THE BROOKINGS INSTITUTION

SECURITY TRADE-OFF? IMPLICATIONS OF CYBERSECURITY REGULATIONS AND INTERNATIONAL TRADE

Washington, D.C.

Thursday, September 19, 2013

Introduction and Moderator:

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

Panelists:

ANNEGRET BENDIEK
Senior Associate, German Institute for International and Security Affairs
Fellow, German Marshall Fund

JOHN S. MILLER
Senior Counsel and Policy Strategist, Global
Public Policy, Intel Corporation

JOSHUA MELTZER
Fellow
The Brookings Institution

* * * * *

P R O C E E D I N G S

MR. FRIEDMAN: Good morning. I'd like to welcome everyone to the Brookings Institution. Thank you for coming here this morning on a lovely day, and of course, thanks to those of you watching on the webcast. Just a couple of procedural notes, first, the usual reminder about cell phones, there's always one. And second, if you wish to engage in this conversation on twitter, we have a hash tag, #TechCTI.

We're here today to talk about confluence of a number of emerging trends that have been dominating headlines themselves, but are starting to come together and bring up some very real policy questions. There are lots of discussions in the trade community about non-tariff barriers to trade and technical standards and how that's changing things in everything from the developing world exporting agricultural products to the west, to information technology questions. At the same time, cyber security dominates the headlines weekly, if not daily. And we are still in the early days of governments trying to figure out what to do in this space of cyber security policy. There are lots of strategies out there, countries are beginning to develop a broad high level strategy, but actually translating that into policy is something that we're beginning to feel around, not just in the United States, but around the world. And the challenge comes when these two forces collide, of how cyber security regulations may impact international trade. And the discussion today isn't going to be quite so much about the relative merits of any particular cyber security policy or the need for regulation.

If you want to hear more about the discussion of cyber security in general, to give a quick plug, there will be a book coming out in January that I've written with Peter Singer called Cyber security and Cyber war: What Everyone Needs to Know, so that will give you everything you need to know. But today we're going to talk about the very particular question of cyber security regulations and how that will impact the international flow of IT goods and services. And with me to discuss that today, we have a fantastic panel that will bring a number of very important perspectives.

So first, we have John Miller, who is Senior Counsel and Policy Strategist for Intel Corporation's Global Public Policy Division. He has been responsible for thinking about their cyber security policy and their privacy policy here in Washington and has coordinated a number of different initiatives not just in cyber security but privacy, human rights, etcetera, and before that he had been a lawyer and focused on a wide range of technology policy issues, as well as engaging in the Washington policy community and has even written an academic article or two.

We also have Annegret Bendiek, who has spent the year here in Washington, D.C. as a Fellow at the German Marshall Foundation. She spends the rest of her time, and here you're going to have to forgive my pronunciation here, German is not a language that I have any fluencies, at the Stiftung Wissenschaft und Politik in Berlin, or the German Institute for International Security Affairs, and she's going to be spending the year here focusing on cyber security policy with a particular insight into transatlantic relationships. So we'll

have some great insight on the panel there. And she has a background in political science, having taught political science, that would be a Ph.D., focusing on the role of Europe as a political actor in the broader community.

And then finally, I'm happily joined by my colleague here at Brookings, Joshua Meltzer, who's a Fellow in the Global Economy and Development Program, as well as a professor at Johns Hopkins, and his work is on international trade policy issues, but he comes here as an experienced trade negotiator and a diplomat, having spent time in the Australian Embassy, here in Washington, and so he's been both an observer and an active participant in debates like this.

So to motivate the discussion, we've released a report today on this very particular question, offering an overview of how different types of regulations may impact trade and the different ways they may do so. And I won't go through the full report but the structure lays out the different classes of regulations we can think about, ranging from government procurement, national security standards, testing requirements and cryptography requirements as well as use of the cloud, cloud computing and international data flows. And we explore different ways that certain types of regulations might trigger adverse consequences to international trade, from sort of the cataclysmic specter of countries trying to actually enforce or to raise national security exceptions to their world trade obligations they've signed, the W2 treaty, they're signatories but they have a get out of jail free card that they can use, the national security, down to sort of the more mundane tradition of just saying, well we need technical

standards for our products to secure ourselves. I propose in this paper further research that needs to be done. This is in the area that brings together a number of important policy issues that themselves suffer from a lack of data and theory. The question of how information technology impacts international development and growth is very important, but also one that most scholars acknowledge is very complex and requires not just good data, but good ethnographic understandings of how countries actually are using technology in different ways. So we need some insight into that. We also need some insight into how cyber security is affecting the market on the demand side. Is this something that we see at the consumer level as a barrier to trade in itself, if countries are raising questions?

Finally, there's, I think, a very real concern that as the cyber security threat grows, and we develop palsy responses, there may arise what I call cyber security ghettos. As rich countries get better at protecting themselves, the threats and bad actors will more and more find refuge in the infrastructure and systems of poor countries that don't have the resources to protect themselves. And everyone in the world needs to understand this threat because as we know, in a networked world, it's not just enough to defend yourself. If your neighbor's insecure, that poses a threat to you.

Finally, I introduce a series of recommendations. They're high level recommendations in four general categories. First, making the point about cyber security ghettos, it's the question of enhancing cyber security capacity. Regulations of course, need to promote cyber security benefits, and draw a line

between regulations and the paper is very clear to not take a particular stand pro or con government interference, just argue that it's important to demonstrate some security benefits, and the importance of a global cyber security capacity, a global defense. International standards should be harmonized. We need to shift away from nation specific standards, and those standards need to balance security needs in very specific sectors and very specific requirements with the benefits that we get from the efficiency of general purpose solutions. One of the key powers of IT is that we have general purpose architectures, general purpose networks that you can run anything on. If we start to impose very specific security requirements based on the demands of infrastructures, then we begin to fragment our architecture.

Finally, we begin to think about the question of how trade and diplomacy can actually promote security, and I know that later on the discussion will dive into some of the recent questions of what we've learned about the American intelligence community in particular and how they behave in cyberspace, and I wonder whether diplomatic and trade voices can serve as a check against the intelligence community's temptation to abuse this cyber domain. So the report is there. I invite you to read it and raise criticisms, respond, take up some of the research questions we have and sort of flush it out and perhaps raise some more questions. We'll start with the discussion, and John, I'd like to get your perspective as someone who's actually building out the IT infrastructure that powers the cyberspace. How are some of these regulations interfering in global trade?

