THE BROOKINGS INSTITUTION

PRIVACY AND SECURITY IN THE CLOUD COMPUTING AGE

Washington, D.C.
Tuesday, October 26, 2010

PARTICIPANTS:

Featured Speaker and Moderator:

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

Featured Panelists:

GREG NOJEIM
Senior Counsel
Center for Democracy and Technology

MARJORY S. BLUMENTHAL
Associate Provost, Academic Affairs
Georgetown University

ALLAN FRIEDMAN
Fellow and Research Director, Center for
Technology Innovation
The Brookings Institution

IRFAN I. SAIF
Principal
Deloitte & Touche LLP

HARRY WINGO
Senior Policy Counsel
Google

* * * * *

P R O C E E D I N G S

MR. WEST: I'm Darrell West, vice president and director of Governance Studies, and director of the Center for Technology Innovation at the Brookings Institution. And I would like to welcome you to our forum on cloud computing, and this is our latest in what has now become a series of forums and papers on cloud computing.

And today Alan Friedman and I are releasing a paper on privacy and security in regard to cloud computing. Hopefully you've picked up a copy from out in the hallway. If not, you can get a copy after this event.

We all know that security has become one of the hottest button issues in cloud computing. There's a realization that as we put more information, data, and services online, we need to take steps to assure that privacy and security are maintained.

Now, some of the threats that are coming up are not new. These are issues that we've seen in regard to desktop computing and laptop machines, as well as in the emerging smart phone market. For example, compromised passwords. You know, we still know that there are people who use the name of their cat or their dog as their password. Now, you know who you are, you're out there. According to surveys, a significant number of Americans still do that or some variation on common words like that. That obviously creates problems regardless of whether you're talking about desktops, laptops, or access to cloud platforms.

Trusted insiders who misuse their position or disgruntled employees, obviously the human factor in cyber security and maintaining privacy, is a big problem.

Now, with some of these challenges we should expect them to get better with time and experience. Some cloud providers are starting to incorporate new encryption techniques in order to safeguard their networks; others are using network auditing tools as a way to protect consumers and businesses. We're seeing backend fraud detection techniques that should improve as we get more experience with data and more users; companies will learn where the greatest risks are, where intruders seek to gain unauthorized access, and the best way to protect confidentiality.

However, there are some issues that won't go away on their own and that do need to be addressed in terms of policy as well as operational changes and this includes issues such as transparency, legal interpretations that are coming out of various court cases, and some of the international risks that we're starting to see just as different nations start to engage in more protectionist acts in regard to the cloud.

To help us think about these issues we put together a distinguished group of experts. To my immediate right is Allan Friedman, who is a fellow in Governance Studies at Brookings and research director for our Center for Technology Innovation. Allan joined us October 1st from Harvard University where he earned his Ph.D. in public policy with a specialty in technology policy and cyber security. Harry Wingo is with us today. Harry is senior policy counsel at Google. Greg Nojeim is senior counsel at the Center for Democracy and Technology. Marjory Blumenthal is associate provost for Academic Affairs at Georgetown University, which to me would seem like that's a full time job, but somehow she also finds time to do technology work on the side. And then our last panelist is Irfan Saif, who's a principal at Deloitte & Touche, specializing in cloud computing.

So, we'll start with Allan. Allan, what are the issues that won't go away, and how should we address them?

MR. FRIEDMAN: Thanks, Darrell. So, first I just want to say, this report is not meant to be the most comprehensive piece in cloud security. There are a lot of people talking about this. Nor is it meant to be incredibly technical. I'm happy to talk about some of the technical details and some people on this panel are also incredibly equipped to discuss them. But the report is meant to highlight some of the key systematic challenges that we worry may not be addressed as the market will evolve.

Some things, I think, are going to get better. So, for example, most cloud models, whether you're using software as a service or infrastructure as a service, have some centralized control manager or delegator or hypervisor, which makes a very attractive target. And we assume over time as attacks come and the security models grow, this will get a little more secure. But there are certain systematic risks, because after all, much of security is an economic problem, it's an organizational problem; it's a human factor problem.

So, what are these in the cloud environment? One of them is this question of control, what economists call a principle agent problem, where if I make Darrell responsible for securing all of my data, Darrell's main responsibility is to operate his business, and that may not be in complete alignment with my complete priorities about what I would like to happen with my data. And the CIO perspective is to turn over control of the data and control of the IT system to the provider, and thus if something goes wrong, it is no longer the CIO's fault, it is now the provider's fault. So, how do we make sure that we have an environment where we have the risk models aligned properly? Another example might be with the privacy preferences for the user versus the long-term priorities of the provider in terms of dealing with law enforcement. They may differ. How do we align these incentives so that everyone works together?

Darrell talked a little bit on certainty under the law. One, how do we make sure that the agreements that are made with the providers are enforced and are more clear? Because currently there's a lot of ambiguity in these agreements and we haven't really seen any test cases about enforcing them. Some of the lawyers on the panel can talk more about that.

There are strong international concerns. The U.S. has a very interesting position where we are very concerned about other nations accessing data both from government agencies, also private actors who deal with the government as well as private actors, but at the same time we're reluctant to adopt strong regulations as the EU currently has, which would impose probably a fairly high burden on the way business is currently practiced.

And there are residual problems with access, control, and authentication, which span a variety of IT policy concerns, but how do we know who is doing what? And moreover, if we're trying to do auditing, what does actual proper use look like? We don't have a clear model for that.

So, we make some recommendations in the report. The first is transparency, this idea that it is very important for potential clients and actual clients to know what is happening to their data inside the system. We need to understand interruptions of service. We need to know breaches of confidentiality and privacy. We need to understand how the protection is holding up and we need to know what those protections are. So, it would be interesting to hear later the panel discuss some of the costs and tradeoffs in broader and deeper transparency, but ideally we'd like to have some standard models for transparency that would allow a potential firm to evaluate a number of different providers or an agency to evaluate different providers for whatever it is they're looking for and actually compare them along dimensions of security.

Why? Well, the second recommendation we see is competition is going to allow a greater rise -- a race to the top for security. Why do we need competition? Again, going back to our CIO who's interested in maximizing their own risk posture, actually giving them the incentives to say I had two options and I went for the one with greater security, means, one, we need a way for a vendor to credibly assert that they have better security than someone else, but also it allows this provider to sort of take advantage of other built-in incentives to fiduciary roles, et cetera, et cetera.

So, we'd like to see security as a differentiating service. Part of that component we talk about in the report is the need for data exportability, the idea that if you're not doing a good enough job, I can take my bat and ball and go somewhere else. And part of this is preventing lock-in, very important to security. Also talk about the purchasing part of the federal government. Now, having policy to promote competition is a fairly thorny issue. It'd be interesting to talk about some of the ideas there.

We need a better understanding of access control. We talked a little bit about that in the report. And integrating the operations side of the business with the IT side of the business to get a better understanding of risk posture. And finally, on the legal side, and I'm sure some lawyers will also talk about that, clarifying a number of issues, both in terms of the contract, but also federal regulations such as the Electronic Communications Privacy Act, ECPA, and the Computer Fraud and Abuse Act, both to deter wrongdoers, and also make sure that people understand what the privacy is of their data as it leaves a local environment and moves to the cloud.

MR. WEST: I like the optimism there, the race to the top on security. Now, that would be a virtuous cycle if we can do that. Harry, how should we think about this area? What do you think we need to do in terms of transparency, user control, privacy, or other aspects of this?

