual incidents. I think that this is fairly different from the kinds of issues that arise in, you know, commercial aviation and the like. But I think the topic is worthy of, you know, really further development.

I think on the liability issue, I would agree with what Jonathan and Mike are saying. I think one should be reluctant to impose what lawyers would call a strict liability standard. In other words, people are going to have to pay out in some defined amount regardless of whether there was any fault; or put it another way, if one were to do that, one is going to probably increase the cost of running the cloud and you can then expect economics to do what economics does and it will transfer that cost to customers. And I’m not sure that’s really going to benefit anybody at the end of the day.

At the same time, as they pointed out, you know, there’s a lot of legal standards that stop short of strict liability. You have negligence standards, gross negligence standards, things like that. And we haven’t really had much in the way of court cases that have set the standard, but I don’t know of anybody in the industry who is assuming that this area is going to be immune from the law. So, undoubtedly, we will see cases in the future and my guess is we’ll probably see courts move to some kind of middle ground. That’s what we’ve seen with other new technologies of all sorts over the last 50 years and I think it’s a relatively safe prediction that one will see that here, too.

MR. WEST: Yes, question right there.

MR. GARDNER: Erin Gardner, Americans for Technology Leadership. Does that liability threshold shift at all when these technologies become, I guess, mandated or adopted by state and local governments?

MR. SMITH: I don’t know that the liability threshold shifts, but I do think that what you’re referring to is something that is going to be a very important part of the marketplace. The marketplace is going to be influenced and shaped to some degree by the policies and preferences that are pursued by governments in their own use, in effect, as purchasers of cloud technology. I think that was part of what Mike was getting at before. And, yeah, I think where I would suggest government should go is to insist on a high level of security protection, but to avoid enacting provisions that are going to mandate for some extended period of time some specific technology that may change. I mean, in our industry we talk about having regulation that we describe as technology neutral and this is probably an area where some level of technology neutrality is going to be needed, I would say. It’s one thing to say you want to purchase technology that complies with an ISO standard, ISO 27001 or you want to purchase technology that complies with FISMA or you want to see certain adoption of open standards and, you know, there is room for, I think, a lot of discussion around those kinds of things. You know, that’s distinct from saying, we’re only going to purchase technology that implements this standard in a specific way.

I think if governments go the second route, you know, you run the risk of becoming outdated very, very quickly and probably influencing the market itself in ways that are not intended.

SPEAKER: But some countries might do that as a protectionist measure. We have to worry about that --

MR. SMITH: I think that’s entirely possible.

SPEAKER: The U.S. Government can be very --

MR. SMITH: Yeah, I mean, already we certainly see efforts in some parts of the world by some governments to advocate the creation of specific standards which they will then adopt as part of procurement or other national policy, in a manner that really furthers industrial policy or protectionist policy. And I think this is, frankly, an area where the U.S. Government needs to show that we’re not going to apply these kinds of things in a protectionist way. So the U.S. Government can be an effective advocate in trying to discourage other governments from doing that.

MR. WEST: Okay, there’s a question along the wall over there. Yeah, the gentleman with his hand up.

MR. GELLMAN: Thank you. I’m Bob Gellman. I’m a privacy consultant and I did a report on cloud computing and privacy for the World Privacy Forum last year.

Mr. Smith, I would like to ask you about your proposal. I think it’s very useful and I think you address some important areas and I think protecting people against government and hackers useful, but I think consumers may need more help.

If you read the terms of service of some of the particularly free cloud computing services, the cloud provider claims the right to use, copy, disclose, publish, do anything it wants with information put in the cloud and I don’t think consumers have any understanding of what those terms of service are. And I wonder if you think that needs to be addressed as well?

MR. SMITH: I think that’s part of this conversation. I would definitely agree with that. I think that if you want to build confidence in the cloud, it probably helps to have some common standard that will ensure that cloud service providers provide clear information in plain language and I think there’s room to say, hey, things can get better. There’s room for improvement in this part of the marketplace today.