MR. MILLER: Thanks Alan, and thanks to the Center for Technology Innovation at Brookings, and the other panelists and guests as well. Technology and innovation have broken down barriers to commerce and communication at a pace and degree once unimaginable. The internet, this engine of progress and economic growth only operates via interoperable hardware and software products, which were historically not very significantly amongst individual countries, and are deployed worldwide. Of course with the growth of the internet has come a corresponding increase in the sophistication and severity of cyber security threats, to governments, to critical infrastructure, to private sector networks, to intellectual property, to privacy, and countering these threats requires thoughtful deliberation by government industry and civil society on how best to improve security and grow trust and confidence in the use of technology without clogging this thing and economic growth. So again, I thank you for your initial salvo in getting this moving along. I think when you look at the paper, and I have had the opportunity to read it, many of the cyber security policies and regulations that you outline threaten to impede this continued evolution and functioning of what's really been a successful model, by erecting costly barriers to cross border commerce, and replacing the global digital economy with a balkanized system, that threatens continued advancement of both technology interoperability and innovation. I put the impacts into three broad categories to take a look from an IT perspective. You do have direct economic and market impacts on global competitiveness, have impacts on interoperability of technology, and also the cross border flow of data, as I

discussed. And then there really are negative impacts on security and trust that can result from security regulations, which may sound nonsensical, but I'll attempt to explain.

First the economic impacts -- Intel and many other IT companies invest significantly in cyber security R&D and in building secure products and services, and we advocate that governments adopt cyber security policies that foster such innovation. Security, along with power efficient performance connectivity is one of Intel's 3 computing pillars, in fact, and it's around which we concentrate our development efforts. And Intel's committed to advancing security in IT products and services that reflect the latest and greatest in cyber security protection. We believe that cyber security policy should advance this goal in maintaining the IT industry's ability to innovate and compete in global markets, by operating in economies of scale. In our view security regulations such as those outlined in your paper, I think you mentioned some of them, but you know you have local certification and local testing requirements, server requirements, country specific technical standards, country procurement requirements -– they're really not only unnecessary for providing better security, but they create a negative environment that is harmful to IT companies globally, and trade.

There are a few reasons for this. Historically, the IT industry builds, wants, and sells globally, using highly complex and globally integrated supply chains. Many of the proposed security regulations highlighted in your paper effectively function as market access frustrations that could make it difficult

for IT businesses to continue to operate at economies of scale, leading to dramatic cost increases and product unavailability in certain markets.

For example, looking closer at the local testing and certification requirements that we've seen proposed in several economies, as pointed out in the paper, a number of different countries seem to be pursuing this path and mandating that certifications be conducted by certifying institutions that don't follow international standards, product evaluation –- these types of approaches increase manufacturing costs because companies will likely need to produce multiple sku's of products which would otherwise be the same, for sale in multiple countries, product development will slow causing significant delays in time to market and actually preventing the security solutions from getting out there. And compliance costs, of course, will also dramatically increase if such an approach is widespread adoption. Some proposed security requirements are in fact so onerous they may result in driving some companies from certain markets entirely. For example, we've seen requirements that some companies turn over source code, to allow for this type of in country security testing, and it's simply a non-starter for a lot of companies whose business is grounded in IP. And I think the IT industry generally has been successful in advocating against this sort of source code escrow requirements, but it's by no means assured that that's going to continue indefinitely.

Second, I mentioned the impacts on interoperability and cross border data flows. This proliferation of silo'd technical standards and localized security are requirements as discussed in the paper, could impede the seamless

functioning of the internet and global digital economy as we know it. Multiple country specific standards are requiring that non-domestically sourced equipment undergo differing security requirements, can lead to balkanization of the global digital infrastructure that we have helped build, and can threaten the continued interoperability of the innovative technologies that have fueled the internet's growth.

And then other security based policies that we've seen, such as proposed requirements for domestic servers, most recently we've seen the Brazilian government pursuing this, and you called it data protectionism in your paper. The net result of that is likely going to be a slowing or even diminishing across border data flows, which of course are, again, integral to the internet economy itself, and electronic commerce. So requirements such as forced localization of servers pose a very real threat not only to the functioning of the internet itself and that economy, but also to established institutions, that many companies, and citizens indirectly, have come to rely on the U.S.A. safe harbor framework, and in the emerging system of cross border pricing rules in development just recently developed by APEC.

And then finally, there are the potential negative impacts on security itself. The paper outlines the national security rationale underlying many of the proposed regulations and few would question the sovereign right of nations to pursue cyber security or other regulations that will legitimately protect their national security. However many of the proposed security requirements outlined in the paper, while well intentioned, are grounded in a fundamental

misconception from the perspective of a technology company that focuses on security. And that misconception is that the location of manufacture or the country of origin of origin is somehow dispositive of the security of that product. In fact, geographic based restrictions are simply not a reliable way to create better security. Fundamentally, product security is a function of how a product is made, used and maintained, not by whom or where such products are made. Geographic based restrictions not only ignore the reality that most supply chains for IT products are global, but run the risk of creating a false sense of security for the countries who are advocating for these provisions. To advance their national security entrance, at a time when greater global cooperation and collaboration is essential to improve cyber security, geographic restrictions in any form risk undermining the advancement of global best practices and consensus based standards for cyber security, for instance, secure development life cycles in the IT industry. Further, these policies resulting in weaker security will in turn erode individuals' trust in the internet, and the ability of the electronic devices to protect their privacy, thus further threatening the promise of the internet and its ability to continue to spur economic growth. There are many other dimensions in this problem that I know we're going to get to in the panel discussion, and I'm sure the other panelists will talk about them too, so I'll stop there, but in closing, I do want to thank you again for getting the ball rolling on this important topic and I'd further echo your call into the further research and study into the economic impacts of security regulations.

MR. FRIEDMAN: Thank you, and now, this is sort of a very slightly

U.S. centric approach, the large international type companies are predominantly based in America, so I'd love to get your perspective across the Atlantic. How do you see this issue shaping up from the perspective of Europe?

