DIGITAL-2016/10/07

THE BROOKINGS INSTITUTION

SAUL/ZILKHA ROOM

DIGITAL POLICY LESSONS FOR THE NEXT ADMINISTRATION

Washington, D.C.

Friday, October 7, 2016

PARTICIPANTS:

CAMERON F. KERRY, Moderator
Ann R. And Andrew H. Tisch Distinguished Fellow
Center for Technology Innovation
The Brookings Institution

JANE HOLL LUTE
Chief Executive Officer
Center for Internet Security

DEAN C. GARFIELD
President and Chief Executive Officer
Information Technology Industry Council

NUALA O'CONNOR
President and Chief Executive Officer
Center for Democracy & Technology

* * * * *

P R O C E E D I N G S

MR. KERRY: Good morning. So yesterday at a similar discussion Darrell West who directs the Governance Studies program that I'm part of presented a paper that showed the losses to economies and some national economies that come from internet shutdowns. Today we're going to continue to explore the global role of the digital economy, and I'm Cameron Kerry. I'm the Ann R. and Andrew Tisch Distinguished Visiting Fellow here at the Brookings Institution and part of the Center for Technology Innovation in the Governance Studies program. Today I am presenting and we're releasing a paper called "Bridging the Internet Cyber Gap: Digital Policy Lessons for the Next Administration." It is a look back at what the Obama administration has done in this field and based on that what the next administration can learn in particularly some recommendations about how we can splice into the DNA of the federal government and the White House and the Executive Branch, the lessons of the last seven years.

So I'm going to present briefly the paper. Hopefully we'll have the presentation up on the screen so I can do that. I think most of you have paper copies, but there is a URL which you'll see on the screen if you want to link to it. And please silence your cell phones. We encourage you to Tweet under the hashtag #digital policy.

So the paper draws on my experience at the Commerce Department through the first administration into the beginning of the second administration. As the general counsel of the Commerce Department, I led the inner agency committee, a subcommittee of the National Science and Technology Council that produced the Consumer Privacy Bill of Rights and led international engagement on privacy issues particularly with the European Union. I also performed the duties of the Deputy Secretary on cyber security issues and a number of other security and law enforcement issues and served for a spell as the acting secretary before the confirmation of Penny Pritzker. We

had over the course of those four years some successes: the development of the Consumer Privacy Bill of Rights, applying privacy principles to the new user-generated digital environment. And I think some progress in engagement with the European Union, and I think progress in working with partners within the administration sort of put into the national security discussion. Issues about innovation, about competitiveness, about internet governance and trust in the digital economy. Well, of course, all of that changed when the Snowden stories broke. And it was apparent to me at the outset what the damage would be to trust in American companies, trust in the global internet to trust in America's brand, but I think some of that damage was compounded by the initial response which was said to trotted out the President to say, don't worry no U.S. citizens are being spied on. And of course this sent a red flag up around the world. I think what we saw in that response was looking at the issues, the Snowden disclosures, through the prism of national security and fighting sort of the previous wars. Wiki leaks, how do we contain the intelligence damage and the spying stories of the 1970s when we had revelations of domestic spying by the CIA and the FBI. And I think with a blind spot to some of the broader implications, and that reflects what I call the "internet cyber gap" in this article.

So you see in the red column we've got intelligence, public safety and security and the agencies that deal with that. On the right hand side, the internet side, human rights and the digital economy. And then bleeding across both are governance and norms. And the name internet cyber comes from an observation by Danny Weitzner who started out in the administrations Commerce Department became the Deputy Chief Technology Officer of the U.S. This world is divided, this world is talking about people who deal with these issues is divided into people who call it the internet and people who call it cyber. Hence, an informal interagency group that I convened we dubbed the

internet cyber group.

So since the Snowden revelations I think we have seen a significant improvement in the way that the administration is dealing with these issues. We've seen as a result of time and a chorus of voices a change in the way that the administration looked at these issues, the engagement of non-security agencies in the discussion and a lot of changes as a result. A lot of this comes about because of the President's personal engagement. He initiated the review board. If you look at who was on that review board, Jeffrey Stone from the University of Chicago, Cass Sunstein at Harvard but formally at the University of Chicago, Mike Merrell, others who the President knew personally as advisors and security and a range of issues and it reflected his personal engagement and produced a number of significant reforms: Presidential Policy Directive 28 which instituted reforms in intelligence and contained the declaration that the United States was going to give to citizens everywhere the same or equivalent privacy protections and dignity to what U.S. citizens get. A significant new international norm when it comes to government surveillance. We've seen diplomatic success on the internet governance front. Language on data transfers and rejecting data localization in the transpacific partnership. The adoption of a new privacy shield framework with Europe and progress on a number of international norms on state behaviors and cyber security on economic commercial espionage and on the notion that international law should apply to state behavior in cyber space.