MR. WINGO: Thanks, Darrell. I'm Harry Wingo. I'm policy counsel with Google. Thanks to each of you for your interest and thanks to you, to The Brookings Institution, for the chance to talk about cloud. And I think what we need to do -- a lot of it we're already doing -- first off, cloud, there's a lot of confusion about the term. I like to tell people it's the Internet, so cloud computing, it's Internet computing, but there's a change. What's different or what's evolving is now you have better access through -- you know, more access to broadband networks. You also have interoperability; the portability of your data is very important, but you also have storage on a scale and at a price point that has never existed before. All these things are changing, but as you -- it's really having anytime, anywhere, from any device access to the Internet, which is really important.

So, as we go into that, of course there are very important questions about privacy and security. As far as the benefits go, they're a lot of the benefits that we know have been there from the Internet itself. It's been so important for so many social, political, economic reasons, but for privacy and security, at Google we like to focus on transparency, control, and security. Transparency in the sense of how do users know what's going on with their information? And so we continue to try and provide tools for users that give them, you know, awareness of what's going on with their data, like, for example, we introduced a dashboard that lets you look at what's going on with the different services you're using at Google. And user interfaces are really important in this area, trying to make it intuitive, trying to make it friendly, something that you can understand. So, transparency is important, but also transparency in the sense of government, in the sense of what are the rules and regulations, and a lot of this is being developed. At Google we think that for the United States side of this it would be great to have -- you know, if we're looking at different things we could do with privacy regulation, just to have it more centralized in the sense of -- a federal sense, and, you know, a lot of that discussion is going on and we support those discussions. Globally, it's very important to have certainty and to make sure barriers aren't being put up with respect to the Internet which could lead to Balkanization and all kinds of problems that could slow down not just commerce, but also free expression.

On the side of having users be able to control what's going on with their information, that's important on the privacy side, but as well we need to consider security and making sure that we're continuing not only to make it easier for users to keep themselves save online, but also to make sure that we're contributing to the wellbeing of the Internet as a whole. So, at Google, we've done things on the security side, for example, like allowing your Gmail setting to HTTPS so you have secure, encrypted e-mail communications as a default. We also have secure search that we recently rolled out. And so, as you're going online from anywhere, any device, it becomes even more important to make sure that you have options. And the market, there is a market incentive for firms like Google and others to make sure that we are protecting users, we're communicating that. And as far as regulation, there are points, places where, of course, the government needs to keep watch over this, but it's always important to remember what innovation can do in this space. And so innovation is pushing things forward and, you know, it's give-and-take. We're learning, we continue to learn, and so we also collaborate with other companies, we collaborate with public interest groups, and of course with the government on this issue.

And so I think cloud, the benefits are tremendous. Last year we put out a report -- or actually this year, earlier this year -- on the $54 billion worth of value that we’ve put into the United States economy in different states, and that’s an economic impact report that we’ve done. And a lot of the cases are small businesses and how they’re using the Internet, and so cloud computing has implications for commerce and it’s just another tool. So, we’re moving from a world where you have all of your stuff just on one box and you pour software into that box and then you wait a while, maybe a year or two, and then you get something else to put in that box, to a world where you’re having continuous updates and you’ve got a machine, it could be your smart phone in your pocket, it could be a tablet, it could be your desktop, but you’re not locked -- or kind of like tethered to just one device, one option. If you’ve got a smart phone that’s enabled with Android, for example, you might as well have a Google Data Center in your pocket.

And so cloud has a lot of exciting opportunities, things that its bringing to the hands of users, and everyone, government also, is also benefitting from all of this. But we also have to really -- we are looking very carefully at the security side and making sure that we respect privacy.

Thank you.

MR. WEST: Okay. Thank you, Harry.

Greg, you have suggested that our laws are out of date and we need new legislation, so what should we be doing in this area?

MR. NOJEIM: I think we’ve got a lot to do to update the laws to accommodate this growing use of cloud computing. And for people who think it’s a fad and it might go away, think again. I mean, you’ve got the company that has specialized in word processing on local PCs offering in its latest version, Word, the opportunity to store stuff locally or store it in the cloud. If Microsoft is going to the cloud, I mean, just think about what that means for what other companies are doing. A lot of information is going to be moving to the cloud because there’s so many advantages of cloud computing: remote access, collaboration, you can reduce your IT costs, it’s going to be more efficient, profitable, and convenient. So, I think there’s a certain inevitability of more movement to the cloud.

But there’s just a lot of questions that we have to work through and some policy decisions that we have to make to accommodate this move to the cloud. One of the threshold questions is, what law applies to data stored remotely? Is it the law where the user is? Is it the law where the provider is? Is it the law where the data is? And I think it’s probably, in many cases, going to be the case that it’s the law where the data is. And if it’s the law where the data is, think about how different the legal regimes are that govern privacy of data. Think about Europe and the rules that providers have to abide by for data that they store in Europe and how different they are for the rules that apply here in the United States. That’s one issue. And it’s influenceable, so for example, it could be the case that the contract that a person signs with the provider of cloud services specifies where the data will be stored and thus giving some indication about what rules are going to apply.

Within the United States, we have to think about some of the privacy laws that will govern how that data can be used by the provider or accessed by the provider or even whether the data can be stored with the provider in the first place. And I want to give a special shout out to Bob Gelman over in the corner there. He did a paper called “Privacy in the Clouds” for the World Privacy Forum last year, and I recommend it to you because it starts exploring a lot of these privacy issues.

So, there could -- if the data is medical records, for example, HIPAA, the medical records statute, requires that there be a business associate agreement that’s going to govern how that cloud provider can use or access the data. Some tax laws may make it so that tax preparers can’t store the data in the cloud because they prohibit certain disclosures to others. And then we also have to think about government access to data stored in the cloud. This is an area where CDT, my organization, has worked very hard to increase privacy protections. Here’s the problem: There’s a couple of cases dating from the ’70s -- *U.S. v. Miller*, and *Smith v. Maryland* -- that throw into question whether even content stored by a third party business is protected by the Constitution. Do I have a right to tell somebody to whom I’ve entrusted data that they can’t disclose it? Do I have a Fourth Amendment right against the government when it wants to get that data from the third party? These cases throw that right into doubt so you’ve got to rely on statutory protections. The key statutory protection is the Electronic Communications Privacy Act. When was it drafted? 1986. It has been updated in little ways, mostly at the request of law enforcement, but hasn’t had a good look at on the privacy side since it was adopted.

So, it has a strange construct, it says that if you have -- if you’re communicating the data in real time, there’s a high level of protection, but if you’re storing the data with a third party, there’s a very low level of protection, law enforcement can get it with a subpoena based on relevance. That is something that we’re trying to change. We’ve worked with companies; Google is one, in the Digital Due Process Coalition, to try to seek legislation to make it so that all content stored remotely would have to be accessed only with a warrant based on probable cause.

Another issue to think about when it comes to cloud computing is the effect of the disclosure to the cloud provider on other rights that a person might have, like legal privileges. If you sign a contract that allows the provider to use the data or access the data for some purpose, have you waived your legal privilege if you had it in the first place? I mean, say it's a law firm trying to store data with a provider and it wants to claim a privilege -- or it wants the clients to claim a privilege over that data, there's some question about whether it would continue to apply. And also think about bankruptcy. Say the provider goes out of business. Your data stored with the provider is an asset that the court will have to deal with in the bankruptcy proceedings. What happens to it? What are the rules?

