THE BROOKINGS INSTITUTION

IS THE INTERNET STARTING TO FRACTURE?

Washington, D.C.

Thursday, September 25, 2014

PARTICIPANTS:

Moderator:

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

Panelists:

CHRISTINE BLISS
Assistant USTR for Services and Investment
Office of the United States Trade Representative

LIXIN CHENG
Chief Executive Officer
ZTE USA

JAMES MULVENON
Vice President, Intelligence Division
Director, Center for Intelligence Research and Analysis
Defense Group, Inc.

RICHARD SALGADO
Director, Law Enforcement and Information Security
Google, Inc.

DANIEL SEPULVEDA
Deputy Assistant Secretary, Bureau of Economic and Business Affairs
U.S. Department of State

* * * * *

ANDERSON COURT REPORTING
706 Duke Street, Suite 100
Alexandria, VA 22314
Phone (703) 519-7180 Fax (703) 519-7190

P R O C E E D I N G S

MR. WEST: Good morning. I'm Darrell West, vice president of Governance Studies and director of the Center for Technology Innovation at the Brookings Institution, and I'd like to welcome you today to our forum on "The Future of the Internet and Trade in a Digital Era."

We do have a Twitter feed set up for this event. It's #techctiTechCTI. That's #techctiTechCTI. So if you wish to post any comments or questions during the forum, feel free to do so. We are also broadcasting this event over C-SPAN, so we'd like to welcome our audience from around the country as well.

Since its inception, the Internet has thrived as a platform that facilitates open data flows across national boundaries. Commerce and communications has grown due to the ability of people in diverse areas to connect with one another. But in recent years, there have been a number of challenges that have arisen that have run the risk of Balkanizing the Internet and undermining trade and cross-border data flows. This includes protection of sentiments, interoperability challenges, and cybersecurity threats, among other types of things. And so the result has been a crisis of confidence in the digital economy as a whole.

So to help us understand these issues, we brought together a panel of distinguished experts. Ambassador Daniel Sepulveda is the deputy assistant secretary of the Bureau of Economic and Business Affairs in the U.S. State Department. In that position, he coordinates international communications and information policy, and prior to that he served as a senior advisor to Senator Mo Cowan of Massachusetts and also as a senior advisor to Senator John Kerry. And the ambassador was telling me just last week he has a new son who was born, so if he yawns from time to time, please

understand the family considerations.

Christine Bliss is the assistant U.S. trade representative for services and investment in the Office of the U.S. Trade Representative~~.—~~. She oversees multilateral and bilateral services and investment negotiations~~.—~~. She is the lead negotiator in the WTO service negotiations, and she has also worked as chief counsel and acting assistant trade representative for monitoring and enforcement.

Lixin Cheng is senior vice president of ZTE Corporation, and also the chairman and chief executive office of ZTE USA~~.—~~. He's been with the firm for two years now, and previously was on the board of directors of the San Diego World Trade Center.

Richard Salgado is the director of law enforcement and information security at Google, and in that position he oversees the company's worldwide law enforcement and security efforts, and prior to that he worked in security for Yahoo, and he has also been in the U.S. Department of Justice and also served as a federal prosecutor.

James Mulvenon is vice president of the Intelligence Division of the Defense Group, and he also serves as the director of the Center for Intelligence, Research, and Analysis~~.—~~. ~~She~~ So he is an expert on various aspects of cyber issues and intelligence gathering.

So I'd like to start with Daniel and just ask him, what do you see as the biggest current challenges to international trade and cross-border data flows?

MR. SEPULVEDA: Thank you very much~~.—~~. Thank you for having us~~.—~~. It's an honor to be here, and thank you to my fellow panelists~~.—~~. Assistant USTR Bliss and I work together at USTR a couple years ago, back when I was a younger man.

You know, I think in terms of the challenges to international trade relative

to digital data and digital data flows, the biggest challenge is cross-jurisdictional issues and the concerns that people have about implementing their particular laws on behavior that takes place and information that is housed in other markets.

So what we do to try to effectuate that, the solution to those challenges is really both bilateral and multilateral~~.~~. We ensure that we have good working relationships, not just between the offices of the state, but the offices of the Department of Justice, the Department of Homeland Security, the USTR, and others~~.~~. And they're working with their appropriate counterparts on whatever issue is a particular concern to that given market~~.~~. I hold bilaterals with multiple markets on a regular basis, and the way that we organize them is that on the first day we will have industry and my counterparts from the other country and industry from their country and myself and my colleagues from the interagency sort of challenging each other about what the challenges are to doing and conducting business on a fair basis across borders with that particular market, and seeing if there are ways that we can resolve particularly outstanding issues.

The other issue that we have is the vision of the Internet by some countries as something that disproportionately benefits the United States or the West, in which they are consumers and not participants in a market~~.~~. And in that case, the situation there is that you get traditional protectionist tendencies in that situation where what they will try to do is force production in a given market or force investment in a market in order to create a digital market or an Internet economy within that particular country.

The problem with that is that that sees the Internet, and information and communications technologies, and communications in general, not as a platform for development but as a source ~~for~~ of development~~.~~. That is to say that it's a piggybank

rather than a bank, in the sense that information technologies in a global market is essential to the growth of sectors across an economy. So keeping it as open as possible has benefits that spread widely across health care, agriculture, all over the sectors of the economy to ensure that you get greater efficiency and effectiveness and productivity out of the people working in those sectors.

So we make two points in that scenario. One is recognize and see the value of the platform as a source for development for your entire economy, and secondly, let's work on capacity-building efforts so that you can use the open and global infrastructure of the Internet and information communications technologies to build legitimately competitive producers within your markets. And that's actually, I mean, that's happening. You see that occurring around the world with innovative products and services coming out of different parts of the world and serving both local and regional markets in a way that products and services that we develop and use the platform from here can't do or don't know how to do because they don't know the market as well.

So all in all, I think the biggest challenges here are ensuring that we preserve what works about the Internet, the voluntary nature of it, the economies of scale of a global network, and ensure that we are including and becoming increasingly inclusive both in the decision-making about how information works and in our deliberations and respect of what it is that others expect from the network.

MR. WEST: Thank you.

So Christine, you focus on trade issues. What are the challenges that you're seeing?

MS. BLISS: Well, again, thank you very much for the invitation to be a part of this distinguished panel, and I appreciate the opportunity to be here.

Certainly, this is a very central and important part of the administration's trade agenda. And we start from the premise that digital trade and information flows are becoming a more and more important source of our GDP, employment, and just overall business productivity and the opportunity for innovation. And from that point of view, in terms of challenges specifically, I think I would say the number one challenge that we see, and it very much overlaps with some of the comments that Danny has made, is localization requirements in various forms. I think most specifically tied to the Internet, it's either in the form of local server requirements, the requirements to have a server in country to provide your service, and the downsides of that I think are extremely obvious. The cost is tremendous, and it can, in fact, deter companies from even going into a specific market if they know they have to set up a new local server in that country.

Secondly, having to store data locally within a country is also a tremendous costly barrier. And again, we understand some of the motivations, which may be security, privacy, but we believe that there should be and can be ways around that so that again the tremendous cost involved in setting up separate data storage centers can be avoided. I think those are two of perhaps the most pernicious practices that we see. And again, often tied to the comment that Danny made, that countries see this in some instances as an opportunity to encourage the growth of their own Internet industry.

But we absolutely agree that, in fact, that often turns out to be counterproductive because of the high costs, because it ends up undermining often the quality of the services that can be provided, the level of competition. And really, the transfer and dissemination of technology that comes through open investment and encouraging greater use of Internet. And this is particularly true for small and medium

enterprises, which again is an area of particular interest to us and in terms of encouraging trade opportunities.

I think it was eBay that did a study and showed that those sellers that sold through eBay participated in exporting basically at a 90 percent level, as compared to those small- and medium-size sellers that did not participate in online sale who exported at a rate of about 25 percent. So we think that there are real gains that can be made, not just in the United States, but across the globe. And again, those kinds of localization requirements are self-defeating.