The question I ask in the paper is how do we make sure that what the administration has learned endures as the people who learned lessons move on. So there were several specific points. The first one is sort of a conceptual point that national security policy making needs to reflect the importance of economic issues in general and the digital economy in particular. We pay lip service to the notion that the economy is

important to our national security. We need to incorporate that into our policy making. The digital economy is a huge component of that. Accenture puts the digital economy this year at contributing 33 percent to US GDP almost $6 trillion, and that's only going to grow as these areas continue to expand. It presents a number of opportunities and a number of challenges for our economy in the future. And that has implications for how we go about making policy.

And the first is that the President and other top leaders need to champion an interconnected world. Some of the success over the past three years has been because of President Obama's engagement, because of Secretary Pritzker, Secretary Kerry have been involved and been out speaking on these issues. That needs to continue. We need to build up the principle of the presidency and anybody who has been involved in communications and government and campaigns knows there is no substitute for the principal to deliver the message.

There are also some structural things. The way that we organize. The executive branch around digital issues needs to reflect the scope and the significance of these issues. That bears on how the White House operates decision making there and it needs to reflect the breath of the issues involved. The center of energy and decision making in the White House apart from in terms of the policy councils, really it is the National Security Council because it is so well established, there is so much that funnels into it. The National Security Act says basically the National Security Council gets made up of the national security advisor, the secretary of the defense and the secretary of state. Anybody else is optional and up to the president. And currently secretary of treasury, trade representative, secretary of commerce, the deputy of national security advisor for international affairs, a new creation of the Obama administration, are there if international economic issues are on the agenda. That needs to broaden, there needs to

be a presumption that all of those economic agencies are at that the table.

We need to strengthen the other councils on the economic side, the National Economic Council, the Domestic Policy Council, the National Science and Technology Council so that they have by executive order like the National Security Council does the imprimatur of the president any structure of an inner agency structure underneath that to work with. And we need all of the agencies involved. I'll hold out the Commerce Department as an example because it is the one I know best but also because Secretary Pritzker has fully embraced the digital economy as central to the Commerce Department Role and appointed Allan Davidson as senior advisor on the digital economy and has strengthened the class agencies bonds and focused on that issue. The State Department has done the same thing with its cyber coordinator. More agencies need to be looking at these issues that way.

The other recommendation is also structural. We need to open the architecture of decision making effecting the digital agenda and the ecology of the internet. One of the reasons that I think the Commerce Department has been effective is because it is out there engaged with the academic community and the business community and very invested in multi stakeholder processes. Those are the kinds of processes that we need for decision making in this area. Whether it is on norms of cyber warfare or commercial issues like global data privacy issues.

Finally, the simple point that personnel is policy. You can have the right structures, but you've got to have the right people making those decisions. And the paper includes as you may have seen a digital policy plum book those positions that are important to digital policy making.

So these are I think some simple lessons in some respects obvious, but the details matter. There is that maxim that operations is policy just like personnel is

policy. I think everybody in Washington by now has memorized "I want to be in the room where it happens" from Hamilton, and it makes a difference who is in the room. That's a function, and that's going to ultimately shape the outcomes. So that is a function of the structures that establish who is part of the decision making process that ultimately is in the situation room for the deputy's meetings and the principal's committee meetings. And of course who is sitting in those seats will make a difference as well.

So now to discuss these issues and kind of broaden this and look ahead for the next administration let me introduce our panelists. So why don't they come on up, and I'll make the introductions when you can see all their faces. So sitting to my right is Jane Lute. She's been engaged in these issues in a variety of ways. She was formally the deputy secretary of the Department of Homeland Security, and in that capacity was a key leader in the administrations' cyber security policies and has continued to be involved in that as president and now member of the board of the Center for Internet Security. She also was a career military officer and worked within the National Security Council in the Clinton administration in the 1990s and also the Bush '41. To my left is Dean Garfield who has been a leader on these issues on the outside as the President of the Information Technology Innovation Council. A key policy advocate, not only here in Washington but around the world. And finally to my left Nuala O'Connor who now heads the Center for Democracy and Technology and is a key player in advocacy in this area. One of the things I call out in the paper in terms of people is the number of staffers at the Commerce Department and at the White House who at one time or another in their careers were at CDT. Nuala also brings to this a perspective of a number of other positions having been a chief privacy officer within the government. She was the first chief privacy officer at the Commerce Department and later at DHS and also having worked in several positions in the private sector including GE as their chief privacy officer. She sees these issues from

a number of perspectives.

So let me begin by talking a little bit if we can about sort of the fundamental premise of the article that the economic issues have an important bearing as part of the national security discussion. In 2016 we need to heighten the importance of the digital economy in that. Dean, let me start with you and look a little bit about what we saw in the Snowden leaks and the impact of that and where you think we are today.