So, I've said that the law needs to keep up with technology and that we're working for changes in the law. There's other people who think that the law needs to move in the wrong direction when it comes to protecting the privacy of data, and I'm referring specifically to some proposals that the FBI has put forward to extend the rules of the Communications Assistance for Law Enforcement Act and to make it more difficult to freely use encryption. And the reason it's important for cloud computing is that the last thing that you want is for your provider to have to build in a back door to give the FBI access when that back door can be exploited by the hackers who you know are going to be going after the data that's stored with third parties, and the ways that key escrow would have to be implemented would also create some new vulnerabilities that we would want to think about very seriously. Thank you.

MR. WEST: Thank you, Greg. Marjory, you wrote a paper entitled, "Is Security Lost in the Clouds?" and you talk about the cloud as a "platform for malice," which I like that phrase, it's very catchy, but what do you think are our biggest perils? How do you think the cloud ecosystem should evolve? And do we need new approaches to data and data storage?

MS. BLUMENTHAL: So, like Greg, I looked out and I saw that there was a certain kind of inevitability to the rise and the spread of the cloud. There are many appeals, the economics argue for it, we're definitely moving in that direction, so it's just a matter of the way that I think that I try to say, well, wait a minute, what could be some of the issues, and started to talk with a number of experts, read a lot of literature. In brief, in terms of the cloud as a platform for malice, Greg had talked in terms of different forms of interactions with providers. I try to outline in that paper a number of ways in which providers could in fact be a source of harm, but also fellow users could be a source of harm. So, on that last part I know that the paper that you wrote with Allan cited the (inaudible) paper and that is a great illustration about how the technology of virtualization and co-tenancy, if not implemented effectively, could allow the smart user to exploit a particular location on the cloud to get access to somebody else's data.

There are ways to counter that, but that does require a certain amount of responsibility on the part of the provider to act on what we're learning about the technology. You, I believe, also cited the Anisa work from Europe, which is this incredible, overwhelming catalogue of risks, in fact, it's sufficiently overwhelming that you could understand a lot of users not necessarily bothering to go through that advice, but one of the points that they make is that since so much crime has moved to the net in all of its forms, which I think is why we have this new discussion about Calia that Greg referred to, it's reasonable to assume that providers will increasingly be targeted by organized crime. So, even if the provider isn't intentionally doing or negligently doing something that isn't a great idea, social engineering and other appeals to personnel may still exist.

So, that's just some of the platform for malice concern. All of those concerns, I should note, are really focused on the public cloud, that when you look at a large enterprise or the government operating its own private cloud, then the discussion is, in fact, something different.

As I looked out and tried to think about the future, there were a couple issues that I wanted to flag. One is this notion of a cloud ecosystem. So, it's one thing if you are a user of the many offerings of Google that you might expect to be able to have some interaction among those applications and make use of the fact that in a way Google may be large enough to be its own ecosystem, but as we think about different kinds of data that you might have stored on Google or Amazon or Azure or somebody else, what about the possibilities for interacting and exchanging among those different clouds? So, there's some work on standards for that. It's hard to say where that would go. You have your partisans for openness who want it to be fully open and then you have some commercial realities that may argue against that. But I think that the ecosystem is interesting not only for the functionality benefits that one might get, but also that if it's hard to assess risk in one cloud provider's domain, it may be even harder to assess risk when you're talking about an interconnected cloud construct.

So, all of this kind of, you know, evaluation of what the options were, led me to wonder whether we should not be thinking about different ways to organize our information, that is, it may be that we're going to have the cloud, it is the way to go, it gives us lots of benefits, it's not necessarily the case that we want everything to go to the cloud. And so being more intentional about what we put where, I think, requires some thought. And also to think about the lifecycle. Again, Greg referred to the history of ECPA and the history of looking at whether data was in transit or data was at rest. Well, if you think about data as having a lifecycle that includes many kinds of moves and there may be more risks during the moving stages, you might want to make different choices about what you move or how you move it, and what you keep to yourself and what you give away, recognizing that if, in fact, you keep data to yourself, you have to make sure that you do protect it adequately.

I did want to respond -- or should I wait -- to a couple of things that I've heard? Okay.

So, the issue of transparency, I, in other contexts, have often called for transparency and disclosure in the notion that if companies, organizations, did make clear what it was that they were doing, then consumers could make better choice. So, a question I would have for some of my colleagues on the panel is, what does it mean for transparency if you're transparent about terms of service that say, I, the cloud provider, am not going to be responsible for your data, which you can find for some of the major providers? So, it's transparent if you bother to read the terms of service, but I'm hoping that this future with more involvement of the cloud, may involve a different division of labor, a different evolution of risk sharing, or at least more clarity and transparency about what risk sharing is all about.

I guess I will leave it at that for now.

MR. WEST: Harry, she was looking at you when she asked that question, so, before we turn to Irfan, did you want to respond to that?

MR. WINGO: Yes, I'll respond very quickly. As cloud continues to evolve, in terms of service we believe in data portability, and so that really goes to choice. And one of the things that Allan mentions in his paper, which I think is a great point, is about competition. And so the discipline of the market will definitely apply to consumers being informed, realizing what the terms of service are, and you will see different models develop as far as what you want to happen with your data, the level of protection, and the options that you have.

We have a general service Gmail, but we also have contracts that we do with business, and so they're -- so, I think choice is really important and also the discipline of the market, but you have to have that interoperability. We've got a cadre of engineers that have been working on portability with respect to cloud services. WE call it, no kidding, the Digital Liberation Front. We've got -- there's a raised fist -- raise your fist, please -- that actually we -- it matters to us because we realize that this will lead to competition in the cloud, it's absolutely important, and as we discussed -- I said I'd have a short answer -- but if you can move your data out, if competition means you're just one click away, that imposes a discipline on us with respect to terms of use and all sorts of other things.

MR. WEST: Okay, Irfan, I want to bring you into the conversation. There are different types of clouds, Marjory has mentioned the difference between public versus private clouds. I'm just curious, in terms of, you had mentioned in our conversation before the panel started that we needed policies that are more cloud-centric, so I'm just curious what you mean by that? Do we need new standards? What needs to get done?

MR. SAIF: Sure. Thank you, Darrell. So, my perspective, everyone, is really going to be from -- a little bit from the trenches. My role as a partner at Deloitte, they specialize in security and privacy, and so a lot of what I do is really helping CIOs and business unit leaders and others devise and execute security strategies for their environments, and so that includes, of course, adoption of cloud.

And so, as I've been working with these folks, there's really a number of challenges they continue to face. Certainly a lot of them are not new. A lot of them are the same challenges we've been seeing for a number of years. I think there's many entities that struggle today, particularly on the commercial side, with even some of the more basic blocking and tackling kinds of security challenges, and so I would say that some of the -- some of the changes that cloud brings, broadly speaking, you know, some of them require a little bit of different thinking than they've applied in the past. I certainly think that in many instances certain cloud solutions can be very helpful in improving the overall security posture of an enterprise if they use them appropriately.

So, I think there's a lot of thought to be provided there. Ultimately, you know, with respect to cloud, Marjory talked about public versus private, I also think there's a need to distinguish a little bit in terms of software as a service, versus other types of cloud solutions, so platform and infrastructure as a service, where potentially there's more handoff, there's more collaboration, if you will, with your particular cloud provider, and particularly where in those instances there's more responsibility on the part of an enterprise in terms of managing some of the security attributes of what they build in the platform, or in the case of infrastructure, there's more responsibility as to how they can figure and deploy those infrastructure technologies. So, you know, they have basically more responsibility down the stack than they do with something like a software as a service solution where it's much more constrained.

So, I think there's some consideration there to how you delineate. So, when we talk about cloud, using the term, of course, very loosely, it actually means, of course, a number of different things.