I think there’s room to say that as cloud service providers do that, there’s a common set of questions they need to answer. I would stop short of telling everyone they must answer the same question in the same way, because I think, inevitably, free services are probably going to be attached to greater usage rights for cloud service providers than services that people are paying for. And I think that there’s room for healthy competition in the marketplace over the degree to which different providers use information. But you actually have a hard time establishing a competitive marketplace if you don't provide consumers with clear information. So, you do need transparency and the transparency needs to be effective.

SPEAKER: I think we also need the third-party evaluators. Transparency doesn't work if, as you say, people can't understand what they're being told. Companies can be as transparent as possible, but that might just dump a lot of data and information on the consumer. Consumer Reports and Better Business Bureau, these organizations, I think, are going to have a more important role in the future in evaluating which companies are really meeting the needs of consumers.

MR. ROCHELLE: And I think -- the clarity, I think -- and I'm surprised, Bob, that you didn't address the question to me, but the clarity of the information, I think, is the most critical thing. Because the way you stated it is not quite -- I mean, it makes it sound like everything someone puts in the cloud, and I'll use Google just as the example and my specific product, something like docks and sites, that everything you put in the cloud can be used the way you described, and that’s not the way the terms read, although they might be interpreted that way. The way they read is that if you publish them, if you make them available -- so when you first put them out there and the clarity comes with -- and I struggle with this daily, when you put information in the cloud, that’s not publishing the information, that’s putting it in the cloud. It’s still under your account, you have control. If you then say I want to make this more broadly available, then because of the “laws of the web” the way the web works is that search engines, ours and every other one -- in fact, there are different restrictions that are very standard and that’s another reason for standards, I think -- will just grab that information if it’s openly available. So it will be made available and we have to state that that’s true, but it’s a misnomer to think that everything you put in the cloud under your account will be made and owned by the provider. That’s not actually what the terms say.

SPEAKER: Just to raise another variant on this issue, at the latest Internet Governance Forum in Egypt, a representative of the European Union stood up and said, “We need a right to obliteration.” You need a right to sweep clean your electronic record. And not many companies are offering that yet, but certainly consumers, in many cases, want that.

SPEAKER: We announced yesterday that after six months with the Bing, with our search engine, we’ll completely obliterate the IP address. So, you know, I do think it’s an appropriate question and it is a good part of the conversation.

MR. ATKINSON: Let me just add on this point, to me it’s a little sort of disingenuous people’s attitudes towards a lot of this, I think, is I’m getting this thing for free and I’m demanding my rights. You know, go buy a server --

SPEAKER: This is America.

MR. ATKINSON: Yeah, this is America, and if you want rights, buy it. You know, the company is giving you these things for -- unbelievable amounts for free. I mean, I look to use the example of Google Mail. I think it's -- what are you up to now, 7 gigs or something like that, and, you know, I use this example that providing that amount of storage in 1995 would cost about $13,000 per person. And so, you know, Microsoft has the same kind of product, all these companies, and they're doing it for free. And yet, I'm demanding that they be liable and that I can sue them and make a lot of money and that they have -- I just think we have to be realistic about it. If you want that kind of service, go buy it.

MR. WEST: Okay, I think we have time just for one last question, so this woman in red right there.

MS. GRANT: Hi. Susan Grant, Consumer Federation of America. I should just preface my question by saying that I'm tired of this argument that if something is free; it means that you have to agree that anything can be done with your information. And my question is should there be some legal limits to what cloud providers can do with your information, limits in terms of the types of information that they can use or the purposes for which they can use it?