MR. GARFIELD: Thanks for the question, and thanks for doing this. I think the paper was well reasoned and well timed and also the categories you created are I think are the apt ones. The Snowden disclosures created huge and significant global problems for the tech sector. Where we are now is and when I say we I make a distinction between the U.S. government and the 60 plus companies that I had the privilege of working for and representing is a bit distinct. So with regard to the companies one of the things that we are still endeavoring to do and still challenged by is rebuilding trust on a global basis. We've made some headway there, but still when I travel around the world there is the suspicion about U.S. based companies, around data security, and whether data is secure when housed by those companies in spite of all of the evidence to the contrary and the reality that it is. And so that is an ongoing process that I think will be ongoing for a while. Not all of these concerns that we see are legitimate. Some of it is simply protectionist and using the Snowden disclosure as an excuse to bolster domestic players.

As far as the U.S. government I think we've learned a lot but I think, as evidenced by your article, there is still important work to be done including in all of the categories that you described. I think the National Security Council is first among equals, if you will, and there is significant work to do to ensure that the data point that you shared from Accenture on the role of the digital economy is truly engrained in their thinking as

well as their action.

MR. KERRY: So Jane, Nuala, Dean mentioned restoring trust. Both of you were involved in aspects of that. Talk a little bit about the role of trust and its relationship to cyber security and the relationship of that to sort of a broader array of issues. I'll ask you the same question with respect to privacy.

MS. LUTE: That's also Cam and thanks for this opportunity. I think the question of trust that you and Dean put your fingers on interweaves what I consider to be the three core questions related to cyber security and these core questions are essential for us if we are going to successfully move forward in this world and we have no choice. We have no choice about moving forward successfully in this world. There is no enterprise in the marketplace today that delivers value without relying on IT and access to the internet. And there is no enterprise that is secure in its endeavors. I mean whether it is public sector or private sector so we have to get this right.

And the three core questions that I ask when I talk about this are, how do we architect systems we can trust from components we can't? Question number two: How do we ensure the integrity of our identity and our information in an open internet? And question number three is, what will the role of government be? So all of these I think are implicated in trust. When we talk about trust what do we mean? There is that emotional component of trust which relates to likeability, but most of us can set that aside. Trust really emerges from this notion that you've got a value proposition that you reliably deliver. I know what you do, and you do it regularly in predictable ways that I can trust. But that is really, I mean there is so much more a dimension of trust now that the public across the board are asking themselves what else is going on? What else? Because while I do value the value proposition that you represent, and I do respect the fact that you can reliably deliver it, I really want to know at what price? What are we paying for

this, what else are you doing? I think it is fair to say for all of us who travel internationally that broadly the view is overwhelming that the United States militarized the internet and took it from its intended purpose (if anyone knew what that was) into a realm that really served the national security interests of not only this country but other governments are doing this as well. So the U.S. is not exclusive in this notion. But there really is a sense I think that trust can't be found because there will always be a higher purpose, a secret purpose that people are up to. I think it is really fundamental and now endemic. And we talk about restoring trust and establishing trust, and I think it first begins by acknowledging that governments have special needs, uses and activities online and that they pursue those needs, activities and interests in ways that are reconcilable with the rules and laws of not only their own society but of the international community.

There is a whole separate set of questions regarding whether or not you think we can manage life online both as a government or as a society. And people by principally taking a national security lens to the challenge - I'm not sure about that personally - but I think the issue of trust interweaves every dimension of what we're talking about.

MR. KERRY: Nuala.

MS. O'CONNOR: How beautiful. I just adore listening to Jane and thank you to Cam. I just want to call out Cam and Brookings for having such an incredibly rich and also diverse panel. And by that I mean including at least one Republican on any panel here at Brookings so thank you for that. It is a delight to be here and thank you also for the Plum Book, the digital Plum Book which I'm afraid I'm going to have to burn before I return to my office because we have given enough at the office to this administration and I'm sure we're going to see some big changes in the next couple of months. It is a wonderful paper and I wish I had had it when I started in the Bush

administration so many years ago because the only hand off was basically me calling Peter Swire and saying what do you think I should do once I get there. It has been a great, great road for privacy professionals, for security professionals, for folks who understand the technology industry working in government.

And Jane is absolutely right that the big question is whether or not people trust these institutions both in this country and elsewhere, whether they trust their private sector institutions. I see the compelling issue in the Snowden disclosures as one of the blurring of the lines of the data that we transact with private sector actors and the data that we give voluntarily or otherwise to government actors and the blurring of that wall or the breakdown of that wall between the private sector and the public sector unknowingly apparently in many cases and whether that is going to continue or whether there is going to be a hardening of the boundaries between the self and the state, the self and the company and the company and the state.