The other thing to realize too, I think a lot of my co-panelists have already said this, is, you know, there's no question that there's huge adoption and so I deal with very large enterprises, I also deal with a lot of small businesses and startups and there's huge adoption across the spectrum in terms of using cloud services for a variety of things. I've got clients that do everything from software and application development, they use productivity tools, e-mail collaboration, even enterprise resource applications like financial tools in the cloud, and there are some that have said, you know, we're going to build our own, so they're going to build a soup-to-nuts private cloud. So, there's everything in between, and so I think, you know, we need to take that sort of element into consideration as well when we talk about these issues and challenges broadly.

I think that, you know, in the paper that Darrell and Allan have put out, put out a couple of great thoughts and one of them is really the idea that hen we think about security and privacy, and we're talking about confidentiality, integrity, and availability, it is important to add the three additional elements that they've put in there, you know, as it relates to accountability, as it relates to assurance, and as it relates to resiliency, right. In my view, we do need to think about cloud -- when we talk about security and privacy, we do, to some extent, need to broaden the conversation and the enterprise to talk about risk, and what does it mean to mitigate risk appropriately, whether that's IT, whether it's the business, whether it's -- you know, I think you mentioned tax earlier, right, whether it's tax or HR or finance. You know, across the business there are implications and I think one of the very interesting things that I see day-to-day, is that security is often tackled in a siloed manner, and I'm sure many of you see this too in your own environments, and I think one of the challenges with cloud is that it's very easy to go out and procure potentially significant cloud services without a lot of people in your environment knowing about it. Right? You cut through a lot of the procurement, you cut through a lot of the processes that have been put in place and, you know, I've encountered a number of situations even very large clients where IT or other leads have not known that a business unit has gone out and procured certain cloud services and made certain decisions, and part of the challenge is that those decisions may be contrary to, you know, the corporate stand or enterprise policy, right, and so if there is an incident then you've got some -- you've certainly got some challenges there to deal with, right, and so I think part of it is making sure that, you know, the broader conversation we're having today around policy and around governance, I think that needs to -- there needs to be a sort of micro focus at the enterprise level on what is your strategy, what is your governance framework, what are your policies to define and manage how you're going to assess risk in your corporate environment, how you assess risk within your extended -- I'll call it your extended enterprise, right, your supply chain, because today very few entities really just do business on -- within themselves. There's a lot of business partners, there's a lot of third parties, there's a lot of, you know, different solution providers that are in the mix, and so how do you apply those standards consistently across, and I think that, you know, it sounds simple, but in practice a lot of companies struggle with that today.

So, I would just say that, you know, ultimately all of that is going to be important, understanding how companies assess their risks today, and are those risk assessment processes really going to be able to embrace all the new risks or additional challenges that cloud and other similar technologies provide is going to be key. And I think the other thing is, today, when you look at the environment that businesses are operating within, you've not only got things like cloud computing, you've got, you know, a whole bunch of changes going on. This cloud is a lot of social media and collaboration, and of course, as Harry and I were talking offline, cloud is all about collaboration.

So, you've got those solutions, you've got all the social media and other collaboration tools, you've got mobility now, and end uses enabled in a way that you never had before, and so I think to some extent your typical enterprise doesn't have as much control as they used to and, you know, that's something that they've got to accept, but I don't think that necessarily the policies and the frameworks and the tools that they use nor necessarily the skill sets of the people they have, are up to speed with all of those changes.

So, I'll leave it at that, Darrell.

MR. WEST: Okay. Thank you very much. I'd like to throw out a couple of questions for our panelists and anybody who wants to jump in, can, and then after that we will open the floor to any questions or comments from our audience.

First of all, in terms of moving forward, I mean, Greg was mentioning some of the legal rulings that have tended to treat remotely stored information differently than personally stored information, so I'm just curious, like the last major legislation was the Electronic Communications Privacy Act, 1986, 24 years ago. Obviously a lot of things in the digital world have popped up since them, so I'm just curious what our panelists think in terms of how we should actually change ECPA? How should the technology community work with law enforcement to find a compromise on some of the issues that divide those communities? And how do our panelists see this issue playing out post-election with likely republican gains in Congress?

And then the second issue that I'll put on the table, or this may be like the fifth question, I don't know, is in terms of the cost curve, and what it looks like for additional security features, because, you know, it's easy on the one hand to call for more security. We all want more security. I'm just curious in terms of cost considerations, how much are we talking about for what level of security? Anybody wants to jump in.

MR. WINGO: I'll actually jump in with the second question first on the cost curve. A lot of the security enhancements that we're providing for cloud services are free, which is kind of great for consumers, not free to us, but we were able to absorb this cost because of our approach to how we do computing. We were born in the cloud. Our flagship product, you know, for delivering ads, it's over the web, you access it through a browser, and so we have looked at continuing to make changes for security and so that means that there's a choice, though, of course, but I think everyone has to move forward on this, make the decision for themselves what they're going to do, but the cost has to be weighed against the benefits that you have for collaboration, for example.

Outside of our advertising platform we've got Google Docs, that's a great case for showing tangibly what cloud collaboration can mean.

Right now, how many people here still have, like, say, a system where you've got your documents stored only on your one computer and you have to e-mail it to yourself? Raise your hand. Okay. How many people here have used Google Docs, if you raise your hand? Okay, great. So, the difference is, with Google Docs --

MR. WEST: Or other products.

MR. WINGO: Or other products. So, collaboration on the cloud means you're able to open that up no matter where you are. If you have web access, you have access to your document, and we've moved forward to make sure that web access is secure. We actually just recently announced that we're doing two-factor authentication which means you've got a password, something you know, but also something you have, like you can actually have a one-time code sent to your cell phone or your smart phone, and you put that combination and you log on. You've got access to the document, which is shared, you could be anywhere in the world and I can actually see my teammates putting edits in that document; we're all in the same sheet, literally, because it's up in the cloud. So, that's collaboration. The benefit of that -- and so the cost, if you've got these companies like us where we've got this infrastructure in place, or actually these facilities, if you will, one of the largest private super computers is one way to look at the different servers that we have, but they're actually data centers that are spread throughout the world, and so the cost of doing things -- you have to consider the scale, and so -- but there's also the cost of not doing it. If we don't continue to move forward, you won't have consumers continuing to use these applications and there's this pressure in the market, people want access, they want it to be convenient, and they want to be secure.

So, I'll jump in on that one. Greg will have a lot more to say on the second question.

MR. NOJEIM: So, say you're using Google Docs or another similar service and you're wondering, well, what I'm doing here is pretty sensitive. What are the rules for, say, law enforcement access to that information? Court order required? Probable cause? They have to know that I'm up to no good to get that information and the answer is that for something like Google Docs, they need a subpoena, and that means that the prosecutor writes out a document, there's really no vote at a grand jury or anything on whether this subpoena should issue, and the subpoena is sent to a third party and served, you get notice, but it's on a mere relevance standard. There's no judge saying, you know, I think that Greg's up to no good. I've got probably cause, I've got strong evidence that he's up to no good, and therefore I'm going to issue a warrant to get that access. No, it's just a subpoena and there's no judicial -- there's really no judicial oversight.

What ought the rule to be? Say that same document I was creating on my own PC. How would law enforcement typically get it? They would -- they can subpoena the PC. They typically don’t do that, though, because then I get notice. What they typically do is they serve a warrant and they have to go in front of a judge, prove probable cause, and then they can get my PC and the information in it.

Why should there be discrimination between those two platforms? Our answer is that there shouldn’t be, that the law shouldn’t discriminate in terms of privacy between what I store locally and what I store remotely, particularly given that things are moving to that remote storage place.

So, our view is that the law has to move with it and that probable cause ought to be required.