Another aspect of this, and China in particular is engaged in this practice unfortunately, and that is favoring indigenous technologies and standards. And that can also be a very serious barrier, a deterrent to investment, and one in which we have long sought to try and discourage.

In addition, I think there are a couple other things I'll just mention briefly aside from the whole localization issue which we spend a great deal of time trying to dismantle. Secondly, I think lack of interoperability of privacy regimes, and certainly in that regard there's been a lot of highlight and attention on differences between the U.S. and the E.U. regimes and a lot of work, very good work that's going on in that sphere between the United States and the E.U.

Censorship is another issues that we've had to confront. And again, there can be legitimate basis, certain instances for censorship. But again, at the same time, particularly in countries like China, and in some instances Vietnam, it can be a serious barrier to increased trade and investment.

And then finally, I'll mention just straight market access barriers that we've run into in this sector. First of all, restrictions on investment. In some instances,

there can be no investment at all in Internet and related sectors~~.—~~. Secondly, there can be restrictions on related services, like distribution, very critical to carrying out the service in the particular sector~~.—~~. So there are traditional kinds of trade and investment barriers that we seek to attach as well.

And again, I won't spend time on them, and they're not within my particular province of trade negotiation, but certainly IPR infringement is another very significant barrier that continues~~.—~~. And I would add to the list, finally, to some degree I think customs barriers or lack of clarity and customs requirements is something else that has created a barrier for companies.

So that's a long laundry list, but I think it gives you an idea of the real scope and spectrum of the kinds of trade barriers that we're seeking to deal with through trade rules and Internet-related services.

MR. WEST: Okay~~.—~~. Thank you.

So Lixin, what are the current challenges in trade in cross-border data flows that you're focused on?

MR. CHENG: Again, thank you, Darrell, for putting this panel together~~.—~~. I am also very honored to be part of this distinguished panel.

The challenges, I think the ~~(inaudible)~~ Balkanization of the data flow cross border and also the trade (inaudible) really reduced the opportunity for the international (inaudible)~~.—~~. We reduced the economies of scale, and also forbidding us to further innovate and also time to market for bringing affordable technology to everyone~~.—~~. As probably you know, ~~(inaudible)~~ZTE was founded back in 1985 with a mission to provide affordable communications~~.—~~. Since then, ~~(inaudible)~~ZTE actually benefitted from the free information flow and the free trade~~.—~~. So now we are 160 countries, and we are

working with almost every single carrier in the world~~.~~. And we are also starting to invest in the U.S., so now we are the fourth largest actually smartphone provider in the United States.

~~(Inaudible)~~ZTE's success is coming really from a couple of things~~.~~. Number one, it's a partnership~~.~~. Because of this flow information so we'll be able to establish partnership with American companies, for example, like (inaudible), Qualcomm, Intel, Broadcom~~.~~. So we will be able to integrate the innovation and the products into our product, with efficient engineering in China and supply chain and sell worldwide~~.~~. So that is what we call the ACW basis model for us.

And another important thing is really the trust~~.~~. It's very important for technology companies, when we deliver the products, we should have high integrity and also security~~.~~. So we need to earn the trust between us and our partners and customers worldwide~~.~~. So we have to do whatever we can to make sure that those kind of trusts are not jeopardized.

Another thing that is very important for success being a global company, you have the global strategy, but it's also very important that you act locally~~.~~. So it's our goal that we always comply with the local regulations and also local laws~~.~~. So in a fragmented Internet and challenge of the data flow and also (inaudible) really put challenges to us, as I mentioned earlier, how we can further grow with that.

So if I could make a proposal, I think one step forward is really for the government to jointly agree certain things~~.~~. First of all, you should not judge a company or product or services ~~(inaudible)~~ of the job for origin~~.~~. Because today it's a global economy~~.~~. So (inaudible), you know, we produced in China, but actually are running Google operating system with CPU, the brain, from Qualcomm~~.~~. So I think then we sell

globally.—. So we need to overcome that.—. Rather, we judge the company or product based on its own merit.

Also, the comment globally, they have to come together to agree on standardization and code of conduct, so then we can make sure the Internet, you know, the same exemption, you know, this kind of prosperity brings to the world and the productivity improvement will further prosper the economy and also help us to manage the overall challenge in front of us, even for the environment issue and those kinds of issues moving forward.—. So the next generation Internet, the potential will be fully utilized so we can enjoy more growth for the world economy, prosperity, and also creating more jobs.

Thank you.

MR. WEST: Thank you.

So Richard, what are the challenges that you're focused?

MR. SALGADO: Well, thank you.—. Good morning.—. Thanks for having me.—. I'm also honored to be sitting here among such experts.

I think it's somewhat telling that somebody who has a job that I have is speaking on a panel about trade issues.—. My job is really around compelled data disclosure from Google, and dealing with the issues of countries around the world seeking information about Google users.—. And I also work on information security issues, protecting the privacy of the user data.—. It's all one big umbrella trying to protect user data.

What's interesting about this is the world ~~or~~ of surveillance and the world of trade has now collided or combined in absolutely an undeniable way now.—. For my purposes, and I think this has probably been the truth for some time now, but my

observation was, of course, after we saw some revelations about some of the NSA programs, we saw other jurisdictions concerned about what they perceived as expansive surveillance authority by the U.S. ~~Government~~ government to kind of hunker down and try to figure out how can we protect ourselves and our users from NSA, from U.S. ~~Government~~ government surveillance~~? ~~?~~ And one of the natural reactions to that, I think, even if very misguided, is to consider data localization laws, sort of under the misimpression that that is a good step, a reasonable step to take~~.~~.

So from a cross-border trade issue, that presents some very significant problems for a company like ~~google~~ Google and for its users~~.~~. And we've heard some of the other panelists talk a little bit about this~~.~~. A country says you've got to have a data center in our jurisdiction, and you've got to put some class of user data in that data center~~.~~. It presents as others have noted here, tremendous inefficiencies~~.~~. The value of a cloud as we think about it is lost when you break it up into little pieces, so you just have lots of subclouds~~.~~. The efficiencies are gone~~.~~. You can't de-duplicate data anymore~~.~~. You're going to have to re-replicate it everywhere~~.~~. You have latency problems~~.~~. It's very expensive~~.~~. You have security issues presented when suddenly the data can't be disbursed in a secure way among lots of data centers that wouldn't share the same catastrophic fate as one might if there was a tremendous storm or some other kind of accident~~.~~. So you have network outages~~.~~. You have data loss as a result of this~~.~~. Sort of the natural ecosystem that would develop if you didn't have to put data in particular jurisdictions because of political, legal requirements~~.~~. All that is lost with data localization laws.

There's an irony to it as well, which is there is a presumption I think, that data localization laws would be good for the local country that's imposing them, partially,

perhaps, because it would give incumbent companies in that country an ability to probably take advantage to be able to compete. But of course, what it overlooks is the fact that local businesses, businesses of all types, actually take advantage of the services that are offered by cloud providers. An awful lot of companies use the services of Google and Amazon and Sales Force and lots of other companies out there to run their businesses, and they take advantage of the efficiencies that are offered by the cloud. So really, what happens if a country imposes data localization requirements is it harms those companies that would otherwise be able to take advantage (inaudible) scale.

There's also, I think, security issues that are presented when you do this. I kind of mentioned the idea that a good, secure data storage scheme is going to have data, not just in one place where it's susceptible to attack or it's susceptible to some outage or act of God that knocks a data center out. Just smart distribution will allow you to stay up, keep up time at a maximum, allow traffic to route around damaged areas of the network. If you start imposing artificial rules on what the network architecture is supposed to look like, you start losing those benefits and you start exposing data to security threats that otherwise we would easily be able to (inaudible). So in the long run, data localization requirements, I think, are really very bad, not just for the companies that are taking advantage of true cloud network but also (inaudible).