But I heard another really compelling question that I think is really informing certainly CDT's work in the coming months and years but a lot of industry and a lot of government relationships and that is will we be governed by ourselves or will be governed by the algorithm. And I think that is a compelling question for our relationships with companies and increasingly with our always on, always automated world. Whether it is in financial systems, whether it is in government systems, whether it is in security whether it is simply in our surfing habits online but as the internet moves from 1.0 to 2.0 of mobile to 3.0 of everything everywhere all the time in your home, in your car, everything will be automated and that is wonderful. This is great productivity, it is great advancement for human achievement for energy, the environment, education, healthcare. But the minute decisions that are made about you on a nanosecond basis can profoundly affect the knowledge you have, the power you have, the relationship you

have with the community at large, your family, the institution. I think Tim O'Reilly said it best recently when he asked the question whose black box will you trust. I love that question, I think that really has made me think about my relationships certainly with my former employer Amazon, with our U.S. government and with the global conversation around the internet.

MR. KERRY: Okay so Nuala you talked about this blurring the lines between public and private, you talked about the perception of militarization of the internet. Do those reflect a problem in how we've approached these issues, and what do we do about it?

MS. LUTE: Certainly from a point of view of cyber security, we are not where we need to be. And why not? I mean we all know that it is, I think we all now can say, we couldn't even a few years ago say that we all know but I think we can say that now that we all know that we need greater security and a greater attentiveness to security with our lives online. We are dominated now in an environment where the risk is almost entirely assigned to you to resolve if you're an enterprise. Every enterprise is sent a message that you have to be your own pathologist. You have to know what threats are out there targeting you, you have to know what your vulnerability is to those threats, and you have to take steps in your priority determined order to address them, and that's nuts. That's nuts. We're all on the same internet. Ninety percent of what you're seeing, I'm seeing. Ninety percent of what every enterprise is seeing, every other enterprise is seeing. But we don't act as if we understand that. We do understand it in our everyday lives, we wash our hands right? Let's just say yes. We brush our teeth, we floss, why? Because these basic hygiene measures prevent 80 to 90 percent of the preventable diseases and the things that can cause great harm if we don't do them.

We're acting instead online as if we don't understand any of this, and

that for too long, in my view, we acted as if we were waiting for government to tell us what to do. And government was for its part, and I was a part and Cam you were as well -- we were wrestling with this notion that major cyber problems were a matter for the national security community. You make this point in your paper. For too long we treated them as a matter for the intelligence community and the national security establishment instead of a matter of public safety and security where everyone gets engaged. So yeah, I think though now we have made that pivot we are engaging everyone, there is clear recognition that the private sector has a lot of not only stake in the game but role to play in its own security. And we're now sort of mapping and figuring out both the Obama administration through a series of executive orders, legislation however haltingly progressed on the Hill. I think nobody can say they're satisfied with as far as we have come given our reliance online, but we have made that shift finally.

MR. KERRY: Dean, do you agree with that?

MR. GARFIELD: I completely do, and I think one of the points that you made is, can you have secure systems even where you have vulnerable components? And critical to doing that is making the pivot that you were talking about where there is a recognition that it is multi-faceted, multi-layered, and multi-national, and I think we are making that pivot. There is certainly a lot more that we can do including addressing the issue that you raised, Jane, about the global concept and belief that we've militarized the internet. I think there is a sense, unfortunately, that is inconsistent with what you said, which is everyone has or the perception is everyone has. When I travel internationally, what I experience is the sense that maybe everyone is doing it but the U.S. has perfected it, which compromises U.S. based companies in a particularly pernicious way. So I think an important part of our work is countering that because the trust is really both security and privacy in combination so I think we have to work on both fronts in parallel.

MS. O'CONNOR: And I think this dichotomy that people have stated over and over again that it is privacy versus security is just so overplayed at this point. It is so hackneyed it is almost not worth addressing. But please strike the word balancing from your vocabulary in this conversation because I've always said certainly when I was at Homeland Security, and I loved your color coded slide because I realized I was working in the red zone and I was a blue player and take from that whatever you want. But addressing the issues of human rights and civil liberties in a lense that is entirely post-9/11 United States is certainly a very hard conversation but one that has to happen. I think the challenge for all of us is to realize that good individual privacy is bolstered by excellent security and excellent security is comingled. I've always said they are two sides of the same coin; they are not antithetical but they are absolutely values that can live in partnership, but they have to be done intelligently. The challenge I think for all of us working in the internet space, and I'm so privileged to have a team of technologists and computer scientists at CDT who are preaching data hygiene and systems hygiene on a daily basis, that we are not doing even the simplest things frankly to keep ourselves safe and we need to start there. But the challenge really historically is the internet is not architected for security originally. It was architected to share academic papers and to share research and to share information. So we really are bolting on frankly systems and data security in a way that we have to think very hard about what was this system designed to do, and what is it actually doing, and what are the values we're trying to promote? Because the code is law as we all know. So how are we programming not only the personnel and the policy, which you're absolutely right Cam, are essential to the government operations and understanding of technology. But is the systems architecture actually doing what we think it needs to do? And 25 years on from the dawn of the commercial internet and the first website and the first official sharing of information by

Tim Berners-Lee and others is this both the community that we thought we were going to have and is the architecture supporting the rights that we think we deserve.