One other example of a way that the coalition that we’ve put together is dealing with these discrepancies in the law, you send an e-mail, think about the lifecycle of an e-mail. You’re creating the e-mail on your computer, and say you’re using Gmail to send that e-mail, or another similar service. While you’re creating it, what’s the rule for law enforcement access? Subpoena. You hit send, it’s in motion, it’s at its highest level of protection at that point. Do they need a warrant? They need more than a warrant. They need to show a judge that there’s not a good way to get that same information except getting it from the provider. It’s kind of like a last resort requirement. They need a super warrant to get that. It lands at the inbox of the person you’re communicating with and it’s also stored with the provider. I mean, the provider has it as well. What’s the rule then? For the first 180 days, there’s a court order required. After 180 days, it’s a subpoena again. Why? Why would that be the rule? I mean, the e-mail that I save the longest is the most sensitive to me, it’s that message I didn’t know how to deal with, it’s really that very sensitive piece of data. I'm going to save that longer, and yet it's at the lowest level of protection. You know what's getting the highest level of protection? My junk mail. My junk mail, because the FBI says that once I open it, it loses the high level of protection, moves back into the subpoena land, and I never open the junk mail. So, it's at the highest level of protection until it reaches that six-month rule when my junk mail too is least protected.

MR. WEST: So, does that mean we should be opening those Viagra ads?

MR. NOJEIM: You know what it means; it really means that we need one clear rule that communications content is going to be protected by a warrant requirement and probable cause. That's the one clear rule that we're -- one of the two clear rules that we're trying to promote in this Digital Due Process Coalition.

MR. WINGO: And Google's also part of that Coalition and very much agree with what Greg said because, as you move forward to what expectations are for consumers, I mean, we use these tools increasingly and we have to make sure that we keep up with technology and what consumers expect, and a lot of people don't realize that those lower levels of protection vis-à-vis government access to some of your most personal communications is there, so we think that ECPA reform and what the Digital Due Process Coalition is supporting, we're on board, we're part of the effort.

MR. WEST: To our other panelists, what do you think we need to do in terms of ECPA reform or other actions?

MR. FRIEDMAN: So, I actually can speak more to the cost curve side of things, and I think Harry's right, a lot of security components really are -- you have a single investment that you then can apply to all of your customers on the provider's side.

But some of them, I think, are a little more cost intensive and two examples are, one, just the idea of security over time, so systems as they are exposed to the attack surface will degrade in security, just as the attackers learn more about it, as more public information comes out, they are more at risk, and so it is an ongoing cost to the provider to constantly monitor incoming threats, revise their own platform, and that is incredibly difficult to do if you have to make major changes on a system that is live and that is supporting users. It's the proverbial fixing the plane while it's flying.

Another component on the cost curve actually applies to the client, and that's this question of identity, authentication, and access control, and this may not be part of the initial cost estimate for the client. They say, hey, I can get all these savings if I put stuff in the cloud, and the cloud will monitor who's doing what, which is great, except responsibility for actually identifying yourself as you come in, as you leave the organization and get what you're supposed to get, is quite tricky to do well, and requires a decent amount of time and a lot of consultation with people like Irfan to actually make sure that you're covering all these bases that you need to do, and it introduces new threats to the system, it introduces new potential for lock-in as well as additional costs.

MR. SAIF: So, I would just weigh in, I agree with that. I think that, you know, part of the challenge really becomes that security a lot of times for cloud, or even other online environments, isn't necessarily done well, particularly the first time, and I think that, you know, the way that people think about security, sometimes it's -- oftentimes, I'd say, it's a bulldog. You know, tackle some of the challenges after the fact, and I think there's a problem there. I think not doing something well obviously raises the cost too.

I think the other consideration is, you know, in the more complex kinds of cloud solutions one might adopt, where, for example, you have a hybrid cloud and you’re integrating some internal elements and you’re integrating that with an infrastructure as a service provider, and you have some infrastructure and some applications deployed in that environment. Some of the challenges of integrating all of your security between what you have on premise and what you have in the cloud, some of the challenges associated with correlating the information about what’s happening within the cloud, with information that’s happening within your environment, a lot of those challenges haven’t necessarily been, you know, well experienced on the enterprise side, and, therefore, there’s a lot of start up costs there that may not otherwise exist, and I think the other element too is a lot of the talent in terms of the people that are tackling these challenges, well, let’s be honest, a lot of them are going through this for the first time, and so there’s also a learning curve that needs to be understood there as well.

MR. WEST: Marjory, do you want to jump in?

MS. BLUMENTHAL: Well, I wanted to follow up on something that Allan had said that also related to something that Irfan had said a bit earlier, and that is that if you’re going to talk about the cloud as expressed by social media, there is some research that talks about the conflicting incentives, because there you have the providers who are offering a product that is, as Irfan said, all about collaboration, all about sharing, and it’s not always clear that the provider is going to be as vigilant in protecting privacy or other qualities, and I think that because these technologies are relatively new, and they’ve been growing so fast, and we’ve been discovering what all the good things are that you can do by sharing data, that we haven’t really worked through what security might be for something that is fundamentally somewhat public and shared. And that’s where I think we need to work on, sort of, more of the theory.

MR. WINGO: Just a thought on the cost curve, and over time, as Allan mentioned. Let's consider the security situation as it exists now with the paradigm that we're moving away from, which is box computing, I'll call it, you know, you've got your desktop. Unfortunately, the burden has been put on the user to do the patches that are required, for example. Sometimes it can take a month -- you know, something comes out in the wilds of the Internet, you're already exposed, but you may not actually be informed about your exposure until later, then you've got to take the steps to update it, and there's a lot of great work that's being done by anti-virus companies, but there are also a lot of gaps. So, one change that can happen here for the cloud is you can have a lot of that pushed out to the provider.

Google, we're rolling out Chrome OS, and so we're actually getting into netbooks, so the same way that you've seen Android, some of our code, it's open source -- that's another important thing, when things are open and you can comment on it on the Internet and it's open protocol, open source, and the web -- you know, the Internet is giving you feedback, that's an important dynamic on lowering the cost of what it takes to improve security. DOD is actually looking at that. So, on the laptop -- or, rather netbook side, and these are, you know, smaller computers, they're built for like really great broadband access, you can actually -- we're coming out with Chrome OS and the idea there is to have system hardening, to have sandboxing, to have process isolation. So, right now in box computing a lot of times your computer, something can get into it, and you actually have no window into what's going on, and so definitely for consumers, that's hard, it's hard to keep up with. So, for cloud, one of the models is, you know, if you've got these machines or, you know, you're able to write some of your data to our data centers, then what happens is Google, or Amazon, or Microsoft, the provider is providing, if you will, a digital Fort Knox that’s taking care of your data, and the machine that you have that you’re doing the access with, they can be designed to keep you out of trouble. And so user interface with security is something that’s overlooked. That needs to really be paid attention to a lot more. We get that. We’re part of that discussion, research and development, but that’s one thing on cost that I’d like to make.

Also, on the difference between public cloud and private cloud, one thing to keep in mind is if you’re connected to the Internet, some of those distinctions, if you’ve got access, you’re part of the Internet, and so, that’s -- you have to be careful about that. That’s why I also like to call this not cloud computing, but Internet computing.

MR. WEST: Okay. Why don’t we open the floor to questions and comments from the audience? So, I think we have some microphones that will be circulating. We have a question right up here.

Actually, we don’t have our microphones yet, but maybe you can ask your question and if people can’t hear it, I’ll repeat it.

SPEAKER: So, my question is about the intersection between transparency and the cost curves that Allen was talking about --

MR. WEST: Okay, here we have a microphone for you.