I think another aspect of this, the Snowden revelations about NSA surveillance, come in the form of countries that may be tempted to try to build their own surveillance infrastructure to match what they view, anyway, as being the capabilities of the NSA. So what we're starting to see now are jurisdictions considering aggressive surveillance laws that would have extra territorial reach. They would purport to require companies that aren't even in their jurisdiction to engage in surveillance for them. It

may be an entirely legitimate investigation.—. It may be that the need for the information is undisputed and it may be that it's entirely appropriate by most of our standards that an investigation could continue, but these laws are being imposed upon the providers to comply with them.—. And yet, they are extraterritorial.—. And in fact, may-be imposing on those providers obligations to things that are in violation of other laws that are applicable to those companies.—. So the result is a rather chaotic situation of conflicting surveillance laws and privacy laws, which are really meant to protect sovereign interests of the different countries, but are aimed at an entity that actually has no way to resolve all of that, and that is the private sector companies.

The real answer to this is not layer up on layer of conflicting national laws aimed at these providers, but I think as the ~~ambassador~~Ambassador, and as Christine had mentioned, are bilateral, multilateral, diplomatic arrangements between governments to be able to sort out their competing equities in privacy and surveillance.—. So I think in both the short-term and the long-term future, that's one of the larger threats we're seeing.

MR. WEST: Thank you.

So James, I know you have a lot of expertise on security issues.—. What are the problems that you see?

MR. MULVENON: Well, you're right, Darrell, I'm not a trade person, so I'm going to go at this from a slightly different angle, which is to say that for me the greatest current challenge is shaping the structural evolution of the Internet, particularly in the governance regime that sits on top of that.—. And there's some obvious structural causes of the fracturing that we're talking about today.—. We've sort of jumped in to sort of how to fix it without really beginning by saying, why is the Internet fracturing in significant ways?—? And I think, you know, it's both, you know, the economic stakes,

which are now so great and the enormous percentage of the global economy that relies on these networks, as well as the fairly precipitous decline in the security that we feel on those networks and the real concerns that we have.—. Given those two trends, it's natural that people look to the governance model and people look to the ways in which the legal structures are set up as a way of ameliorating those concerns.—. And it's led to some interesting false memes, like this idea that somehow I can, as a cat's paw of the U.S. Commerce Department -- I mean, if anyone has ever known Esther Dyson, or Rod Beckstrom, or Dark Tangent, it's ridiculous, the idea that somehow I can, as the Commerce Department's bidding.—. But that's led to the opposite pendulum false meme, which is that somehow the International Telecommunications Union under the U.N., which doesn't have the expertise to deal with this, and is really the wrong venue for a variety of reasons that I'm mention in a minute, that we should move to a more state-centered model.—.

And why a state-centered model?—? It's because this idea between these two competing camps that somehow on the one hand the Internet is a global commons, and that really has its origins in the sort of cyberpunk, libertarian origins of the network, versus those who now say because of the economic stakes on the Internet, we need to impose a sovereignty model on the Internet.

Now, I'm here to say my personal opinion is there is no global commons in cyberspace, even though my name is on a CNAS report called the "Global Commons" in a chapter on global commons in cyber.—. I was a respectful dissent.—. And the reason is because the actual structural architecture of the Internet, you know, every node of the network resides within the sovereign boundaries of a nation--state and is therefore governed by its laws.—. The data travel over submarine cables and satellite connections

that are owned by companies that are incorporated in countries, and therefore governed by their sovereign laws. There is no part of the architecture, except for little specs at Sealand and other places, that don't fall into the Westphalian sovereignty order.

And yet people say, well, even all that is true, I still want to live in virtual space as an avatar and still enjoy the freedom and the benefit and the libertarian joys of the commons, even though the architecture that my virtual instantiation is living on, absolutely falls within the Westphalian notions of sovereignty and legal structure. And this is a big philosophical battle that we're fighting right now, and a lot of countries like China and Russia and the code of conduct was mentioned and others, look at the structural aspects of the architecture as it relates to sovereignty and they say, naturally we have a right to not only protect the network, but also to police the content on that network which we regard as part of our national space. And this is a huge philosophical battle when mixed also with the battle over whether Internet standards and other IT standards can be used as trade weapons that we're fighting right now that will really determine 5, 10, 15, 20 years out what the nature of the network looks like.

And so I just wanted to step back for a minute and look at it from 30,000 feet and talk about some of those cause and effects because I think we can then go back down and talk about specific remedies and the ways we (inaudible) have to understand where all of this problem in my view actually comes from.

MR. WEST: Okay. No, it's very helpful to have the background.

My next question I'm going to throw out to the entire panel and any of you who want to jump in. Several people have mentioned these questions of trust. We can all see the tensions that have developed across countries, as well as across sectors.

So the question is, how can we rebuild trust in international trade and the digital economy, and are there particular steps that you think we should take that would improve trade and cross-border data flows? So any of you who would like to jump in. Don't be shy.

MR. SALGADO: Certainly. I think from my little world, the surveillance world where so much trust has been lost, especially for users outside the United States, I think the simple but very meaningful steps would include updating U.S. surveillance law. And we've got some good vehicles for that. We've got great vehicles right now for reforming the Electronic Communications Privacy Act, which is one of our domestic surveillance statutes. Get it in compliance with the constitution. Get it to be consistent with the standards that most companies are complying with anyway in the United States, but the statute is way out of date.

The second is addressing the national security authorities in the United States, FISA. The USA Freedom Act is one vehicle that would do a nice job of addressing a lot of those concerns, particularly around the concerns of bulk surveillance by U.S. national security. Those are two very important vehicles that are there, ready to be passed, and can help reduce the concerns about aggressive U.S. surveillance law.

I think there's also a great need for the United States to be better at being able to process requests from other jurisdictions for user data from U.S. companies that hold it. If we can provide a good working avenue for foreign jurisdictions, non-U.S. jurisdictions to get data through a good process with good standards, we'll reduce the perceived need by these jurisdictions to enact extraterritorial surveillance laws or to put in place data localization. Even simple changes to make it so that we are, the United States, better at honoring our treaty obligations under (inaudible) legal assistance treaties

and other vehicles I think can go a long way to reducing some of the pressure.

MR. WEST: Okay, Daniel?

MR. SEPULVEDA: There's a couple things that I want to say. One, I think that we should put this in context and perspective. In the first instance, yes, there have been a lot of moves in the press and in discussion about data localization. The biggest threat, the most real one was in Brazil where in the Marco Seville, which was passed in Brazil earlier this year, there was at one point provisions mandating data localization. Those provisions were removed from the bill in part because of the recognition within Brazil that doing so had negative repercussions for Brazilians themselves, and that we're seeing that kind of educational process taking place around the world where people see that it's not really in their self-interest to engage in data localization processes.

As it relates to the steps that we can take to restore some degree of trust or restore some degree of collaboration and comradery on these issues, the E.U. and the U.S., under the direction of the Department of Commerce here and their counterparts in the E.U., are working on updates to the Safe Harbor for E.U.-U.S. transmission of digital data. Again, I think that there's a recognition within the European Union that it is as much in their interest as it is in ours to ensure that we have an interoperable, mutually recognized system of distribution of information, because of how important this is to the entire economy in both sectors.

Another step that we're taking is NTIA's announcement earlier this year to transfer the IANA contract functions subject to a couple of conditions, to the multi-stakeholder community to ensure that we're talking about what is a truly inclusive, truly global participatory system of governance of the administration of the IANA functions.

And then the third thing that I would talk about is capacity building in those parts of the world where introduction to Internet communications and the global network is coming on at a slower pace, but now gradually increasing in Africa and Latin America, Southeast Asia. You're seeing what are around 16 to 20 percent -- 16 and 22 percent, penetration rates for the Internet growing at exponential rates and those countries and their governments are asking us and others to help them with building up incidence incident response teams and putting into place the right legal and regulatory infrastructure to ensure that information sharing is possible so that you know and can mitigate against threats and attacks.