MR. GARFIELD: I was saying to Cam before we started that in general governments and not just the U.S. government, our instinct is in spite of having the people and perhaps even the paradigm for addressing these issues is to nibble at the edges. So it may be that in order to integrate all of what we're talking about here into our government, we have to be a bit more radical in rethinking the structures and the systems and the institutions that we have in place to advance these issues. So the idea that these are not balanced equities is completely but actually can be advanced and parallel. It is completely inconsistent with how we've organized our thinking and the government around these issues.

MS. LUTE: I really agree with that. One of the quibbles I had with a really excellent paper and a true reflection and if anything, it really understates the role that Cam played during his time in the administration certainly when we overlapped and continually raising and driving these issues. It may be hard to imagine now, but in 2009 there was still a great deal of sense that we were looking at issues of first impression with respect to our reliance on IT, the role of the internet, what governments role would be. The quibble I have with the paper -- it's not a quibble actually, it was actually a knife fight for me for four years -- was the role of defense and the role of the other departments and the role of the civilian voice versus the military voice. I mean again, I think we've reached an equilibrium that is sustainable going forward. But when you think about the problem at a large level we were treating it, and I think we do need to continue to treat a lot of these things as a matter for national security. The national security is strategic, it is centralized, and it is top driven. And I can't think of three words in the English language any less descriptive of the internet than strategic, centralized, and top-driven. We really need a

model that is much more close to homeland security, if you like, but the public safety model which is transactional, decentralized, bottom-driven where people are not only engaged with a sense of responsibility for their own transactions but also whether they're driving those transactions, whether they are a pedestrian or whether they're a passenger. We've all played these roles with great ease and facility in our physical lives and we need to move to this comprehension online.

MR. GARFIELD: So where does that leave you with the next administration and how to think about this?

MS. LUTE: So I think it is not, I mean 20 years ago 16 million people online. Eighty percent of the people online were English-speaking North Americans. Today 3 billion people are online, 50 billion devices, 100 billion devices, it is extraordinary. There is no enterprise that delivers value in our economy without relying on IT and access to the internet. Government must play a role. I think as Cam eludes in the paper we need to endogenize our – that's the wrong word. We really need to take on board the fact that security at a national security level is not the only dimension of the problem that we're solving when we address these issues. So cyber has to be first and foremost. There are players across the inner agency. I couldn't agree more that personnel is policy to a large extent. There will be, the next administration will have to place a regulatory priority here on cyber, a policy priority but also an operating priority here, all three.

MR. GARFIELD: This is a real world example. The debate around encryption. Our experience in that debate speaks to part of the challenge. So you had the FBI leading the public dialogue in many respects. DHS playing some role but an unclear one. The desire of the administration and the president to find a solution and the tech community largely reacting from the outside with the exception of when someone

from the administration would parachute in to Silicon Valley, pull a bunch of CEO's together and then leave. And so with us trying to figure out and pick potential allies in the administration who we thought could be an advocate at the table with uncertainty as to whether they were actually at the table.

MS. O'CONNOR: You mean the administration didn't speak with a unified voice on encryption, Dean? Is that what you're saying? Shocking.

MR. GARFIELD: Well it is less the lack of unity and more a practical example of the multilayered nature of these issues and the lack of a current construct for dealing with it in an intelligent way. So how do we avoid that again in the next administration and accelerate getting to a point where we are set up. We do have the categories to develop…

MR. KERRY: Yes and you're segwaying very neatly to a topic I wanted explore a little further, but before I do that I'm going to add one more lesson to my recommendations: Don't get in a knife fight with Jane Lute. Everything that I would say about opening up the architecture I think applies to things that happen on the defense, the cyber warfare side, how those things get don't get be done without the way multi stakeholder process that involves the companies that have a stake in that and everybody else. So I think what goes to the recommendations, I mean let me ask each of you what do you think in particularly in the pivot that we've talked about -- what do you think has worked well, and what would you change?