MS. PFLEEGER: My question is about the intersection between transparency and the cost curves. Many people who use the cloud and the Internet think that services are free, when in fact they’re really not free, that the providers are harvesting information about where we go, what we do, what we store, and selling it to other people in order to support what seems to be free, and so, as we move more and more toward a cloud model, how much transparency will there be to the user in order to enable a decision about tradeoffs between privacy and functionality?

MR. WINGO: I didn’t get your name, ma’am?

MS. PFLEEGER: Shari.

MR. WINGO: And also where you’re from or who you’re --

MS. PFLEEGER: Sure. I’m Shari Lawrence Pfleeger. I’m the research director at the Institute for Information Infrastructure Protection.

MR. WINGO: Thank you. Thanks for your question, Sharon. So, as far as transparency, this is something we care about and we want to let users know what we’re doing. So, take interspaced advertising, for example. We’ve given a tool recently where you’re able to set preferences, if you’d like, to be aware, if you want to opt out, we’ve got an enduring cookie that lets you do that, and also for all of our services to understand what’s going on with privacy, we have a dashboard that applies to Gmail, to Picasa, and all the things that we offer, and so those types of self-regulating actions by different firms is very important, and I think again recognizing that consumers should be able to make a choice to move if they want to, that’s’ why data portability is so important, because if you’re locked in, in the cloud, you really don’t have those same options, the market can’t impose the same discipline, and so we agree with you and we’re actually making steps at Google to help users in that respect.

MR. NOJEIM: Sharon, what I haven’t seen but that might exist, if somebody has seen it, tell us about it, is a comparative study, something that compares the different cloud platforms in terms of privacy, how is data being used. Do you know if one exists? It seems like something obviously needed.

MS. PFLEEGER: So, there’s a guy named Roland Trope who’s a lawyer in New York, and he wrote about a hundred page paper for the American Bar Association on whether lawyers should be using the cloud because of attorney-client privilege, and so he has -- his paper is very detailed and very good looking at terms of use from different cloud providers and what the privacy implications are across the different providers. So, you might contact him. I can give you his information afterwards.

MR. NOJEIM: Okay, just for everybody else's use, is the paper online?

MS. PFLEEGER: No. I don't know -- I saw an early version of it so I don't know if it's publicly available yet.

MR. NOJEIM: Okay.

MR. FRIEDMAN: There's, also along that line, a paper out of Queen Mary School of Law in Canada that does -- compares terms of services, terms and conditions, and also finds what you alluded to earlier, Marjory, that, you know, there is transparency, just we have no liability. Everyone says that.

MR. WEST: Okay. Other questions. Over here?

SPEAKER: I had a question. Could you discuss the various levels of privacy that are afforded by the system in different venues, and time, and use, and archival purposes, and wonder how that affected civil law and disclosure and specifically to Mr. Saif, how would you counsel your clients as far as where they should keep their data regarding potential civil suits and discovery and access as well?

MR. SAIF: So happy to start. I mean, I think a lot of it is, you know, again, don't treat this like a siloed problem, so I would imagine that most of my clients have established records retention strategies, they've got e-discovery strategies in place, and so, you know, most of those use some level of risk to determine where they should be putting that data, and so I'd say, again, you know, for them it's about figuring out, well, are you comfortable given the protections that exist, given the contracts you have with those providers, you know, are you comfortable putting your data outside of your own, you know, control, if you will? And the answer with some entities is, yes. There are some clients -- frankly, I have one client that has actually said, no cloud computing resources of any kind unless they exist in our data center. And so there’s no publicly addressable services, if you can. Now, I’d argue it’s pretty hard to manage that in this day and age, however, you know, that’s kind of the reality.

So I’d say, you know, broadly speaking, don’t treat it necessarily any different. That’s today, and that’s kind of where most of them, frankly, are going today.

MR. WEST: Okay. There’s a question.

SPEAKER: Yes. One of the benefits of the cloud is that the little guy can better access technology and pricing that used to be reserved for the big guys, and so with sales organizations kind of featuring benefits and privacy and security capabilities, and the lawyers then protecting the provider with language, are we -- like especially if brokers come between the users and the provider, are we moving into a scenario where, you know, the big guys end up with production, but little guys do not? And how can that be better addressed?

MS. BLUMENTHAL: Well, not having thought about this fully, my guess would be that this is one of those areas where we’re going to have trial and error and we will evolve a set of protection for the little guys because it is true -- I was listening to John Seely Brown last week talking about a number of startups that he works with in Silicon Valley, and the reason that they exist as ten people companies is that they’re able to use computing resources in the cloud. So, I do look at this technology as being, you know, somewhere early in its lifecycle and I have reasonable confidence that -- whether it’s case law or formal legislation or regulation, we will evolve those protections.

MR. WINGO: I had a thought on how this helps the little guy, as you said. So, Internet computing -- there's a great book by Nicholas Carr called *The Big Switch*, a great overview of cloud and some of the important dynamics, and what you said about -- this just makes you that much more effective as a business, and Mr. Carr uses an analogy to electricity hence the title *The Big Switch*. A hundred years ago, or before electricity was really rolled out across the country, individual firms had to construct their own generators and electricity source. That's what we're doing with IT right now, we're moving out of that world. And you can see the benefits that are out there, but you also need the options for different markets.

Now, for electricity, it's interesting, there's a lot of changes going on there. Consider the smart grid, and some people ask, can't we have more localized generation, and the options to choose green power or other power, but that's still evolving. On the side of the Internet -- but there's no questioning what an impact that that electricity switch -- you just plug it in and it works. That's an aspect of cloud computing that could arrive, but you need the interoperability, you need the data portability, and as Marjory said, part of having the trial and error is having that competition and the discipline that the market imposes and having consumers realize that they actually can choose someone else with just another click, that's important.

MR. SAIF: Darrell, if I could just add one comment to that. I think the other thing to realize is, for those small, you know, eight, ten people companies, and I actually deal with some of them, you know, one of the realities is that actually in their early stages a lot of cloud providers provide them far better security than they'd be able to actually do on their own. So, you know, one of the important factors for them to consider is, how can I collaborate with other entities or how can I create an extended supply chain or higher value services and how can I leverage all these cloud technologies that are there, and how can I do so in a manner that -- you know, far more cost effectively and far more securely than I could otherwise be able to achieve.

So I think, you know, the flip side is, there is a lot of immediate value to them using those services versus trying to do it themselves from a cost standpoint, and in fact a lot of the VCs will tell you that from a business plan perspective they're not willing to fund a lot of technology investment as part of those costs because, you know, frankly you can get, you know, potentially superior services in the cloud.

MR. NOJEIM: And as a final note, the question built into the assumption that there is an accountability anywhere for information security, and anyone who's been following the economics of information security will tell you that it's still a very mixed bag and it's unclear whether there is a strong accountability system built into current law.

MR. WEST: Okay. In the very back there's a question.

MR. JORDAN: Frank Jordan with the Business Software Alliance. My question is about the multiplicity -- potential multiplicity of security standards that apply to public cloud, (inaudible) of a cloud provider, they have a public cloud provider, they have multiplicity of customers, and these customers may be subject to different security and privacy requirements. You know, you think of HIPAA if it's a health care related customer and (inaudible) or et cetera, et cetera. So, now, the cloud provider may not know depending on the areas of privacy policy in terms of service what data they hold. They may be blind to it. You know, I just run, you know, capability and whatever you upload and download from my service, I don't know, but the customers, obviously, they know, and they have to care.