MS. BENDIEK: First of all, thank you very much for being invited here. It's the first time for me here in Brookings Center and it's a pressure and a pleasure for me at the same time, to speak here because I'm from a European and German perspective, I think various revelations and I would like to mention that first we change, I think a little bit our partnership between both sides of the Atlantic, and I would like to explain why. I came here in July and I will spend until the end of April next year, and I realized that a lot of newspapers are reporting about privacy issues from the U.S. American perspective. But the problem is that all these N.S.A revelations really touch on the privacy rights on many Europeans and international citizens. And I am not sure if really the U.S. perspective has got this really strong enough in mind. So many voices on the European side of the Atlantic are afraid that the U.S. are interfering with European rights and an illegitimate way. The practices of the N.S.A. of snooping on the European allies are considered to be reflecting imperial overstretch. And this imperial overstretch in the sense that there is a strong partnership here in the U.S. between the government and big mighty multinational corporations. And they see that as an inadequate and arrogant interference with a privacy offence. It is like reading in the diary of your sister or brother. This is what a lot of Europeans and Germans feel. I can say of course there is a strong, and still a strong partnership between the governmental and executive parts, but this is what the public and normal

citizens feel in their everyday life in Germany and in a lot of parts of Europe, and I think especially in the northern part and the eastern part of Europe. Yesterday the GMF published a report on transatlantic trends, and you will see at the same time that a lot of European and U.S. citizens are in favor of deepening the transatlantic market and they are really willing to support it, but I think under certain conditions. I will explain which conditions these are. It is detrimental both in economic and political terms, and endangers, I think, important current political projects. It is probably true that Europeans and Germans sometimes overreact and that might be, and have no reason to be afraid of U.S. measures aimed primarily at fighting terrorism. But it's also true however, that Germans have had a very negative experience in their past with governmental surveillance practices. And because the experiences of the past still shape much public perception of today, and they will not be overcome easily and must be taken seriously, I would like really to strengthen this point again.

Taking these considerations into account, both sides of the Atlantic must put effort into rebuilding trust, and I think, thank you very much, this was also a big point in your report and you underlined it I think on the page 2, that trust is really a basic condition for entering into a strengthened and deep integrated market. If you have no trust, then customers and consumers will not go to your business or you. And they will favor business enterprises based in Europe or based on European standards on data use and data protection. And I think this should not be our goal, and therefore we should go hand in hand and find a compromise between this data use and data protection. And I think both

are very important. And there are two issues that really lead to a transatlantic free trade and investment partnership. And this is, have guarantees inside of security, and have guarantees in privacy. So what we see in the context of cyber security is, the first important thing is that in the European Union, the European institutions launched a cyber-security strategy, which is very much dedicated towards the fight against cybercrime and building resilience. And the European Commission proposed at the same time, a directive with measures to ensure harmonized network and information security across Europe. And the proposed legislation will oblige companies, and this is contrary to the U.S. approach, to be audited for preparedness and to notify national authorities of cyber incidents with a significant impact. So they are still struggling with what a significant impact is, but I think, and it seems to me that in Germany and also in Europe, this directive will go through in the next period.

So the directive also suggests that market operators will be liable regardless of whether or not they carry out the maintenance of their network internally or if they outsource it. So the EU's singled out a number of receptors which it claimed required a more action on cyber security including private infrastructure operators, and energy transport, banking, healthcare services. This is not critical. But key internet companies, including payment services, social networks, search engines, cloud services, app service providers, e-commerce platforms, video sharing platforms, and voice over internet providers were also earmarked by the EU strategy. And they would be obliged not only to fulfill minimum criteria for security, but also they would be obliged to inform U.N.

institutions or the government when major cyber-attacks have been found.

So in the U.S., the proposed cyber security framework as you mentioned in your paper too, is on a voluntary basis, and a quote allows any organization, no matter how good or bad at cyber security to be CSF conformant. So in some, Europe and the United States are currently implementing different levels of cyber security and privacy regimens. And this creates inconsistencies for companies operating in both jurisdictions and will complicate negotiations to what proposed free trade and investment yield. But I'm sure and I'm convinced that these private actors would push the EU institutions, and here the EU institutions, European Commission and the European Parliament is very important to mention because the European Parliament has got the last say on the finalizing and approval of a free trade investment agreement with the United States. And I am sure that these private companies would push not only the Brussels institutions and European governments, but also at the same time, the U.S. government, to find a compromise on this topic. Because what we see in Europe and in Germany is now more and more people try to find browsers for example that are not based or operate under U.S. standards and U.S. data protection standards. And I think this is a trend, and take this trend seriously, would be my recommendation. Probably in the next part, and I come back to this, I would go more in detail on the privacy aspect of this transatlantic free trade and investment agreement.

MR. FRIEDMAN: Certainly not a question that is going to go away any time soon. So we've got the transatlantic question. Josh, I wonder if you

could put this in a global perspective. You've been following both the transatlantic trade negotiations as well as the Trans-Pacific partnership, and have been a longtime observer of the WTO and how that impacts. How do you see this kind of information security regulation, IT regulations in general both evolving and having a real impact?

MR. MELTZER: Thanks Allan, and let me just say, congratulations on your paper, for those who haven't picked it up, it's out in the back. I certainly recommend it and having a good read of it. I guess taking a step back and thinking about national security, I think it's the traditional dictum at least since probably the time of Machiavelli that no state should rely on others to furnish the weapons they need for their own defense. Yet we've seen the proliferation of trade in weapons. But we might be coming actually to a point where we're seeing a re-assertion of this dictum as countries come to reconceive and understand national security in an age of the internet and economic interconnectedness. But I think these discussions today have also revealed that there are some key distinctions that we probably have to keep in mind when we think through this national security issue in particular, international trade and economic locations. And Allan's certainly done a very good job of addressing some of the cyber security challenges that rise in the trade and the implications. We've also talked on the panel just now about the same issue on the privacy impacts and how this sort of plays out into the trust and security on the internet and trade as the driver of commerce. John's been talking about cross border data flows and the issue there.

And there's another issue which we may pick up in the panel context, which is also the one of economic espionage, which the Mandy Report talked about earlier this year and the implications there.

I think certainly when we think about this issue, the key concept here is this idea that we're living in the interconnected world. And I think there are two valuable ideas that come together here. One is global value chains, and the other is the internet. And both of them intersect with this idea of IT products at least, because we have IT products which we have and are to some extent really a paradigm example of global value, where you change, often manufactured across a number of countries, in Asia, in the Asia Pacific region. So this raises questions from an IT perspective of the security of the supply chains. And then we have the issue of a lot of these IT products being incorporated to access the internet, software issues. And this then makes a whole bunch of other things such as infrastructure where the IT parts are caught potentially as national security concerns, in a way which really didn't exist in the past. It conjures up an image of war fought of their power grid as being a vulnerability but now you don't actually have to be in a hot war to think of this as a potential national security issue. So the question that Allan plugs in his paper, well what can governments do here to address legitimate national security concerns while taking into account the impacts this might have on trade, the broader economic system when we are so interconnected.

Now one of the questions here, and I think one of the key concerns in your paper Allan, is so, when we think about for instance the trade

rules, we think about the WTO, everything about FTAs, we have this national security exception, so the concern is, well, governments may just say this is national security, it's going to fall under this exception, it's a whole audit potentially of rules and regulations. Again it becomes carved out from WTO disciplines.