MS. LUTE: So I think Dean's question set your subsequent question up really well. Many people think this was a false fight, that it was always available to the FBI to hire someone to crack into this. And so and the issue rapidly became not only a politicized one but sort of a patriotism test. Why wouldn't any company support law enforcement particularly in an environment to where we're trying to combat domestic

terrorism? I mean it is a very, very legitimate question frankly that industry must answer, and they're not answering it, in my view, at all in the kind of way that the public can do anything with. I mean and the question is why should we deliberately hamper law enforcement's legitimate efforts to keep us safe under the rules and help us solve that problem.

So Dean is exposing, I think, one of the key truths that we have all learned, and Cam talks about this in the paper and in the recommendations: we need multi stakeholder engagement. This doesn't really mean co-management, but it does mean really multiple inputs in problem solving. Not in a unity of command way but in a unity of effort way. So I think that is important.

I think the reality also we have to confront and industry is trying to keep itself at arm's length from this is that information legitimately comes under pressure from three sources. It comes under security pressure or intelligence pressure to conserve it so that we can learn more. We got a piece of information, that is really interesting and important; let's conserve it, keep it hidden, keep it secret so that we can learn more. By the way, secrecy does not scale, if we've learned nothing over the past six years. Secrecy does not scale, but security must scale. Security must scale, and they're not the same thing.

The second source of tension on information is operational tension, and that tension is to use information, to do something about it, to keep people safe, to interdict a threat before it occurs.

The third kind of tension comes from the law enforcement community which is to preserve information so that you can successfully prosecute a case in the court of law. These are very legitimate tensions, and if industry wants government to do its part, industry must do its part and get in the game responsibly. So the basic point I

would say is the right one, we must build a bigger table for these issues. The national security community is not used to have a very large table. The homeland security community, the law enforcement community, the public safety community is used to having a much larger table -- more so, much larger -- but industry has got to reflect on its responsibilities here too.

MS. O'CONNOR: I don't disagree with the idea of corporate social responsibility in the digital age, but I don't agree with the question that is what else should industry do or why aren't they helping more which is roughly, not exactly what you said but that is somewhat the question. I think the question is really, why is the government assuming that a company should infuse a product defect into an existing product? There have always been locksmiths. Has the government employed locksmiths to break into everybody's apartment, or if there might be a crime they can get in before it happens? I think it is a question of boundaries. Boundaries of the relationship between an individual and a company and the employment of technologies that are legitimately available to an individual.

And the encryption debate I think, everything that Jane said is exactly right that it has become highly politicized. It became a political test. It became a loyalty and citizenship test for companies, and that is exactly the wrong framing. But it is a much more, I think, complicated economic conversation that companies need to have. In the world of strange bedfellows, CDT partnered with the Chamber of Commerce on a number of recent amicus briefs in this endeavor, and I'm really taken with the arguments that we are asking companies to defeat their own security, which is a legitimate point of sale, an element of the product that is being offered. But as my technologists tell me, listen, encryption -- it's like sidewalks. These are basic elements of living in the digital age, and of course my friends at the FBI and the NSA and CIA certainly all employ encryption in

their own. In fact, we had this debate about the campaigns and who is using better encryption, and the Clinton campaign is certainly using some of the best and highest quality encrypted devices and programs and systems.

So again, it goes back to the larger conversation of, where is the boundary between the long arm of the government and the private sector? I think that private sector has a lot to do and certainly is thinking about its role in national security not only in data and encryption and systems but also in speech and community and the conversation around global terrorism. But I am very, very skeptical and someone said to me recently, well these are not sins where you can criticize others because you've done them yourself. But if they fly out to Silicon Valley to impress upon companies that they need to do more, I am highly, highly skeptical about that request by the federal government.

I think the better question is how can the federal government better organize itself and what tools does it need as you point out Jane, it has always been the efforts of the CIA and NSA to break encryption on their own terms and in their own way. But to ask companies to do their work for them I think is a highly questionable action--

MR. KERRY: So what are the changes? How do you build what you see is the right boundaries in public and private sector into the way the government operates?

MS. O'CONNOR: Well first, as you point out, personnel and operations. I mean the lack of a coherent voice on encryption alone, the lack of a coherent, kind of, convening strategy around data, around privacy, around citizen versus government and the digital relationship and the digital self is something that we've made great progress. Certainly, over the last seven or eight years we made progress in the previous two administrations. Really the story goes back to Peter Swire as the first person, the first

federal government official with privacy in his title in the first Clinton administration. So this is a multigenerational walk. The government is still behind, though. I think we all agree that they are not employing the best and highest technologies and norms that the private sector is. I would trust my data frankly to some of --I won't name and names, some of them are former employers -- to the private sector security of multinationals based in this country probably better than I would many of our federal government agencies, which as we've all seen have suffered massive security breaches in the last several years partly because they've been under resourced, under staffed, underfunded.