So, potentially those customers impose on their provider a multiplicity of standards which isn't necessarily very practical because they don't -- it's not like -- they're not all on a scale and you could say, well, the provider will just like provide the top level. They're more -- often divergent. So, how do you deal with that situation? Is it a case where maybe the provider should be able to say, well, I comply with some kind of like cloud standard for security, like SAAS70 or something like that which should really sort of be like a safe harbor for all of the others? Or, how do you deal with that?

MR. NOJEIM: It's that -- it can't work -- it can't work that way. It can't work that way because if the data in the hands of the -- I'll call it the entrusting party -- is subject to one set of rules, that party can't evade those rules by entrusting that data to the cloud provider. The rules have to follow or prohibit. Okay? They have to follow the data or they're going to prohibit that entrustment of the data with the cloud provider. It can't be the case that the cloud provider says, well, we abide by this standard and the standard doesn't meet the standard required for the sensitivity of the data that's being entrusted. It just can't work that way.

MR. WINGO: I have a thought on that as well. So, thank you for your question. We're seeing this with federal use of the cloud, for example, and Darrell had a great session on that earlier in the year. Google has gotten FISMA certification at the moderate level, which applies, really, to 80 or 90 percent of what the federal government does, and we're seeing federal clients come over so they can have all the benefits of collaboration, cost saving, increased security as well, but as Greg said, the requirements follow and you have to take whichever requirement is there for a particular customer. We will address that, and in addition to FISMA, we also have SAAS70 Type II certification for our cloud, and on the federal side we also -- you know, we announced that we're going to have the ability to, you know, make sure that the federal information is just here in the United States, which was important.

So, you know, you’re seeing market responses. I think we’re the first to actually go through that FISMA certification process, which is the law, and it can adopt, it’s flexible, and it applies to cloud computing. We got the blessing from GSA and, you know, I think that was groundbreaking and we’re proud of that. There’s other companies that are about to get their certifications as well. So, in answer to your question. Thanks.

MR. WEST: Okay. There’s a question right here on the aisle.

MR. ALTMAN: I’m Fred Altman. I just have a naïve question. You were talking about the data portability, what prevents -- I mean, how do we know that the provider who’s giving up the data to another one actually has no traces of that data left that can be subpoenaed or whatever?

MR. FRIEDMAN: So, the question of deleting data is actually quite a tricky technical question, and then when you start to build in the organizational dynamics as well as the fact that your data exists multiple places for redundancy gets very tricky. In terms of how do we know that someone doesn’t have the data still lingering, you can say, well, we’ve lost the ability to address it, so we can’t physically point to it, so it could still be sitting on a platter somewhere, but beyond that I think this gets to some of the points that were being made earlier in terms of what happens if it’s bankrupt -- if your provider is bankrupt, or it’s sold? Who actually owns the data that’s on there? And I think most people on this panel would agree it’s very important that it -- that the originator of the data has as much control as possible, not just in terms of taking it out, but controlling its future.

MR. NOJEIM: I would add, if I could, just -- I think it’s important that if people or companies are thinking about locating data with a cloud provider that they look really closely at the terms of service. Do the terms of service specify the place where the data will be held? Are the terms of service changeable so that the place where the data is held could change without one’s consent? Would one get notice if the place where the data is held is changed? Can you lock in the place where the data is being held with your agreement? I think that’s important, in part, because it determines the law that will apply to that data.

MS. BLUMENTHAL: I would echo and even expand upon what Allan said about how this is, I think, a central question that we don’t know and it’s early and there are technical reasons why it’s hard, and we don’t yet have the legal or procedural reasons, but then I listen to Greg and I think a further challenge is that if you talk to the people who are building the technologies of the cloud, what they will argue is that if you really want to get the cloud, and not the data center, then you’re not going to know where the location is, and we are increasingly moving or contemplating technology where you can do lots of dynamic movements, and it’s in the provider’s interest to do that, to balance the load, to manage the cloud, to get the most out of the infrastructure from a provider’s business point of view. So, if you have all of that mobility then how to mesh that with the kinds of protections that Greg would like to see, I think, is a hard problem and something else that we have to work through.

MR. NOJEIM: And it gets really complicated -- that’s a really good point, because then it gets really complicated. Say you’ve located the data in a state; most of them have these laws, that require notification when there’s a breach. Who provides the notification? I mean, will the provider automatically provide notification if there’s a breach? Does it matter where the data was located, which state, for you to get that notice?

MR. WINGO: So, we have a white paper, security white paper that talks about, you know, what we do for deletion, but as Marjory and Greg have said, there are a lot of interesting questions. I think on data breach, this is an area where we will look to Congress to, you know, have a system, or there’s been talk of what we could do for a federal approach to breaches, but for deletion, again, this is an area where you will see market forces come to play and, of course, you know, consumers will make demands and want to know more about exactly what’s going on, and so we will continue to offer tools to be more transparent and to give consumers meaningful control over all aspects of their data including deletion.

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

MR. QUIGG: Hi, my name is John Quigg. I work for a local nonprofit. So, as we’re discussing this, the lens that you’re using is fairly U.S.-centric, however, a lot of the data is being stored overseas as we speak, and the law problem that we’re discussing certainly is -- we’re handling this through the legal sphere, and I don’t see, having worked in security for the past 10, 15 years, I don’t see the legal community being able to move through case law or statute as fast as the technical problems arise, and so, yeah, we do get to the right solution eventually for the problem five years ago. How do you see the trend line on this working over time and are we going to get ahead of the curve or are we just going to have to move out by fiat as this becomes more complex?

MS. BLUMENTHAL: I don’t know that there is an easy solution because I think that the technology is getting ahead. I do wonder about the plausible path toward some of the novel technical architectures that are being explored in the research community.

Now, on one hand, some of what’s explored in the research community never goes anywhere, but on the other hand, Google and other companies, you know, have benefitted from federally funded research in the past. So, one paper refers to something called the locker system, and it's focused on people who don't want to give their personal data in the public cloud to lots of social media sites, they'd rather have control. So, they call for what I might call a super third party that holds their social networking information, and there's just this additional separate repository that controls social network information from their data. It's a totally different approach, and I probably have butchered the example, but I wonder whether, in fact, we'll solve some of the technical problems and some of the privacy concerns if we are able to adapt some of the technology.

However, having said that, the Googles of the world -- Amazon, Microsoft, others who are involved in the public cloud -- are moving out so fast that I would share a certain amount of pessimism, but hope that after, perhaps, an awkward decade we'll be in an interesting place.

MR. WEST: I like that delicate balance in between pessimism and hope.

MR. WINGO: John, first thanks for your service, and I think it's, as Marjory says, it's not an easy question, but one concern is the bad place that this could go. You could have balkanization, you could have different countries internationally deciding that they have to exert more control. Security is a legitimate issue, but sometimes security can mean different things in different countries, different regimes, and we have concern about what happens with free expression, in addition to just commerce, and people in a particular country being able to have all the benefits of the Internet.

So, cross border data flows is complicated, it's a tough issue, but what's really important is for -- and the United States gets this, the Administration gets this -- to recognize the trade implications, the implications for Internet commerce. And, you know, we spoke briefly before this, I'm a Navy guy, so, you know, as far as look at the difficulties and the struggles that happened with law of the seas, for example. So, this is not an easy area, but what we do know is that it's very, very important to get right.

MR. WEST: I've heard a couple different ideas in this regard. Some people suggest we need an international treaty, that countries actually agree on what the standards and norms and expectations are. That, of course, would be very difficult, if not impossible, to actually achieve. An intermediate strategy that some people are starting to suggest is kind of analogous to trade negotiations of having particular countries and/or parts of the world. For example, we're now working with the World Economic Forum on U.S. versus European approaches to the cloud, and there's going to be an event in DC and there are going to be some recommendations presented at DAVO, so there are people that are starting to think about these issues, but as everyone has pointed out, you know, they're very difficult when you start navigating international situations.