Before I get to the national security question of course we would have to find a WTO inconsistency in the first place so we could sort of speculate that there might be an issue where you prefer domestic supplies, there are government procurement issues that come up in that context, but let's assume that there's some sort of WTO inconsistency and that there is a national security issue, and an exception that's being claimed by the government. So the basic question is how big is the national security exception? This is sort of an issue which is dogged. I think the trade world for a long time, I mean there's quite a well-known comment by Premier Nikita Khrushchev talking about U.S. export controls and how they should be applied to buttons because they could be used to uphold soldiers' trousers, right? I mean, how big is national security?

Now if we actually look at the WTO national security exception, what does it say? It basically talks about measures which would otherwise be doubly consistent but were doctored for central national security concerns, and these are qualified by whether it's for fissionable material, trafficking arms, war or other emergency situations. Now the key question here has always been who determines whether or not the regulation, the government's claim of national security actually fits within the WTO exception. In a WTO context, I don't think

this has been definitively settled. My sense is that you would probably have a situation with panels in the case where this is before WTO disputes are embodied, the panel would retain the provident to decide, but it would probably extend a lot of difference to the government's claim; this is actually essential national security.

Interestingly, in the most recent U.S. Free Trade Agreement, that with Korea, there is an iteration of this issue in the exceptions provisioned there, where what constitutes essential national security is essentially redefined. And importantly, there's footnote to that exception, which basically says that in the case that this comes up before a WTO tribunal, the tribunal will accept the government's claim that this is essential national security. So in a sense, the Korea FTA at least, seems to point towards this idea of auto-determination namely that it is up to government to claim national security, and once they claimed it there's no room for a panel to disagree with that.

Another area we've been talking about on the panel is this issue of standards. And this is also something that Allan addresses in his paper. And here we sort of get into another WTO agreement, the TBT agreement, Technical Barriers to Trade. Now there's a range of complicated issues here. On one level, there is this concern about the economic impacts of essentially standards that are going to make it difficult for countries to make, it's going to require additional testing for security reasons, and it's going to impact on scale when it comes to global value chains. Now the TBT agreement does attempt to get at the, in the sense that it does try to limit unnecessary regulatory or gratuitous

diversity, instead of standards. And one way it does that is through this expectation that countries should essentially try to harmonize standards where an international standard exists. But, and the but here is very important, essentially you only have to do that where that standard would be effective and appropriate to fulfill a legitimate objective. And in this case what it means is that if the international standard existed and it wasn't considered sufficient, certainly the international security would be good enough to be reason to adopt your own standard. So, that is probably not going to help us all that much in many respects.

The TBT agreement does also have a range of, I consider pretty robust procedural rules regarding the development of standards, and these are sort of another avenue where countries can at least have input into the development of standards. We'll get into this a little bit more, because this actually might be where we're heading at least when it comes to this particular issue. Another key discipline in the TBT agreement is similar to the one on national treatment. I mean article 2.1. Now the one thing we do know about the TBT agreement is that it doesn't have an explicit exception agreement for national security. It doesn't actually have an exceptions provision at all. But recent WTO cases, country of origin labeling, the Tuna II case, clove cigarettes, these all came out in very close succession, have basically said that the balance and gap between national treatment and the exceptions provision is itself for now reflected in the national treatment provision in the TBT agreement, so in a sense, the type of exceptions that we know of and that exist in the gap now essentially

are in the TBT agreement, so again, what this suggests is that an essential security claim would survive in the context of a standards case under the TBT as well.

So I think what this points to, at least in this specific context where we're concerned about the breadth of the national security exception and its implications under the trade rules, is that they probably define the limit of trade in many respects, and so there's probably not a legal solution to many of the challenges that we're talking about specifically in this area here but what we're actually looking at, and Allan, you get at this a bit in your paper, is that we need to develop mechanisms to try to get governments to take into account the trade and economic implications of national security measures. So this is really going to be more a question of diplomacy, of politics rather than law.

MR. FRIEDMAN: Well thank you Josh, and by the way, for those who are interested in learning more about international trade law and IT flow in particular, Josh had a paper that came out earlier this year that was very, at least for me as someone who is much more comfortable reading technical standards in the international treaties that govern how you're allowed to define technical standards, it's a great introduction to the legal side, if anyone's looking for that. So, let's take a step back and tell some scary stories. So, John, you used the word balkanization. And I'd love to hear, the panel tell some worst case scenarios of where we might be heading, or if you don't think it's as big a threat as we've been talking about, but around this concept of a balkanized internet, or a balkanized global trade society.

MR. MILLER: I think all of the panelists have talked about some of the risks already, but I think in particular looking at for instance, the national security exception that Josh was just talking about, I think there's a very real, and looking at again the silo'd regulatory approaches being taken to cyber security, there is a very real threat, kind of a domino type of affect and a kind of cascading series of bad policies that could end up resulting, because simply, at the same time, at least as a global technology company, at the same time, we are advocating against such policies in India or Russia. We're also advocating against them here in the United States. And the world is watching the development of this area everywhere. So to the extent that, frankly, just one policy really gains traction in one country, I think that there's a very real risk of retaliatory effects everywhere, and it is going to be a situation where you have a company that is a global company that does business all around the world potentially, having to comply with forty, fifty, who knows how many sets of technical standards, requirements and local certification and testing requirements, etcetera. So I think that balkanization is a real threat because it's going to interfere with the ability of companies to do business globally, and the same way they do business, and this isn't just an issue of corporate profits, prices will increase, security technologies won't be able to get to the places that they need to get to and consumers will suffer by having worse security, and it in fact will mean higher prices in the technology they buy.

MR. FRIEDMAN: I think it's a really good point that it's not just about the price of the technology, that we're actually going to make security

worse if we don't have a way of easily and efficiently distributing ways to secure the stuff that already have. Annegret, do you see a threat from sort of a balkanized world?

MS. BENDIEK: Yeah, of course, first of all, I think we have to distinguish between the OECD world and the non OECD world and I think the OECD world is based on principles and standards and I think of course it's in our interest to maintain these principles and standards and we have to struggle and fight for compromise which kind of standard we would like to see in the future for that data use and data protection. Because it is not only about security, and security is a very vast term, you know? When I think about security from my perspective as an academic working for the Stiftung Wissenschaft und Politik for the German city, we are politically independent, I would like to add, for me it's human security, you know? And human security is linked to consumer protection, but has got the perspective of the individual and use of the consumer, using the internet and going into the cyberspace. And I think we are here really in the beginning. And I am not convinced, and when I have looked at critical infrastructure protection in Europe, I am not convinced that private actors are able really to do self-regulation. And we have seen it in the past, and if you look for example at the seven and eight sectors of critical infrastructure in Germany, of course you will see, of course the banking structure has got high standards, but if you look for example to the house sector, then you see all the transport sector, then you will see, okay, these standards do not fit anymore, really to the challenges we are facing.