And then separately, the president has announced a series of reforms relative to our intelligence practices, and among those, within that package of proposals there are proposals to improve the MLAT process, which is the Mutual Legal Assistance Treaty processprocess, by which governments can ask us and access information necessary to the enforcement of their laws at home relative to information that's housed here. But again, I would go back to the point that I think that what we saw maybe in the immediate wake of this known disclosures hasn't really manifested itself in a closing or a fracturing of the Internet. At the end of the day, you do see proposals from some authoritarian states to either wall off aspects of their Internet or to impose international regulatory standards on what people can do and say and transmit across the Internet, but you don't see that being adopted by a significant portion of the world. And Brazil's migration, in particular, at a post-conference that they held earlier this year called (inaudible) in Sao Paulo really manifested itself in the vast majority of the participants from the world at that conference, agreeing to the multi-stakeholder system of Internet governance and agreeing to the importance of the free flow of information across

international boundaries.

So I think to some degree there's a glass half full story to be told here and that we're making some good and significant progress, both in collaboration and cooperation with our colleagues abroad.

MR. WEST: Christine?

MS. BLISS: I would just join in on that and absolutely agree with what Danny had said about Brazil, and I think it was a good example of how hearing from companies and stakeholders in Brazil about the real problem with localization requirements that Brazil had proposed had a very positive impact in that instance.

I think there are plenty of challenges that remain. I think, for example, in Indonesia, we're seeing a trend in the opposite direction, which is of great concern, and localization area. India remains a huge problem in that regard. So I think we have plenty of work to be done. And I would say from our perspective what we're trying to do and will continue to do is through our active negotiations, the most prominent one being the TPP negotiations and our services -- ecommerce, telecomm, and investment chapters -- there are a series of about five core provisions we think are really aimed at what we've been talking about this morning.

The first is that we negotiate a prohibition on tariffs on products that are distributed electronically so that they will not be subject to customs duties, and we think that that's something that started in the WTO but we've extended through our FTAs and we think is a very, very core and important rule to reinforce.

Secondly, we negotiate nondiscriminatory treatment of digital products, which again can be a pernicious kind of barrier to entry into a market. So establishing the more we can make progress through our regional FTAs the better.

Thirdly, cross-border information flows~~.—~~. We have a mandatory binding provision that we're negotiating for the first time in TPP that countries are signing up to, that requires that they allow free transfer of data flows on a cross-border basis, which again goes directly to what we've been discussing today.

Fourthly, we're negotiating a rule which would prohibit the requirement that countries require servers be located in their own territory~~.—~~. And again, we ~~believe~~ think it cuts right to the heart of the core concerns that are raised with regard to localization.

And then finally, what we do in our services chapter on a cross-border basis, we negotiate on the basis of a negative list~~.—~~. And the reason we think that that's so relevant to what we're talking about today is that you want to be able to cover virtually anything~~.—~~. And I think as we all know, in the digital area, innovation is ever present increasing, something we want to encourage~~.—~~. So the more you have trade commitments that are based on a negative list, then you are able to cover new services as they are created, as they grow.

So we think these elements combined, the more we're able to pursue them, if we're able to create agreement among the TPP countries, we're pursuing similar kinds of requirements in the TTIP negotiations with the Europeans~~.—~~. We are also pursuing similar requirements in the TISA, the plurilateral services negotiations, which we have roughly 24 countries, 48 if you count all the individual E.U. member countries together~~.—~~.

But what's important about that is those core rules that I've just described, if we can propagate them among that large a group of countries, then I think we will go a long way towards really directly addressing, or at least giving ourselves

another tool in the toolbox to take on what, again, seems to be the most pernicious problems, particularly of localization.

Finally, on the investment front, which again, I've been talking more about the cross-border piece, but through our bilateral investment treaties and also or investment chapters, we also believe that the removal of market access barriers, when a company decides it does want to invest and it makes economic sense and it fits with their business model, that they're not barriers to foreign direct investment and as in the case of the China example, there are not discriminatory requirements that require you to use local technology or use local standards.

So I think it seems to us that having those tools -- it's not the complete answer -- much of what Danny has alluded to is also an important part of the whole piece of addressing the issue in terms of multi-stakeholder organizations that we need to develop in terms of Internet governance, bilateral dialogues, which are also important, all this working together, we think, can make significant end roads.

MR. WEST: Lixin, what do you think we should do to rebuild trust in trade in the digital economy?

MR. CHENG: I think the invention of the Internet, and this has really brought significant improvement of the productivity, and also the global trade. I think it's obvious. Recently now people are concerned about cybersecurity and privacy and that has really come from certain requirements from different (inaudible). So to that extent I agree with (inaudible) that the Government really has to jointly sit together. I agree with the standard and the code of conduct as I mentioned earlier. And also, don't judge the technology origination, or the product originalorigination, or service organization origination from different geographical areas. We have to make sure that that

framework is established.

And also, today's prosperity of this openness of Internet and also economy, is really because of the contribution from all the technology companies.—. So the technology companies also need to work together across international borders to make sure that we can react and contribute to such kind of framework so that we can innovate and develop a viable -- commercially viable system, and technology to enable such kind of openness of the Internet.

And today, again, any success of a global company depends on the trust they gain, (inaudible)they build, and they maintain with their customers.—. So if we lose the end-users' trust, and I think we will lose fundamental of our business and then the prosperity of the world economy.—. So that is very important for us keep in mind.—. No matter which government, for what kind of purpose, and make sure that the prosperity of the economy and the development of the industry is there.

So I want to say today, you know, the fragmentation of the Internet is really coming from the concerns about cybersecurity and privacy, and I have to say that a fragmented Internet would not bring security or privacy protection to the cyber world.—. And cybersecurity, enhancements of cybersecurity and the protection of privacy should not jeopardize the openness of the Internet.—. So we have seen (inaudible) get global trade, but I think also with (inaudible) there is a missing piece.—. How are we going to ensure the free flow of data in today's everything connecting world?—? I think that's also something that needs to be done by different governments.

MR. WEST: Thank you.

So James, what are the steps that you think we need to undertake here?

MR. MULVENON: So whenWhen I think about trust in this context, you

know, it's difficult in a world now where I can't even trust my new refrigerator, which I discovered in my home network logs last night, was surreptitiously trying to go through my home network to communicate back to its manufacturer to download the latest firmware, I didn't even realize there was a wireless antenna in the damn ~~antenna~~refrigerator~~.—~~. But fortunately I had my firewall configured properly so it wasn't able to get out~~.—~~. So sad refrigerator; happy James.

MR. CHENG: Not e~~E~~verybody is an expert like you.

MR. MULVENON: Well, and that's what I'm about to get to Lixin, which is the problem -- and you'll be surprised to hear this from me, given what I do all day in the intelligence business, but for me, the basis of trust in my daily life is robust transparent encryption~~.—~~. When I receive messages from people, the way I trust those messages is because of the digital signatures of those messages~~.—~~. And I've been an avid user of encryption for over 15 years, and it's been almost a fanatical user of it~~.—~~. And I will say that I realize this is the trend of the day~~.—~~. Everyone now has suddenly discovered encryption~~.—~~. Journalists have all of a sudden figured out how to spell encryption~~.—~~. They previously didn't know about it~~.—~~. Mr. Greenwald admits that he ignored all of these entreaties for so long~~.—~~. But at the end of the day it has to be robust~~.~~ . It has to be transparent as to how it's being used~~.—~~. The engineering, when it needs to, has to fade into the background, but sometimes it needs to be front and center~~.—~~. But it also has to be easy enough for my mother to use~~.—~~. It can't be that you can only be a crypto paranoid if you can run GPG on the command line~~.—~~. It has to be something that is based in at a basic level into what we're doing.

Now, I will say, you know, as an Apple fan boy for many, many years, that the recent moves by Apple, for instance in ~~IOS~~ iOS 8, where they took the burden of

the robust encryption away from the user and the configuration, and baked it into the way the system was built, is going to be the trend of the time, and that's to the benefit of everyone who doesn't want to spend the intellectual capital to figure it out.