The OPM breach affected I'm sure many people in the room. It sure affected me and all of the family members around the world who were on my various forms that I submitted to become a federal official. So certainly funding and staffing and knowledge and internal operation -- certainly it's a great thing that many agencies have chief privacy officers: Becky Richards, my former staffer at DHS now at NSA doing amazing, amazing work. FBI in particular certainly understaffed and under resourced in cyber warfare, and I think the interesting conversation we can all have is work that we're doing and others are doing and thinking about active defense and hacking back and what the responsibilities and the roles and the ethics of private sector actors and governments are. It is perhaps too decronian to call these war and use these war metaphors, but these are very serious threats to national security that are threatening individual data and companies as well.

MR. GARFIELD: So if I may: I think you are absolutely right, and where we all agree seems to be around the role of the presidential leadership, the importance of policy, the importance of people and personnel. I think where there may be some disagreement, and we're all struggling with -- and I think it is important to acknowledge where the complexity of the issue and the need for expansive thinking and getting to an

answer -- is what the right paradigm is and whether right now part of the paradigm is the image; the blue and red image that you put up, where in many respects these agencies are competing with each other. And we in the private sector see that competition and try to leverage it for purposes of advancing policy.

So how do we shift to a paradigm where the complexity is appreciated and if there is a competition, it is a healthy competition. And part of what I think you suggested was, who rules at the National Security Council? And maybe that's a part of it, is the permanence of the people who are sitting at that table -- the Hamilton quote. My instinct tells me that that is a part of the answer but perhaps not the complete answer, and something more radical is necessary, but I'm still struggling with what that is, Cam.

MS. LUTE: I think this is one of the key questions. In order to answer, Cam, how should government organize to play its role, and how should we meet out the assignments and responsibilities? We first need an answer to the question, what should the role of government be when it comes to cyber security and when it comes to helping this community of societies and this American society manage its way forward? I mean the Federal Bureau of Investigation is an investigative agency. It is a federal investigative agency. It is not the federal police force; it is the federal investigative agency for crimes committed at that level. I mean it is an important storied and valuable history and role in our society. The National Security Agency we now know a lot more about it than we ever did. Its fundamental job is -- well aside from its fundamental job, one of the things that it has to do is protect .mil. How big is .mil? Let's say .mil is the size of this remote. How big is .gov compared to .mil? Let's say it is the size of this stage in three dimensions and how big is .com compared to .gov? How big is IPV6 compared to .com? So let's understand, what is Homeland Security? Homeland Security is again a relatively new agency. It is 12 years old. It is not one-year-old for the twelfth time, there is a difference.

This organization has evolved. Its role is very, very different than any of the other federal agencies in the national security space. For one thing, it interacts with the public. It interacts with the public, five to seven million people a day. How many people does the intelligence community interact with? None, by design, right? I mean sure at the margins, but it is not five to seven million people a day.

MR. KERRY: It depends what you mean by interact.

MS. LUTE: I'm talking about lawfully. So is there a role -- So in the homeland security space Washington is not the national command authority; it is the federal partner. Believe me, in Florida they understand the role of the federal partner right now as hurricane Matthew is bearing down. They understand what to expect from the federal government in discharging its federal responsibilities in terms of authorities, financing, mobilizing resources, et cetera. So we need to bring this model into this space.

I mean, TSA, all of you know and what all of you may not know is that the airlines and the airport owners and the states and the municipalities all have a role to play in TSA, in transportation security for you when you go through an airport. And they are used to doing business every day with the private sector airlines, with the private sector airport owners with the states and the municipalities, similarly the Coast Guard. The Coast Guard punches way, way, way above its weight. It is the only military agency that regulates its operating environment. It actually is a regulator. There are less than 50,000 Coast Guards men and women, but they operate with that regulatory power and authority. They operate with partnerships. Captains of the port are almost always civilian either private again or municipalities. These are models for engaging in problem solving for what we deal with every day. How many people are affected by the Coast Guard? I don't know, 90 percent of the population of this country lives within one hour of a major

body of water, everybody.

MR. KERRY: So Dean, your (inaudible) having somewhat more coherent decision making. You may want to be careful what you ask for. Apply that for example to the encryption today. And that could have produced a different outcome or a worse outcome from your standpoint if the resolution was to say, all right we need to take some steps to build in access to encrypted technologies. I went through a version of this in 2010 on the first version of going dark when Bob Muller, the then FBI director, was ringing alarm bells and saying we need to address these new technologies and increase our access. Hands up in various ways, and I think I could have gotten rolled at that time had the issue been forced and not gone into a more prolonged discussion, ultimately came to a standoff.

MR. GARFIELD: But we can all leverage chaos for theory for our benefit. But I think the principle that you start with is that there is -- and the point that Jane was making that HS is 12 years old not 12 one-year olds, successive years of being one year old -- is that we can learn from the evolution of society and humanity. So we can talk about this in varied macro ways, but how human beings are interacting with each other and the tools with which we interact are being transformed in ways that we couldn't even imagine two years ago. And so rather than pretend that we have all the answers, I think it is important that we begin to create platforms, institutions and get the right people in the room to wrestle with these issues so that we can move forward in an informed way.