MR. FRIEDMAN: Why not have an IP addressable heart monitor?

MS. BENDIEK: Therefore, I think that there is a role for the government, and we have to distinguish the government role between three dimensions. So the first is security. And I think here the government has got a role to play in the sense that they should guarantee minimum standards. And then I see the field of the dimension of the economy and you look at the value chain and then I think you need this government as a change agent, because I think that we are confronting with industry 4.0 we call it in Germany, and I think here you can find sustainable future solutions for different parts of the whole of our society, when it comes to education, when it comes to environmental policy, and I think it's in the benefit to our wellbeing as society.

And then I think how we are looking at the sphere of social communication and all the social life. And I think here the government should play no role, in the best sense. But it's hard, so it's hard because we see that if some agent, agencies are so strong, that they can interfere in individual privacies, and also private companies. Then it's becoming critical. Therefore, I think my assumption is the government has got different parts to play. But I think when it comes to transatlantic relations again, it's our goal to make or to bring this transatlantic free trade and investment partnership alive, then it goes beyond normal free trade and investment agreement. It will set norms and standards. Then of course I think in the long run, it's in our own interest, from a European but also from a U.S. perspective, that we as the west, or we in the OECD world, find minimum standards for the big challenge of big data.

MR. FRIEDMAN: Alright. Josh, do you have thoughts on sort of a balkanized internet, Balkanized trade society?

MR. MELTZER: Yeah, I think that picking up on both panelists' comments that the potential for balkanization of the internet and this issue of cross border data flows, I think it's something to spend some time thinking about. I think one looks at, for instance, what China has achieved in terms of its control and regulation of the internet. You can see the potential for systems to become increasingly closed in some respects. I think what, though, is also important here, is this issue which has been raised, which is the question of trust in the internet and they NSA issue, whatever one thinks of it, I think is certainly brought to the fore, this issue of trust and this issue of privacy, and the extent that consumers are going to be increasingly willing to provide personal data in the furtherance of ecommerce online if they don't feel confident about the way that their data's going to be used. Now it's a much bigger debate I think beyond the specific issue of what one thinks about the scope of U.S. surveillance of the web. It's also, I think, comes down to some very, at times, significant differences even within the OSC data between the OSC and U.S. and EU about the concept of privacy and the way consumers think about privacy of data. What actually is a technical issue about what actually can be done, for instance, can you actually have a right to forget? Is this actually achievable? And so it's also an issue about communication with the public and making sure that, I think there's a better set of dialog about what actually is going to be possible going forward.

MR. FRIEDMAN: It's a great point. It's one thing to talk about the

right to forget and it's hard to figure out how that translates to a notice that says there are cookies on this web site. I wouldn't say that's a sufficient privacy warning. So as we move past this into, and Annegret, you alluded to this, in a discussion of how we're going to address this, it's not just enough to stand up and say this is a problem. It's not even enough for companies to try to raise their interests, particularly when those companies are increasingly seen as representing one country's interests. So what are some of the institutional factors that we're going to have to rely on to rebuild, as all three of you mentioned, to rebuild this trust and promote the benefits of global flow of IT goods and services? Josh, do you want to continue on your line of thinking?

MR. MELTZER: Well, I think possibly the TBT, the transatlantic partnership and trade negotiation is going to be one big call where this is going to be key issue and there's going to be an opportunity to discuss it. I wasn't sure when you were referring to large companies pushing for compromise whether that was a good or a bad thing. Hopefully, there will be compromise so I kind of feel that would be a good thing. But breaching essential different ways that people understand how their data should be used, I think the conversation will occur across the transatlantic, but I think it's a conversation that's going to have to be broadened out globally in many respects. I think that's probably one of the mechanisms going forward.

MS. BENDIEK: Yeah, maybe we should come back to the profit and the benefit how we can boast here out of the transatlantic proved it investment partnership. As far as I know there are some studies coming out that

they will highlight the benefit for the U.S. government. From which the government can hear out of the TTIP will be higher than for the Europeans, first of all. The second point is that the U.S. government is at the same time negotiating a

Trans-Pacific Partnership. And I think the U.S. government needs a kind of perspective of TTIP for a better position negotiation position with the Trans-Pacific region. Therefore, I think and also, in our best interests, because we have here the most dance and intensified economic partnership globally, it should be in our interest not to have, I think also from the European perspective, not to have our European and German perspective on transatlantic partnership but also to try to get into the U.S. perspective, so the U.S. side. And I think this is valid also for the U.S. side, that they should try to understand why the Europeans would like to see these kinds of minimum standards. This is my first point. Because I think the U.S. –- it's not any longer in the position, it's in the perception from the Europeans, that they can rule the world and give us together the stability we need alone. And I think it's too costly, you see it in your bloodshed.

MR. FRIEDMAN: That's a separate panel.

MS. BENDIEK: And even the Europeans are confronted with the economic problem, and I think we are on the best way to handle it, but nevertheless, when you look in population terms and then we will see that other areas in other regions are popping up. And in the best sense, I am convinced that in the term or in this fear of privacy, we need of course, not only exercises in the field of cyber security and the U.S. and the Europeans have done that in the

past, but we also need new exercises in the field of data protection. Which means that I think the newly established working group on data protection would show that most of the European governments and data protection supervisions would ask for, for example, a no spy agreement, which is negotiated between the U.S. and Germany, but they would also like to see it between the U.S. side and the Europeans. And that would be a kind of trust building measure. That you know Europe aligning together to N.A.T.O. and you will enter into this TTIP but at the same time you have to know that you do not spy on each other.

MR. FRIEDMAN: We're going to circle back to that in a moment.

MS. BENDIEK: But I think this is trust, and without trust, you will never enter in an intensified free trade agreement, that is for sure. And that is not my personal conviction, this is what I can see when I read all our European newspapers. And therefore, I think it's a very important point.

MR. FRIEDMAN: John, there's a question on organizations and institutions that might help in this area, particularly allied to technical standards. Are there natural leaders that you see bringing us together?