Two-factor authentication. As the father of two teenage daughters, a big fan of two-factor authentication of pictures in iCloud. And the idea somehow that -- and we've moved it out in our corporate networks, but there are all of these measures that are coming along, and you'll see an industry I think that is growing up now that understands that there is this desire for it. But that will naturally lead -- and we need to be prepared for -- another clipper chip debate. It's going to lead to another reaction that says, okay, the world needs robust encryption, but now what is the legal and privacy and governmental oversight regime that allows for key escrow and everything else? So we have to ~~girder~~ guard our loins, and understand that that is coming and we're going to have that discussion, and I think there is a balance that can be struck there.

But we also have to deal with, again, with the use of cryptography standards as trade weapons. In China right now, the rise of their national SMX standard and the insistence of using their market ~~leverag~~leverage, the fact that so many IT products are manufactured in China, to use that as leverage to force vendors to make their products compatible with Chinese crypto standards, without a lot of transparency. I mean, the iPhone 5 in my pocket has a dual WAPI Wi-Fi chip in it. But when you talk to Apple, they can't even tell you what the WAPI side of that chip does. That's the Chinese wireless security standard. There could be a rogue WAPI node in this room, I wouldn't even know. We're trying to figure out even how to design an app to be able to figure out whether that's true. That is not transparent encryption. That is not a transparent cryptography standard regime. So while I'm arguing for robust encryption,

we clearly have a lot of work to do in the engineering of making that possible.

MR. WEST: Why don't we open the floor to questions from the audience?

Now, I'm used to being worried about the government~~.—~~. I guess now I need to worry more about my refrigerator.

MR. MULVENON: And your toaster.

MR. WEST: So questions from the audience?

There is a gentleman right here on the aisle.

MR. ~~STERLING~~SILVA: Thank you.

MR. WEST: If you can give us our name and organization, please.

MR. SILVA: I'm Alberto Silva, professor of law at the University of Chile.

I wonder what is the actual size and scope of the problem of localization, because we have here about initiatives in Russia, China, but the issues that we have already of localization in place in several democratic countries, I understand it is the initiative of the USTR to push for (inaudible) in localization is actually because of the localization requirements in Canada~~.—~~. There are also localization requirements in Australia law~~,~~ and in Taiwan law~~.—~~. Those are not bills; those are laws in place~~.—~~. And not to talk about their requirements or localization by the UPN union, although a little more open because it is requiring that the servers process data in safe countries, and they define what is a safe country.

So what is the difference between the localization requirements that you are talking about -- China, Russia, or Brazil -- and the requirements of localization of those democratic countries I just mentioned?

MR. WEST: Okay~~.—~~. Anybody want to jump in?

MS. BLISS: Well, just briefly I could start by saying that I would certainly agree with you that localization is still a widespread problem. I don't agree, though, that I think TPP and the elements, the core elements that I mentioned were designed particularly for Canada. We had a much broader concern when we developed those elements, which certainly preceded TPP, and exist more broadly across the globe. And I think we make the same argument with each trading partner that we meet, and it's very much along the lines of the arguments that you've heard from the panel this morning, that there really is an economic case to be made that having localization requirements, local data storage, local server requirements, can be self-defeating and can ultimately not have the high quality of services and competition that you want to see in your own economy. And I think we've made a fair amount of progress, certainly among (inaudible) for that notion. We're not quite there, yet but we have. Similarly, we're making a similar argument among countries that are participating in the (inaudible) negotiations which is a much broader group, and we've just begun with the European (inaudible). So I agree with you that localization is not confined to nondemocratic societies. It exists in democratic societies as well, but I think the economics and the argument that we make is quite similar though in terms of efficiencies and can we find ways around those requirements?

MR. WEST: The gentleman right here with his hand up. There's a microphone coming from behind you.

MR. HALL: Hi, my name is Joe Hall. I'm the chief technologist at the Center for Democracy and Technology.

Mr. Mulvenon had talked about sort of the move to have more ubiquitous encryption and more usable forms of consumer security tools, and he talked a little bit

about sort of the shift as Professor Orencare talks about in terms of moving standard capability from being more law enforcement friendly to protecting the user more~~.—~~. And Professor Jean Camp yesterday put it really starkly in the sense, that she said we could mandate that cars should be able to explode on command or the engines command when being chased by the cops, but we don't do that because exploding cars are dangerous~~.—~~. And I'm wondering if the panel, if other people, or Mr. Mulvenon, have thoughts about sort of the international implications of this stuff~~.—~~. Does that put more pressure on the desire to sort of make the (inaudible) process work a little better~~?—~~? Are there trade implications of more ubiquitous consumer-grade strong crypto and security?

MR. MULVENON: The thing is there's an obvious dilemma which is to say that to argue -- because you almost want to say, well, I wish we all had better encryption, but the bad guys didn't have better encryption~~.—~~. Right~~?—~~? Well, that's obvious~~.—~~. But the problem is that given the level of insecurity, given the fact that this network -- let's be honest~~.—~~. I used to work at RAND~~.—~~. We were like node five on Arpanet~~.—~~. And you talk to all these guys down in the basement that worked on it~~.—~~. They said, "Look, we never intended this network for any malicious behavior at all." It was supposed to be for scientists to communicate with ~~each other~~one another, and all of a sudden we've built this edifice of the global economy on top of it, and we've been gluing security onto the side of it ever since~~.—~~. And every once in a while someone will come along and say let's re-architect the whole thing~~.—~~. Let's repair the damaged airplane at 30,000 feet with the giant hole in the side~~.—~~. Right~~?—~~? You know, difficult~~.—~~. Not impossible~~.—~~. Kind of a NASA level problem~~.—~~. And at the end of the day I have circles~~.—~~. There's team Mulvenon and then there's my company and then there's the country~~.—~~. And so I'm trying to secure the boundary lines that I can secure~~.—~~. And if that has the ancillary

effect of allowing people to use commercially available tools to be able to do things that I don't like, for me that's just a cost. I mean, good policies are not cost-free policies. Good policies always have costs. And for me it's a good policy to have widespread distribution of commercial-level, easy to use, security products, and then we have the engineering problem that comes along with, well, what do we do about the fact that people we might not like are going to be using them as well? But that's not a reason to then say, well, we're just going to continue to live in this very insecure world in which every time we swipe a card or put our pin into something we're imperiling our entire financial existence.

MR. WEST: Other questions? Michael?

MR. NELSON: Mike Nelson with Georgetown University.

I'm really glad to hear a discussion of encryption and data localization, but I thought it would be useful to look at a specific case study of the Internet of things. We're moving forward here to a world where there's going to be hundreds of billions of devices connected to the cloud, reporting data, and they're going to range from the Fitbit on my wrist to the sensors in a GE aircraft. How is that going to affect both our ability to implement encryption, because some of these devices are going to be ten cent devices and might not be able to support robust encryption, and how will it change the debate over data localization? Will countries want to have more control over the data inside their country? Or will they give up and realize that my Fitbit is going to go across border, the airplane is going to fly over 40 countries in a day?

MR. WEST: Good question. Who wants to address it?

MR. SALGADO: Well, I'm not sure, Mike, if I can answer all of that. I would say that I think the trend you're seeing towards encryption in the obvious products

for encryption, which are really communications-type products, I don't see that stopping, and it shouldn't~~.—~~. It's something Google has been working on long before the NSA ~~store~~story, getting as much as we could encrypted~~.—~~. ~~(Inaudible)~~ Betweendata centers and with users, trying to make it easier for users to encrypt our phones~~.—~~. (Inaudible) encrypt those for a long time now and the next build (inaudible)~~.—~~. So I think we are headed towards an understanding, a societal understanding that encryption is good~~.—~~. I don't see why that would not apply to the Internet of things~~.—~~. There may be practical issues and there may also be differences where the information, depending on the thing is not particularly sensitive~~.—~~. How much milk is in the refrigerator of James' unit maybe, but it's probably a subjective judgment~~.—~~. But I think there may be -- the trend towards encryption I think is one that is strong and we're going to see a lot more of it~~.—~~. I have the same concerns that James was talking about, which is, are we going to relive the crypto battles that we had in the '90s~~?—~~? And I certainly hope not~~.—~~. I'm hoping that we can avoid that having learned the lessons.