There's a question right over here.

MR. GELMAN: Thank you. Harry, you talked about the difficulties of --

MR. WEST: Actually, could you give us your name and organization, please?

MR. GELMAN: I'm Bob Gelman. I'm a privacy consultant. Harry, you talked about the difficulties of managing security of your own systems with some force and I think you had a point, but when we talk about managing your data in the cloud, there are all these issues that have come up here, and some that probably haven't about -- what about deletion, what about the security in the cloud, what about the location in the cloud, and I wonder if the challenges of managing your data in the cloud aren't just as difficult as they are managing your own security?

MR. WINGO: Great question, Bob. I think they're actually -- they're challenging, but they're things that are -- they're challenges in the existing system, I think, that have been shown to be easy to manage, just for the average person. Sometimes unfortunately to the people's peril, to the loss of privacy -- if you don't have security, you don't have privacy -- you have machines that are unpatched, they're being recruited for bot nets, so we know something is -- the system we have now, people need help on this. So, absolutely agree that we have to be vigilant and we feel that we definitely are. We build security in, we have considerations for privacy, when we work on this -- in fact, we have a motto, if you focus on the user, everything else will follow, and so as you move into the cloud, what we're excited about is the -- you know, there are challenges, but we think that we actually can make people a lot safer than they are now, not saying that we won't have -- you know, it's not easy, but there are realities of people not patching, of things being difficult to understand. Now, you should just really be able to pick up your device, use it from anywhere, anytime, and have it just work and be safe. And so, easier said than done, but we are trying, as I mentioned, Chrome OS, what we're doing with the netbooks, and we've had a discussion going on on the web -- anyone can join it, if you just Google Chrome OS, there's a blog, you know, the code is out there, but we -- you know, we think that innovation is going to make a difference and we have to -- we rely on all of our users, actually, to keep us honest, to keep pushing us to -- you know, we get feedback, we think about it ourselves, we're part of a community, we actually sponsor research, we have a site where we've got research on cyber security and all kinds of things, but nobody said it was easy, but I think we're going to have some promising developments.

For example, Two-factor, you know, I mentioned that. We will, at some point, roll that out for our general services. We're part of the open identity exchange, OIX, open authorization, you know, which is a way that you have password reuse as a problem, so we're working on those with open standards. Also, you know, the ability to have, you know, single sign-ons. So, we're doing a lot of work on the security side and we think that actually bolsters privacy, but it is challenging.

MR. GELMAN: Can I follow up? I don't think you really got the point that I was making. If I have to manage my own security, I have to juggle three or four balls in order to get it right and it's really hard to do, and you make the point, and I don't disagree at all, that most people don't do it very well. If I have to manage my cloud services I also have to juggle three or four or more balls, it's just different sets of balls. The management problem is just as compelling difficult as it is managing your own security.

MR. WINGO: So, Bob, maybe this helps. One way to look at cloud security or cloud is you will have secure automatic updates to a lot of what you're doing. So, in that sense, it becomes a lot easier. It's like the easy button. So, think about right now when you've got your own computer, you've got the model of your desktop, it's up to you to put all the patches in to do a lot of that work to make sure you're being vigilant on it if you move to the cloud -- so, that's sort of like having your home -- you have to buy burglar alarms, get a guard dog, if you want to. If you put it in Fort Knox, do a lot of people want to go there to attack it? Of course, you know, you go where the money is, but it's a very different proposition to break into somebody's house versus breaking into Fort Knox, and for us, that digital Fort Knox, if you will, has an MIT inside of it, or Harvard, because you are having all the best -- you know, some of the very best security experts in the world doing things.

So, in a lot of ways the promise of cloud could be, or will be, probably, you'll take a lot of that off of user's hands.

MR. NOJEIM: I think what he's saying -- Bob, help me out with this -- is that consumers are going to have trouble understanding whether they've stored the data with a digital Fort Knox, or a digital, we're going to use it freely, and that having to navigate those -- I mean, I've got to tell you -- so, I have an iPhone and I got an update to the terms of service. They wanted me to read 55 pages of terms of service on my iPhone. I mean, obviously people aren't going to do that. How is it that people can manage the fact that they're going to be storing data with different providers and understand exactly whether they have a Fort Knox or whether they have something else?

MR. WINGO: Okay, I understand. That's a great question and in fact that's something where industry collaboration -- so, maybe what you're asking is, will a Google make sure that we work with Amazon or Microsoft, and you're able to actually -- so, we've got a dashboard, we've rolled dashboards out for our service, which helps with this, but the question is, what is the industry doing? And so, we look forward to engaging with all of you, you know, to try and answer this question. That's an important one. So, thanks.

MR. WEST: I think we have time for one more question in the very back.

SPEAKER: Hi, my name is George (inaudible). I'm with Nokia, and this question is a little sort of more based on web standards. And a lot of the industry and cloud computing platforms have been focused around sort of newer web technologies, because the web standards that the Internet is based on, and the language is specifically HTML4, haven't been revised in about ten years and they don't impact the cloud. But with HTML5, there's a lesser known API within the standard called HTML5 local storage, and it directly impacts providers like Google, in terms of essentially providing sort of super cookies for web services. So, as cloud computing platforms become more advanced, they actually need to cache more data on the client side to speed up that service, and with this API, the amount of data stored on each client computer could be in sort of the gigabytes realm.

And I'd like to know what companies like Google are essentially doing to ensure privacy in that local storage area? Because I know, for example, Chrome OS, which you've discussed today, almost exclusively relies on that, because there is actually no storage aside from memory on those devices, on those netbooks, and I'm not really so much concerned about a large provider like Google handling encryption on gigabytes, local storage in my memory, on my device, but how would you prevent say a small scale web developer who has access to those tools, they want to speed up their private cloud, maybe has three or four machines running, but they're storing maybe your credit card data, maybe your personal data, maybe your address, on that data cache that could then be accessed by a hacker and eventually lead back to the cloud computing service that you're connected to?

MR. WINGO: Thanks for your question, George. Clearly we're doing things with HTML5, we support it. For Chrome OS, we're not -- one of the benefits of it is we won't -- or one of the approaches is we won't be storing things on that device, it'll out, you know, with Google on our data centers. But what you're saying is actually -- it goes to the scale in who you choose as a provider, so you will have those options. This is one thing to consider with a so-called private cloud versus, you know, one where you have multi tenants and you have a larger scale. You will absolutely have to have, or you will have options where there are smaller shops because that's where innovation comes from, but this is an example of consumers having to navigate -- and this goes to Bob's point and what Greg said -- navigate, well, who am I really dealing with, who am I trusting, and so one part of, you know, the Chrome approach is to, you know, the sandboxing idea and actually looking at the ecosystem, watch for there to be tools and for ways for collectively, if you're using a service, to say, you know, this may not be a corner of the Internet that you want to go to, this may not be an application that you want to run, or it may be. There may be those guys who have a couple servers and they've got some new service and if it does well and people recommend it, they will grow. They could also -- but watch increasingly for those guys, or gals, not to have that approach because they may decide to start doing their start up in someone else's cloud, which cuts down on costs. But it's a great question. Thanks.

MR. WEST: Okay. I think we are out of time, but I want to thank Irfan, Allan, Harry, Marjory, and Greg for participating in this forum, and we'll be doing additional papers and forums in the future on cloud computing, so thank you very much for attending.

* * * * *

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