MR. MILLER: First of all, I do want to echo what the other panelists said about there being opportunities present in the trade negotiations that were mentioned. But we've obviously talked about the NSA surveillance situation a few different times already and I think one of the things that that highlights is that this is going to call for more than a mere diplomatic solution. Right now you've got, for instance, I mentioned Brazil earlier, and they won't even come to dinner here, so I think that that raises in some of the issues that

we've seen come up in the internet governance context. You had at the WCIT in Dubai last year major economies advocating for changing the way that the internet is governed, under the guise of security or based on security and I think that because it seems –- because of that lack of trust between governments and because of the fact that the critical infrastructure and the global digital infrastructure itself commercially, is owned and operated primarily by the private sector, government led, top down solutions, whether in the standards area or else where they likely are not going to work, there's going to be a necessity for partnership and multi stakeholder solutions. And I think that was one of the major themes of last year's conference, and working with OECD and APEC and others to expand adoption of efforts to promote trust again, is a very important tool we have, and also just embracing multi stakeholder approaches over government centric approaches, I think is an area that hold promise.

MR. FRIEDMAN: I want to turn it over to the audience now. We've covered a lot of different topics, and the overlap of some very important trends that are going on right now. Just some reminders about the question process here at Brookings. It's customary to rise and introduce yourself, if you wish to remain anonymous, that's okay too, but perhaps the most important features of a question are that they're relatively short and that they end in an interrogative punctuation mark. So we have some mikes in the back, if there are questions from the audience. Yes, on the aisle here.

SPEAKER: Hi. I'm Fred Altman and I have a question involving just overall national security. Obviously, presumably the NSA is gathering all this

information to prevent terrorism, and to some degree has been successful, even for some European threatened terror. I think one has established both who's going to get what information that needs to be gathered to prevent terrorist attacks, cyber or otherwise, and then who's going to do that, obviously if one country does it, it's going to be highly biased.

MR. FRIEDMAN: I think turning on this question of the NSA, and there's this sheer mount of power that they have, I think that was a big complaint. If one country gathers all this information, does everyone have the right? How does that play into the questions that we've been talking about in terms of building international trust? Are we going to ask countries to surrender power or are we going to look for a more equalized environment where everyone has this capacity? Do you guys have some insight into?

MR. MILLER: Well I think it's pretty clear that the NSA surveillance controversies have amplified all the concerns that you articulated in your paper. It's also made the entire area of security policy both domestically and globally more complex. I'm stating the obvious, but in the U.S. alone, there are no fewer than twenty bills that have been proposed that seek to address one aspect or another of the NSA surveillance disclosure, so hopefully Annegret and others will be happy to hear that we are attempting to address them from a policy perspective in the U.S. And I think there's also been, and I kind of alluded to this in the previous answer, it's really been an impact on our ability to negotiate with foreign governments and policy makers because of this lack of trust. And that's another factor. It's raised awareness of these issues to a much wider audience.

It's not just panels discussing security that are aware of a lot of these issues now. All of the political class globally now, and I think Annegret mentioned in her opening that this is something that's talked about on the streets, and it's an issue for people generally. So this is not an easy solution, and I think you asked about, is the technology capacity itself something that we need to bring, or distribute more evenly and not just have it concentrated in one government or another? I think that that's the wrong approach in that we should be looking at what are the rules by which, I mean, these are governments using technology that is primarily created by private industry, so what are the rules that should govern, at a very high level globally, government and our industry interactions with respect to our use of technology, the various technologies, whether in the surveillance context or for censorship purpose, or other areas that impact human rights, privacy, civil liberties, etcetera.

MR. FRIEDMAN: Alright, your thoughts on this talk about no spy clauses earlier.

MS. BENDIEK: Yeah. I take this point, fighting terrorism, very seriously, because I worked larger in the past, and I published a paper on U.S. EU transatlantic partnership in the fight against terrorism. And I know and it is right, that fifty attacks have been prevented because of these snoopings and these data storages. But nevertheless, I think we are coming back to overall questions and, my daughter for example, is now attending a middle school here in the U.S. and on September 11, it was for the U.S. it's a big day. And it's like a trauma in your knowledge and in your experience, in your national experience,

and this is very important, and I think, and we showing up with a lot of solidarity for this event, and as a western ally. And I think this was 2001, and we are now in the year 2013, and we should ask if after twelve, thirteen years, fighting terrorism, we should ask ourselves again, what is the right balance here between security and freedom measures. Because I think it's not the right way also in the transatlantic, to continue this, the war against al-Qaeda and affiliates. I think there are reasonable points you can raise up that the fight should continue, but nevertheless, the question is, is there not a way to go beyond the war on terrorism and the war against private actors? Could we not strengthen in the future criminal law measures in order to fight international terrorism? And that leads me to the point that I think it's time to strengthen international law enforcement in this matter. Which means, for example, that we have got the European Budapest Convention on fighting in this context for fighting cybercrime, and I think it should be, and it might be in the interest of our countries, that we find more and more other third countries which are willing to adopt also this Convention and to implement it. And I think what we are confronted with was phased states, and states around the world, which are not able to safeguard minimum criteria in the fight against not only terrorism, but in the fight against international cybercrime. And I think that here a lot of efforts should go into the field of diplomatic life.

MR. FRIEDMAN: Joshua?

MR. MELTZER: Yes, just briefly. I think the NSA issues are interesting. I'll try to be brave. I think from the U.S. perspective, there are two

very different lenses here. One is, what has been the impact on U.S. citizens, and there's a whole series of constitutional considerations which flow from that. And then there is the broader question about the extent that the NSA has been collecting data from citizens outside of the United States. Now on the U.S. side, you have the debate has been, I think, about whether there are appropriate safeguards in place, what's the oversight of the NSA, in terms of its decision on whether they target particular individuals, the role of FISA, and the like, and whether there are reforms that can be put in place to improve the process. And I think on that front, I'm not suggesting that this is a system that can't be improved, but I think also, when compared, say, for instance, to a variety of countries in Europe, Germany, France, included, there's probably more oversight here of the same data collected here than there is in say Germany and France, though I think that on that side, I'm not saying that all these countries couldn't do it better but that's a particular debate that each country has internally.

Now I think on the question of collecting data outside the United States, I think we just realized how good the NSA is at doing it. Now, everyone spies on each other, essentially, and no one likes it when you find out about it, but it's not going to stop. Now that's not to say that when it comes to countries that are in alliances, who share common western values, there might be a scope of further cooperation, and my understanding is that the security agencies are talking to each other about why is it that further data can be shared in this space. So I think that is going to be a further ongoing thing. This though, gets back to some of the things you are pulling out, which is, there are impacts here which is

sort of how things are played out in the political arena. And the way the public now responds to this, I think it comes to, say, for instance, the trade agreement space, where one of the concerns is that you're going to have, negotiations are going to be cramped, essentially. The space for compromise is narrowed a bit, because there's going to be heightened public focus on this issue, and in a way, whether or not we think it's accurate or not, it's going to depend on how the negotiators come together and reach agreement.