MR. ~~SEPULVEDA~~MULVENON: We have to acknowledge the fact that the trend line, if you will, I mean, I'm not a Marxist determinist, but the trend line right now is that over time we will increasingly live in a world in which -- well, largely for convenience reasons -- let's be clear why we've allowed all of these technologies to come into our life, is because of the incredible, you know, I think Patrick Henry said, "Give me convenience or give me death." Right~~?—~~? That's why, I mean, I'm a slave to my smartphone~~.—~~. Right?

We are living in a world -- just even in the last 10 or 15 years -- in which we are increasingly living in a world in which the mesh of surveillance and wireless interconnectivity is just going to get denser and denser and denser~~.—~~. I thought it was

fascinating that Dick Clark, a couple of months ago, was asked what the future of privacy looks like in 20 years, and he said we're going to live in this, you know, ubiquitous sort of dystopia of CCTV cameras and facial recognition and all this stuff. And then the affluent are going to take vacations in places where there are no cameras. In other words, they're going to go on privacy vacations. I don't believe that because the people who are hosting those resorts are going to want to know all about their preferences, so they are going to be secretly surveilling them in the privacy resort so they can better offer services to them, you know. You know, what kind of chocolate do they want and all that kind of stuff.

But in that world, I'm more comfortable knowing that that is a dynamism that is being pushed by social interaction and the economy and the benefits and the economies of scale and all these things, if within that environment we can set up our own definitions of multilevel security. So I don't care if the toaster is unencrypted. Right? I just want it to toast the damn bread. But I do want my email to be encrypted. I do want my online banking to be encrypted. So having these kinds of, you know, I think belaboring in the markets, I think the market will sort out -- and now you have to give the consumer more tools in order to be able to empower them to sort out how they want that multilevel security to work. And so the 10 cent, you know, thing. But at the end of the day, as much as I love dystopia, we're not necessarily moving to Skynet. We still have to control the machines, right, because they will decide that we're a virus. But at the end of the day, I want to be able to encrypt my communications so that the machines don't know where I am all the time.

MR. SEPULVEDA: If I could just add something. The underlying question of what is happening with data, the size and scope of the data sets and how

they're being used is something that this administration is taking very seriously.—. Most recently, John Podesta, counselor to the president, it's about as high as you can go to ask a question, produced a big data report, which was (inaudible) agencies and it presented a very balanced view of, well, look, there are serious benefits that derive from (inaudible).—. For example, whether it's the Internet of things and rising energy efficiency, how the grid is allocating energy across sectors, incredibly important.—. Or if it's health data and you're able to detect and respond to an epidemic much more quickly than you would otherwise, or any other -- including law enforcement -- mechanisms by which you can use data in order to do something that produces a public good, and makes us all better and happier.—. Now, you have to balance that with the fact that data can be used for good things; it can be used for bad things.—.

So what are those bad things?—? And what can we do about the use of that bad thing?—? The fact that someone doesn't care the information is distributed by their toaster but they do care about their email or their finances, is directly related to harm.—. Distribution of information about how I toast bread leads to very little harm over any extended period of time.—. Distribution of information of how I use my finances, the degree to which I make decisions, financial decisions or family decisions or health decisions, those are very serious, very private, very sensitive aspects of information that can be used to harm you.

So I think I would again commend the big data report.—. I would commend not just the big data report but the fact that this administration, the Department of Commerce in a green paper, the FTC in a white paper (inaudible) when this administration came back into office after many years of not having produced documents (inaudible), not calling for (inaudible), reengage that conversation.—. It's a conversation

that's taking place all over the world.—. The E.U. is doing their own big data report.—. APEC has a number of investigation (inaudible).—. And I think at the human rights level, you're seeing the Human Rights Council at the United Nations having extensive and serious discussions.—. CDT just made a significant (inaudible).

So again, at the end of the day, these are issues we're aware of as an administration.—. We're taking it extremely seriously and at the highest levels are working towards asking the right questions and ensuring that we don't inject unnecessary friction or do harm to what are very serious potential benefits, while at the same time balancing (inaudible).

MR. WEST: Mitzi has a question here in the front row.

MS. WORTH: I'm Mitzi Worth.—. I'm with the Naval Postgraduate School.

Did any of you see the NOVA show last night?—? It was on data encryption and whatever.—. And the proposal as I understood it was that there are ways in which you can somehow educate a particular part of your brain and you have to get trained to do this, that would somehow handle the encryption.—. I didn't understand it.—. It was pretty amazing.—. I wasn't sure I wanted to go through it.—. But I, too, am anxious about giving my credit card.—. And I don't have a lot of money, but the idea that this can make us so uneasy.—. It's so wonderful in so many ways, and so anxiety-producing in others when you think about when you get these kids that want to get in and play and they can stop the electric system going.—. You all have an enormous challenge and I want to thank you for working on it, but I wish I felt a little safer.

MR. WEST: Okay.—. Any reactions to that?

James?

MR. MULVENON: Well, I mean, you know, Alexander Gerschenkron is

the only economist I like, coming from RAND.—. He had this great idea, the advantage of economic backwardness.—. And so it's actually quite depressing for me to travel to other countries that were later modernizers in these areas because they've been able to leapfrog stages of development.—. So, for instance, the fact that I have credit cards in my wallet now that are not chip and pin is ridiculous.—. It's absolutely ridiculous.—. Given the amount of losses that the credit card companies have to write off every year, it would be worth it for them to update the infrastructure so that we didn't have to have magnetic strip credit cards.

But it's a legacy infrastructure.—. I mean, during the six-year sentence I did in Los Angeles, I remember PacBell coming out at one point and saying we're going to rip all the copper out of the walls and we're going to go to fiber.—. And then some actuary down in B5 ran the numbers and we never, ever heard about it again because we had to replace so much legacy infrastructure.—. And so when I travel to countries that have had the fortunate advantage of being able to go from basically dirt to wireless, it really highlights a lot of the issues we have in terms of structural investments.—. We're spending money, stimulus money on bridges, but it should have been spent on IPV6 and things along these lines.—. And so, you know, we're really playing catchup in many ways to some of the trends that we see in places where they didn't have those legacy problems.

MR. WEST: In the very back in the corner is a gentleman with a question.

MR. MARKS: Hi, I'm Jim Marks with Politico.

Mr. Mulvenon, I hope you could expand on something you said earlier about the concerns about national encryption and Chinese encryption standards being

put into technologies produced in China from other companies.—. What's wrong with that, if the encryption itself is good?

MR. WEST: Thanks.—. Maybe you can address that, and then Lixin, too.

MR. MULVENON: Sure.—. Well, that's the issue.—. I mean, a good example, let's go back over -- just briefly over the history of WAPI, which was the Chinese counterpart to the 802.11 wireless security standard.—. When it was proposed by the industrial planning authorities in Beijing, they said to the companies, if you're going to produce equipment and you want to have a single, unified global production chain -- you don't want to have to build a China iPhone and then a rest-of-world iPhone, and the rest-of-world iPhone couldn't be built in China unless it's certified by the resident authorities, you need to make your product compatible with this information technology standard, in addition to Wi-Fi.—. And here is the list of 30 companies that we want you to partner with, and in order to have that partnership, you have to turn over your crypto source code to them so they can build the APIs into the product.