MR. ROCHELLE: So, for the record, that was Rob Atkinson, I believe, not Jonathan Rochelle, as part of Google. I do believe that. We’re offering it for free, but I think it would be disingenuous for us to say that that means we can do anything we want. You know, I think that is what privacy policies are about, to try to clarify what we will do with identity information, what we will do with private information. That PII, as we know it -- Personally Identifiable Information -- is a critical part of offering that service and for people to understand what they’re getting. That just now expands. And now with phones it expands to location data. You know, that’s private. I don’t know everyone to know where I’ve been. And it is very important, I think, to offer not just the controls back to consumers, or I should say not just the transparency, but the controls and to give as much as possible.

The difficult thing we face is that there’s a balance between controls and complexity. The more controls and the more transparency, it becomes too complex for a consumer and they do start diluting in their mind what these things mean. They click through them, you know, they click though the terms because it's just too complex. I'll just trust it. And the balance between the desire to share information and the desire to keep it private, those two things are at tremendous odds today. I mean, you can see it with all the news about Facebook's changing their terms and it's immediately the top story. It's a huge influence on people, but I do think that the transparency at a detail level is useful.

SPEAKER: I think that, to me, your question really just calls again for why we need a more comprehensive privacy law at the federal level in this country, so that there is an opportunity to get a national body of law that answers these questions.

Now, I would take some of what you describe and I'd probably put it into two categories. There's one category where people might say there ought to be a law that ensures that no one can get that information or do anything with it if they have it or use that information in a particular way and, you know, there are certain areas where there is international consensus on this because of the degree to which privacy laws came out of Europe. For example, the European privacy laws have long said no one can ask what somebody’s religion is and if you happen to have that information, you’re not able to do anything with it. And I think that people of the United States would probably say that makes sense in our country as well.

There is a line that then needs to be drawn between things where people would say no one should be able to do anything with that information and another category where people might say, you know, we’re comfortable having people make different decisions, but we want to ensure that if we’re then leaving that to the marketplace, the marketplace really works. And the marketplace cannot really work unless there is transparency, unless there is information about what people are doing, it is provided in an understandable form and in a form that then enables, I’ll say, the Consumer Reports of the world to then go to work and really educate consumers about what their choices are.

You know, if I analogize to automobile safety, you know, I think one can see some similarities. There are some areas where the government says there's some standards that they want all car companies to meet and there are other areas where, you know, we all say let's have competition between the automakers on airbags and let's show that we care about airbags as consumers because then when we pick up Consumer Reports, we're going to get an article that compares the different offerings of the different manufacturers. And ultimately, I think, we'll be well served if competition in the cloud has some of the characteristics that we're more familiar with in other marketplaces that are obviously important to consumers.

MR. ATKINSON: Just to add to that, to clarify my point, I hear what you're saying is that you expect to use the car analogy that every car be a Volvo, and Volvos, I guess, are safe. That's what they say. They're probably safer than cheap cars, but if we made every car a Volvo, we would basically mean that there are lots of people in the U.S. who won’t be able to buy a car because they can’t afford a Volvo, so what we have are minimal standards. You can’t buy a -- what is the -- I guess you can’t buy a Nano in this country, thank god, the Indian car, because they’re $300 cars that wouldn’t pass safety in the U.S., but for India they have a (inaudible). So if we have the sort of gold standard on all of this, then we essentially make the cloud unaffordable. So, I think there’s a fine line between some basic standards and protections and this sort of gold-plated thing. If you want the gold-plated thing, buy it.

SPEAKER: We have a tendency in our industry to use analogies because they’re easier to understand and probably overuse them because then they break down. But at the risk of going too far, I do think that there is a little bit there. I mean, we don’t say that every car has to have all the characteristics of a Volvo. We do say that every car has to have seatbelts. And I think in a similar way we’ll find for the cloud that there are certain standards that are minimums that everybody should adhere to and then there are other areas where we actually want to encourage innovation and competition through a very vibrant marketplace.

MR. WEST: I think all this demonstrates that analogies and metaphors are the most dangerous aspects in public discourse.

But I want to thank our panelists, Michael Nelson, Rob Atkinson, Jonathan Rochelle, and Brad Smith for your participation. Thank you very much.

* * * * *

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