MR. FRIEDMAN: Right. Should also add that I have a piece coming out shortly, on foreign policy that talks about how the allegation that the U.S. government asked an American technology company to change its product for the purpose of surveillance is probably the most damaging long term revelation that we have, for exactly the long term reasons we've been talking about today, that there is this open system of international trade that's usually seen as distinct from national security and this is wrenching those two worlds together. There's a question in the back.

SPEAKER: I'm Frank Jordan with Oracle. My question is for Dr. Bendiek. I hope I'm not mispronouncing your last name. My question is about the fundamental governance challenge presented by the internet in general and cyber security in particular, a challenge in that it is a global phenomenon.

MR. FRIEDMAN: A little louder? The mike a little closer.

SPEAKER: Oh, sorry. It thought it was very loud, sorry. The fundamental governance challenge presented by the internet in general and cyber security in particular, a challenge because those are global phenomenon,

happening in the speed of light, and government and public policy responses are generally developed at the national level, and I think it's fair to say, don't happen at the speed of light. So, in particular, when you consider that governance challenge, and on the very specific and narrow topic of development of technology, design, development, manufacture of technology, what kind of options does it leave to government authorities, even at the regional level of the EU, to develop, I think you said something like minimum requirements or minimum standards, something like that, that would actually help rather than hinder the response. I'll just give you one figure that sort of echoes what John was saying. My company Oracle spends about 5 billion dollars a year on R&D. And actually John's company Intel spends even more, so I'm not here to sort of beat my chest about it, but there's a reason why we spend that much money, and it's because we have a global return on investment so we can afford to do that. And also because there is a benefit in the sophistication of the product, security, assurance of the product, richness of the security features of this product, etcetera. How does that square with a country specific government developed security mandate?

MR. FRIEDMAN: What does Brussels know better than Oracle?

MS. BENDIEK: For example, we make this experience now in Germany, because we are negotiating this thing, as IT legislation, about reporting major cyber-attacks for example, and implementing minimum standards for each sector in the critical infrastructure. And what the government of interior is doing now, and I find it a very open process, they sit together with a lot of enterprises

and dealing with each sector and find sector based solutions. And then they say, okay, of course, minimum standards should not intervene in small, medium or small enterprises for example, when the investment in security is so high that the enterprises after that not any longer able to make their business, then they makes no sense. Then they say of course, we have to be able to distinguish between small, middle and large scale enterprises. And the larger the outcome and the benefit and the profit is, the more we can expect that the company is investing in standards and security. And they also are negotiating that small enterprises should be supported financially by the government. Because Germans like it when it is cozy, cozy in the sense, oh, it's secure, I know my water is fine, I know that the transport system works, and we have not big aspirations, but what we would like to see is a good neighborhood and that things are working well and therefore it's like to have this good feeling of life, and therefore, I think it's the interest of a lot of enterprises but also for the government, but we have got these minimum standards. And then additionally, I think there is a strong belief that quality sells out in the end. And we believe in quality and we believe in testing the quality, and therefore it's like a trademark. And therefore we are willing to invest in this trademark. And let me say that in July, for example, that was the answer which Angela Merkel, the Chancellor, gave in front of the public and it was a reaction, a public reaction on the NSA revelations, that the German government said it would like to see implemented an eight point program on European international data protection. And that entails in principle the idea of technological sub-morality, which is not good,

because it contradicts basically the idea of liberal order and of liberals as a whole. But it would like to see more European enterprises and European investment, and I will not go back to this case Airbus and Boeing, but I think the idea behind is really to strengthen enterprises and to strengthen security measures as a trademark, and to be more competitive and to have something in your hand, when you are negotiating with partners, but also with other third countries, in international trade, and in investment. So, I think nevertheless, that it will be a part of our future, that we have these kinds of minimum standards. And I do believe that multinational organizations like Intel and like Google and amazon and Facebook, etcetera --

MR. MELTZER: Or Oracle.

MS. BENDIEK: They will be challenged in the future, or the other way could be, that they could be even strengthened, but I think this is only possible when they show up with a kind of global or western or transatlantic perspective on consumer protection and minimum standards on individual security.

MR. FRIEDMAN: Okay, we'll check in later. Question here on the end.

SPEAKER: I was wondering, how do you square a very particular presentation of why you have to have some types of protections in countries to minimum standards, but suppose we all start doing that? I think that's what your paper gets at quite articulately. For example, the Chinese have come up with something called the MLPS, the Multi-Level Protection Scheme, which includes a

lot of very problematic provisions for our industry to do business there, and we have posited to the Chinese that actually it will leave the Chinese economy less secure than more secure. So how do you go forward with your idea, your description about what Germany is doing, and if everybody starts doing that, how do you get the most secure outcomes? How do companies like John's company, who built their products to meet the potentially hundreds of minimum security standards, in a way that leaves us more secure? Thank you.

MR. FRIEDMAN: Annegret, do you have thoughts?

MS. BENDIECK: I think that in the past it has been shown that safe regulation is not really the way to go in the sense that if you believe that we are belonging to the western world, and we are believing in western principles, based on human rights, and privacy principles, science not only on a national or regional but also on an international level, if you would like to continue on this path that you would like to believe in enlightenment and that individuals are here in the front, also in the world of consumption, but also in the world of business as a whole, then I think that here a new deal is needed between government and private actors. And this is the first time that private actors have got a role to play in this security field, because the government, despite the NSA at the moment, the governments are not able to handle minimum security standards on their own. Therefore you need, not only for the investment or the regulations, the mighty stakeholder approach; you need really strong public private partnership in the best sense. And public private partnerships means that it is not the end of self-regulation, but it is coming to a common goal. Therefore, I think the phase of

digitalization is also a little bit the end of the phase of liberalism, in when it comes to the cyberspace.

MR. FRIEDMAN: That may be worthy of a full discussion in its own right. I may jump in here and talk about some of the challenges of, there are international standards, and in the paper I specifically mention common criteria and ISO and there are some others. Those have the problems that they also add costs. And you can also go out both into industry and certain government voices and say, well this is too inefficient, and then the final point of which I talk about at the beginning of the paper, is the question of whether or not the, and I think Annegret was really driving at this, that if the market itself won't demand the solutions, then governments can play a role, not in shaping standards, but in shaping adoption. In the United States, the current path is on positive incentives, but that's not to say that a government couldn't opt for the stick as well as the carrot. I don't know if you guys have thoughts on that.