Well, turning over your crypto source code to companies associated with an authoritarian government is not a global model that I advocate.—. And so it has as much to do -- I said when I talked about encryption, I talked about the transparency of it.—. Well, you know, there's a great encryption philosophy that says the algorithms shouldn't be secret.—. That's why I love public key cryptography.—. When the algorithm is secret, it's insecure, because all you have to do is figure out the algorithm.—. And so, you know, if we're going to have a robust encryption system it can't be that when I call somebody and I say what is the, you know, what's the WAPI algorithms, and I'm told by the State Encryption Management Commission in Beijing that three of the four algorithms in that standard are state secrets and cannot be disclosed, then I don't regard that as the kind of

cryptographic standard product I want in any of my belongs.

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

MR. CHENG: Yeah, I --

MR. MULVENON: He doesn't need to defend Beijing. That's not why he's here.

MR. CHENG: I'm not an expert about encryption, and also not an expert on legal. But what I understand from the conversation, I believe this particular case for the iPhone, it's not really because iPhone is manufactured in China, but actually, iPhone wants to get into China because if you sell that phone in China, you need to comply with the local laws and the regulations. The Chinese government requires that you have to support such kind of encryption or Wi-Fi standard. I think that's the case.

For us, for ZTE, for example, we are, today, as I'm speaking, I have 56 devices actively selling now in the United States. So what we need to do is we need to make sure every single phone we sell into the United States complies with the regulations and the laws of the U.S. government required by the carrier partners and make sure, you know, that the privacy of the consumers and the requirements from the carrier partners is implemented.

So, for example, most, I think, our Wi-Fi chips, I think particularly for the United States, we always have either Broadcom or Qualcomm and any other U.S. companies. So I think that's very clear. Because, again, we're back to the original question about the challenges we are facing. I think those are the challenges we're facing as global technology companies. It doesn't matter if it's U.S. companies or Chinese companies. We're all facing the same challenges. That's why all the governments need to come together. I think the key things for this, short-term for us,

you know, we lose economies of scale~~.—~~. So we have to have different products for China and for the U.S~~.—~~. We have to separate it~~.—~~. But ideally, we should have one size fit all, but unfortunately, we cannot do that today.

MR. WEST: (Inaudible)

MR. SEPULVEDA~~MULVENON~~: I want to just address the general concept there which is not specific to that particular chip and having two chips doing the same thing in a given product~~.—~~. It's the idea that it's the Chinese government making the determination that this is the best standard and the best chip to use and mandating the specific purchase from specific providers, that's a problem~~.—~~. Because you can't have every market in the world imposing that kind of nonvoluntary purchasing and production standard~~.—~~. It ruins opportunities for innovation, and it doesn't comply with the idea that voluntary standards should be exposed to the market and the market actors should adopt them~~.—~~. No one forces you to buy anything from Qualcomm~~.—~~. Nobody forces you to buy anything from Broadcom~~.—~~. That kind of forced purchasing is a problem and it's not fair and it's not right.

MR. ~~SEPULVEDA~~MULVENON: And you shouldn't have to include chips with standards that have already been rejected by the International Standards Organization, by IEEE, by ITF, and are nonetheless forced upon you because of market access requirements and the way that the certification process takes place in the country in terms of getting your product certified for the domestic market~~.—~~. Even though the standard itself has been rejected as technically inferior, and we see this across dozens of different IT standards in this particular case.

MR. SEPULVEDA~~MULVENON~~: And the only reason China can do this is due of the size of the market~~.—~~. The Bahamas can't make us impose a cryptography

standard.

MR. ~~SEPULVEDA~~MULVENON: It has other charms.

(Laughter)

MR. WEST: This gentleman here has a question.

MR. RIDOUT: Hi, I'm Tim Ridout, a fellow at the German Marshall Fund. I wanted to touch on something~~.~~, I think it was Richard~~.~~, said about artificial rules about the infrastructure~~.~~—. But I think that's part of what the disconnect is~~.~~—. A lot of these rules aren't artificial~~.~~—. These are the social norms, the laws~~.~~—. It's the social contract which is broken into all these different pieces~~.~~—. This gets back to the Westphalian system~~.~~—. So the Internet is designed at odds with the way human society is designed~~.~~—. So that's why you're seeing it fracturing into pieces~~.~~—. And I wonder, until you have a global social contract, I don't see how you're going to fix some of these~~.~~—. Issues are going to keep coming up~~.~~—. We differ on differing norms on the freedom of speech and just the way you do things, the way you enforce law~~.~~—. All these things~~.~~—. This is what the Internet is confronting~~.~~—. It's much bigger than just these little pieces~~.~~—. So what are tech companies -- this is my question -- what are you doing to both figure this out to understand it and to engage and encourage these sort of global debates so people do talk about how to converge norms, how to converge ways of doing things~~,~~ so we can all basically get along?

MR. MULVENON: The good news -- you know, I'll go against my Irish heritage -- the good news is that these technologies are changing social norms~~.~~—. They've changed the way I interact with my children, with my wife, with my friends, with my coworkers~~.~~—. It's literally changing the way our entire society is working with one another~~.~~—.

The bad news is, a lot of the prophesy hopes at the beginning, the John Perry Barlow Declaration of Independence in Cyberspace kind of idealism has foundered on the fact that, in fact, these technologies provide just as much interesting power to people seeking to control as they do people seeking to liberate. I remember 15 years ago, people talking about how the Internet or cyberspace was just going to wash over all these authoritarian regimes; that they were so atavistic, they were so backward looking, they would never be able to deal with it. And yet, we've been amazed as they responded nimbly to wave after wave after wave of disruptive technologies, some with more success than others. Obviously, you could compare Arab Spring to China or Arab Spring to Russia. But, you know, at the end of the day, there is more of a push-pull. And so what's also embedded in your comment though is the unintended consequences. We're not on some linear trajectory towards absolute good and peace and happiness.

And so embedded within some of these technologies are some unexpected things. Again, as the father of teenage ~~fathers~~ daughters I discover this every day when I go through all the logs of all of their computer use and all their social media use. I spend probably an hour of my day doing that now. And so you realize that these liberating technologies also have these sort of pernicious, unintended consequences.

MR. SEPULVEDA: I want to address the basic underlying question is the Internet is not breaking. At the end of the day there is literally not a country that has chosen not to connect to the global Internet. There is discussion by some politicians in some countries about constructing Intranets within their country and disassociating themselves from the global Internet. But that is actually not happening. I think Iran had taken some steps at creating an Iranian Intranet, that their people would only be able

to use in Iran and that would not be connected to the global Internet.—. I don't think that actually ever took off.—. There was some discussion in Russia about it, but that again didn't take off.

What I think that we're talking about here really is the World Wide Web, which is an application that rides over the Internet, and then services delivered over the World Wide Web that at times allow people to engage in behavior as human beings that is offensive to people in other jurisdictions.

So take, for example, I mean, the most recent case was Turkey.—. During the last election there was a Twitter situation in which people were tweeting out things about a candidate running for office, and Turkey shut down the entire service of Twitter.—. Now, that has since been worked out.—. Twitter is back up and running in Turkey.—. There have been, I think, YouTube and Facebook and others have faced similar situations in different markets.—. So, for example, there are parts of the world there it's against the law to say something bad about the Prophet Muhammad, and people do it on Facebook or Twitter or whatever all the time.—. And it's up to those service providers that are again simply a service on the larger Internet to work with those governments and where they can, if within the construct of their ethics and their terms of service, work something out to ensure that there's a mutual respect of service delivery.—.

But again, I don't want to conflate that with the idea that there are islands with of nonconnectedness in the world technically.—. They're not based on Internet protocol and their networks aren't connecting to each other.—. That's simply not happening.—. There is no Armageddon in that sense.—. But that underlying question of how do you ensure that human behavior in your country that you think is outside of your particular laws and jurisdictions is addressed, that is one of the most challenging

questions that we have, but those are questions that service providers work out with those specific countries.—. So, for example, like Pandora is not accessible, or Netflix, in significant parts of the world because of copyright law.

So I think that these are things that are being worked out in a wide variety of areas, but our goal and our underlying work is to retain a single global network in which each individual device can connect to any other individual device anywhere in the world.—. Now, what people do with that connectivity is a separate question of law and behavior, and we're working out how to manage that.—. At the end of the day there's been a lot of talk about the conflicts and the degree to which some countries trust the International Telecommunications Union, which is a specialized agency of the United Nations, versus how much they trust IKAN, which is a nonprofit corporation incorporated in Los Angeles.—. IKAN is 15 years old.—. ITU is 150 years old.—. So to some degree it's an evolution and a back and forth about what's necessary to make sure that you keep the underlying things that work extremely well about the Internet and provide extreme public benefits in terms of innovation and jobs and freedom of expression and freedom of access to information, while at the same time ensuring that you're respecting everyone and their governments who are involved in this connectivity of global communications.

MR. WEST: It's not just a technology problem anymore.—. It's a lot bigger.

MR. MULVENON: I will say thought that there is an interesting countervailing problem that came up recently, which is when you have a company that provides a social media service that has become a virtual monopoly in many markets, like Twitter, who then unilaterally decides to shield its users from disgusting videos of ISIS savages beheading people, which I didn't want to see and I didn't want my children

to see it either, but it is an interesting thing whether there is a role for government in the sense that, who is to say that Twitter got to decide that they were going to run software to go out and find those pictures and make sure that the users couldn't get them? ? And you could say, well, the market will decide. . Right? ? They'll just switch to a different social media outlet. . Well, but Twitter has an economy of scale monopoly. . At some level do I want them deciding what the social norm is? ? What's the social standard in other areas? ? Are going to block the J-Llaw pictures? ? What are the other things ~~are~~ they going to do? ? Not for legal reasons, not even for copyright reasons, but particularly because of a sense of what they think the social standard should be.

MR. SEPULVEDA: I would disagree that Twitter has a virtual economic monopoly. . It simply does not. . The barriers to entry into this particular market are nothing reflective of a monopoly situation, and the fact that you could access anything that Twitter puts on, on Facebook or any number of other -- if not social media sites, points of information on the Internet. . And I think that there's actually been a lot of talk in Europe and in other places about the idea that either Google or Facebook or other companies constitute virtual monopolies. . That's an economic term with specific definitions and it's just not accurate.

MR. MULVENON: Well, I mean, in the same way that you could say Myspace for a time had that monopoly, and clearly -- I won't use the word "monopoly." It had a preponderance in the market that went away very quickly. . So Twitter tomorrow could vanish off the face of the earth, as have many other social media services because they simply became passé. . I mean, my children will never put a Facebook account up, because that's what middle-aged people like me do. . Right? ? They have no interest in Facebook whatsoever. . So eventually, Facebook will just recede into history. . But the

community that's been created on Twitter has, you know, quantity has a quality all its own. So to defect from Twitter and say because I disagree with their enforcement of a particular social standard means that I'm not going to use Twitter, means I've now voluntarily cut myself off from an economy of scale that actually was beneficial to me because I could use the sort of crowd sourced Hive Mind and everything else. So yes, I have the market option of not using Twitter. But there are costs to not doing that because I disagreed, and there were not alternatives of a similar social scale. So yes, the legal term "monopoly" may not be correct, but in terms of the actual performance and use of that service I think that the same idea is still in effect. It's a debatable concept.

MR. WEST: Okay. I think we have time for one more question.

The gentleman right over there with his hand up.

MR. ERLANDSON: Thank you. Thank you to all the participants for being here and speaking with us.

My name is Anthony Erlandson. I'm with a cybersecurity firm, Cyveillance. And I have a question maybe particularly for the ambassador and Christine Bliss.

You had mentioned sort of that everyone, all these -- that everyone is an equal participant in the web, in the Internet, mentioned the education taking place sort of to realize that the localization laws are actually not beneficial, as well as mentioning the different aspects of negotiations that are being put in place to improve information data flow and trade. But I'm wondering what the U.S. is doing to actually improve trust. Because I think that trust takes much longer to build than it does to be lost. And in the wake of the Snowden revelations, I think a lot of trust in the U.S. as an "equal participant in the Internet" has been lost. So I'd be curious if either of you could speak to that.

MR. WEST: That's a great closing question.

Ambassador, Christine?

MR. SEPULVEDA: Sure. I think in terms of the question of what are we doing to restore trust, you have to break that down into trust between whom. Trust between users of the Internet around the world and the American government? Trust between governments themselves? Or trust between users and commercial entities.

The idea, when we talk about equal participants on the network, what we're talking about is a network that's open and global. That we have as much capacity as anyone else to access that network and to create on it and innovate on it, the fact that we do so disproportionately well is true. But that does not mean that our access is greater than that of others. We have made significant investments in networks and we have more robust networks than others, but Europeans have pretty robust networks, and we're trying to encourage the deployment and the development of much more robust networks around the world, particularly in Latin America, Africa, and Southeast Asia. Because just due to economies of scale and network efficiencies, the addition of every additional user adds value for everyone else, and there is also great social and economic returns to having greater connectivity around the world.

In terms of how do we restore, in the first instance, individual user trust relative to what the American government is doing in the wake of the Snowden revelations. The president of the United States has spoken on this on multiple occasions. The president of the United States is committed to civil liberties. That's where he comes from. He used to teach constitutional law at Harvard University. He has exposed and had our intelligence practices submitted to the review of five independent experts and that was subject to -- with hands off, they did their report, they

made their recommendations.—. The president accepted a significant number of those recommendations and is in the process of implementing them.—. What he has said is that he and these programs and these processes will respect the privacy of individuals abroad.—. How do you implement that and make sure that other people accept that as true is going to be a long process.—. But it's one that we're engaged in.

In terms of trust between governments, there are a number of governments that expressed extremely significant concerns and on which we have been working on a bilateral manner to address their concerns to the best of our ability between intelligence experts and between their operators of their intelligence practices and ours.—. So Germany and Brazil are two obvious examples, and we continue to do that work on a bilateral basis on a regular basis.

And then the other thing we do is we go out to the world.—. We go out to the Freedom Online Coalition.—. We go to the Human Rights Council.—. We go to any number of different venues in which people are welcome and we participate in the conversation.—. They're welcome to challenge the practices of the United States.

Again, this is an evolutionary process.—. Last year there was a Human Rights Council proposal adopted unanimously proposed by Germany and Brazil, and I'm sure they will be coming back with additional proposals and will continue working out what is appropriate.

MS. BLISS: And I would just add to that that, you know, as trade negotiators, being able to build and maintain credibility is one of the most basic things we have to be able to do to do our jobs.—. So I think that's a continual challenge that we face and consider to be very, very important.—. So I think across the board in the negotiations we're engaged in, we're trying to do that and continue to build on the relationships that

we've created.

The other thing I want to say is that I think part of our job is also education, and I just wanted to say as we wrap up here, too, a lot of what certainly has informed the work that we do is I think in the last I would say two to three years in particular, there been some excellent studies that have really I think helped to explicate just exactly how digital trade is really transforming our economy and the degree to which our GDP, our employment, our wages are being impacted by the growth in digital trade.

It's really quite amazing when you look at the figures. If you look at the two ITC studies that have been done just in the last year on digital trade, U.S. GDP has grown by 3.5 to 4.8 percent based on 2011 figures. U.S. wages have increased by as much as 5 percent. So the real concrete benefits, and again, that's U.S. centric, but there are other studies, like the McKenzie McKinsey Study on digital trade that created what we found to be very interesting, the connectivity index. And if you look at that, what they found was that the more connected a country was, the greater the benefit it enjoyed from increases to GDP to employment across the board by 40 percent. And so, again, I think that's part of what we're trying to do and communicate, a sense that we're in this together. That, yes, we as the U.S. enjoy benefits, but so does the rest of the world.

MR. WEST: Okay. We will make that the final word, but I do want to thank Daniel, Christine, Lixin, Richard, and James for sharing their thoughts with us, and thank you very much for coming out.

(Applause)

* * * * *

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.

Carleton J. Anderson, III

)Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2016