MR. MILLER: Well, just to respond to that and some of the last couple of questions to Annegret, I think part of the seeming disconnect may involve differences in the use of terminology. On the one hand I heard Annegret questioning the approach being taken here and in the cyber security framework, because it's being perceived as voluntary, which it is, but I think you characterize it as self-regulation, and I think you said something like self-regulation doesn't work. But on the other hand you're kind of acknowledging that while governments don't actually have the technical expertise to impose minimum security standards or perhaps even to know what they are so they have to work

with the private sector and industry and I also thought the way you were describing what's going on in Germany and the EU essentially allowing for different segments of the economy, particularly small and medium enterprises to perhaps have a different set of standards than large multinational companies, to me, translates into flexibility, which is what this cyber security framework is attempting to do. So I think at the end of the day, there will be some movement one way or the other, but to my knowledge, Europe is watching very closely to what happens with the cyber security framework that's under development here. I think if you're going to preserve flexibility and you're going to acknowledge that private sector expertise is a necessary component in any security solution, that it's not going to be possible to just have kind of a minimum set of standards imposed by government on industry.

MR. FRIEDMAN: I think there was a question in the back. Alright we'll take one there, and then quickly we might even be able to squeeze another one in on the front here.

SPEAKER: Alright, thank you. My name is Tom Klaus, I'm a student at the American University here, and I'm from Germany as well, so I can more or less understand your standpoint. And I've been listening to a lot of things about trust here in the last minutes, and it appeared to me that losing this trust in internet security should be a bad thing. But, from my experience, the internet didn't become insecure overnight. It was integral in it all along the way. And what is happening or has been happening during the last weeks and months is rather that the people got aware of that fact, that this insecurity which I

wouldn't believe to be a bad thing. I think that this is a good thing, that there is criticism, that there is suspicion, suspicious people about that fact. So isn't it a good thing, that the people are aware of this insecurity?

MR. FRIEDMAN: I'm going to use the moderator's prerogative to table the questions of the normative evaluation of Edward Snowden, but what are we going to talk about? But I think what we can do is revisit this question of trust. This is something that the Department of Commerce of the United States has said, why is privacy important, because we need trust. So, are there things we can do to rebuild trust in the fallout of what we've seen this summer? Josh, do you have thoughts on rebuilding trust?

MR. MELTZER: I don't have much to add, I think what I said before about, I think part of this is going to be about having a conversation about probably picking up the question, to some extent, of what can we expect from the internet, and maybe have a better understanding amongst consumers and people generally, about how the internet works and what they can expect from their data. I think on the privacy side, I want to just pick up quickly one of the comments that you made just before about how to get at this issue either through minimum regulation or through in a sense a carrot approach. It seems to me that it's one of the transatlantic divides here, which is a U.S. perspective that essentially the focus is on having a particular outcome on the privacy side and in giving companies a role in trying to achieve that outcome, with some FTC oversight, and the EU approach which is to have a fairly deregulatory approach. And I think the EU perspective, the absence of the regulation here, translates into

a, well it's a self-regulated industry, doesn't really work, and in the U.S. perspective becomes, this is unnecessarily burdensome, and is focused on regulation and is more concerned about outcomes. So there may be a space in there where there may be in fact an agreement and an approach that gets at this broader issue, the fact of different regulatory approaches, not only in a transatlantic space but globally, focusing more on outcomes, and giving industry and their players, who actually have to implement it, the space to do it in the least cost effective, most efficient way.

MR. FRIEDMAN: Thank you. We have time for a very quick question in the front.

SPEAKER: Hi. My name is Ross Hanser; I'm an attorney in town. So, there's been talk in the last few minutes about shared values and sharing and aligning core values especially on this side of the panel, and truly at the level of commitment to the enlightenment, and individualism and liberal democracy and surely that's all true, but I guess I've come to wonder or doubt, if that's true at the more specific level of individual privacy and whether it isn't the case that the core consensus has been fractured a bit. Americans come to this, as you mentioned, from a very scarred perspective from 9/11, and that might lead to a different view of what kind of state power is appropriate and I think you also referenced to earlier or at least alluded to, the history of the Stasi in Germany. Those lead to, or could lead to very different perspectives about the proprietary in ascent of state power in this area. So I guess the question, the interrogative punctuation at the end of this is, do you really believe we have shared values, or

are Americans and Europeans and others sort of set on different courses on this issue?

MR. FRIEDMAN: Very briefly Annegret, and then we'll give John the last word.

MS. BENDIEK: All is relative, you know? But I think we have shared values and I come to this assumption because it's very easy. You could look at other parts in the world and you will see that their mostly different understandings of the social and welfare life are the rule. And therefore, I think if we would like to safeguard our old way of living in this sense, probably not on this high standard, then I think it's absolutely necessary, because we have got swing states. Like Brazil challenging, of course in the future, questions of internet structure and cyber security in a global stage. And look at China, of course. Even in Germany, for example, the official policy is that of course we have got strong allies in the U.S.A., but we have also, and we would like to see strength and cooperation with so-called shaping powers. JA? And these shaping powers of course, for example, China, Russia, Brazil, India, South Africa, etcetera, Indonesia, and I think of course, it's about exploration of new markets, but nevertheless, the transatlantic market is the biggest one globally. And until now we can really shape international standards and rules, but of course, we will be challenge. And I think that the OECD world and the western world in the long run, will struggle to safeguard these principles, because of course, China is challenging us and has got its own memory and history and way of organizing their economy and their society.

MR. FRIEDMAN: Alright. And John, any last thoughts on shared values?

MR. MILLER: Sure. I think there are shared values, certainly amongst western countries, shared commitments to human rights and privacy and I think globally there is really a commitment that everyone has to, or should have anyway, to trust in the internet and in technology, because of the importance that that plays. And I guess I would say that we consider it a value. One of the things we think that can bridge the divide is to talk about accountability as a principle and a value, and a lot of what this boils down to I think –- we've talked a lot about Snowden's disclosures –- is accountability. What are the accountability principles that government should be held to and what are the accountability principles that corporations should be held to. We've certainly done a lot of work in both the privacy and security context to try to put forth the notion of accountability as a much, again, a much better organizing principle than regulation.

MR. FRIEDMAN: Great. Well thank you. So I think from the discussion today that it not only affects everyone, but it really touches on a huge range of issues and we're lucky in that this is a nascent area. It's only going to get more interesting, more complex. So we need to keep exploring it, and there are real differences, but at the same time, I think the differences are not insurmountable. So, I want to thank John, Annegret and Josh for joining me today, and in the interest of international internet standards, today is International Talk like a Pirate Day, so I hope you'll join me in giving them a hearty round of

applause, and thank you for coming.

* * * * *

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