MS. LUTE: I think this is really right, and the clearest example -- and Cam with all due respect and a great deal of affection and admiration -- I'd have to say the Vossenhauer episode that we are recently undergoing, still undergoing where the State Department and Commerce took the lead, negotiated terms. Rossenhauer for those of you who don't know is the arrangement that governs export controls, and there

was a concern that we've got software that we want to control because if it got into the wrong hands, that would be a problem. So without engaging other parts of the system a proposal was made, rules were put out for public comment, and a torrent was unleashed because it did not take account of the other equities at the table.

MR. GARFIELD: And the complexity, I mean it is not a simple issue because managing weapons of mass destruction is critically important. Is that structure and that paradigm the right way to think about cyber security and cyber testing tools? And so I'm not suggesting --

MS. LUTE: The answer is in my view fundamentally, no.

MR. GARFIELD: No. That's correct.

MS. LUTE: If we've learned nothing, we will not manage this world as if it were an intelligence program, as if it were a battlefield, or as if it were one extended criminal investigation. The good news is we have other tools.

MR. GARFIELD: I think part of the opportunity we have, though, with the fact that we now have -- your first point on the president -- principles who are technically savvy, some even sophisticated on these issues, is we have the opportunity to lead and partnership with others in trying to figure this out. I think all too often we're reluctant to say we need to figure it out, but we need to figure it out together. It seems and I think that is part of eroding trust internationally as well, where the U.S. pretends that it has all the answers and moves in a silo. And I say that not to blame the U.S. I think it is important to lead. We see Europe doing it more and more in the area of privacy, and I think they're moving in a faulty fashion too because they're just moving ahead in a way that doesn't reflect today's reality.

MS. O'CONNOR: Well I was going to throw lots of criticisms of what we've accomplished in the last seven years, but one of the really courageous acts was

the ICANN transfer of the IANA functions, and Larry Strickling took on a lot of heat in the global dialogue personally and on behalf of the administration. Despite concerns on very serious political concerns here in Washington and elsewhere, I think showed some humility, showed that we recognize as a country there is a need for a multi stakeholder approach to this, that we don't have all the answers anymore. I think you're absolutely right. The conversation globally around tech and around data and around privacy has been fraught with misunderstanding, and despite Cam's heroic efforts really courageous efforts in this, we certainly as a country are back on our heels post Snowden. It really set us back in the global dialogue.

MR. GARFIELD: Jane made a point earlier, and your articulation was perfect, but I don't remember exactly. And it is an important point about leadership, and the fact that someone is leading doesn't mean -- the fact that it is open doesn't mean you don't have a single or simple point of leadership. I wonder about the IANA transfer and if the success of that is in part because there was a clear line of who was in charge in driving that and an opportunity for multiple agencies and the Congress to weigh in but it was being funneled in a particular way and I wonder if there is -- I guess it is the point you were making Jane. There are models whether it is the Coast Guards or otherwise that may inform our thinking here, and so we need to look at those models and see how they inform our ability to structure things in a more efficient way or effective way.

MR. KERRY: Well I have some additional questions I want to come back to, to look ahead. Why don't we go out to the audience here and see if we have some questions? Why don't we start at the way back there on the left and try to come forward? There is someone here with a microphone, so if you could just wait. Please stand up and identify yourself when you ask your question.

MR. SELLARS: Thank you. I'm Jordan Sellars with FJS Helter Skelter

Politics and Social Sciences, a think tank. My question is, what are Democrats and Republicans political agenda for informational technology in the 21st century in terms of private-public relationships and government affairs?

MR. KERRY: Okay who wants to start?

MS. LUTE: So I'll tell you a joke. What is the difference between Republicans and Democrats? Republicans say okay we're all a club, and the club is open to everyone, and here are the rules. If you want to join the club you have to obey the rules, but it is open to absolutely everybody. And we welcome you. And the Democrats say okay, we're all a club. What should the rules be? So I would say the following. It was a joke.

MR. GARFIELD: It was a thoughtful joke. We had to think about it.

MS. LUTE: I'm also going to answer your question by maybe confounding it a little bit. Where is the public today, not only in this country but globally? There have been very powerful social norms that the public now has really internalized. There is a norm of inclusivity: nothing about me without me. There is a norm of transparency: what is going on, does it affect me? Well I think it affects me so I want to know what is going on. There is a norm of reciprocity: do I have to do this? Does everybody have to do the same thing? And a norm of accountability for what is happening and what has failed to happen. Where are our politics? We look at the norm of inclusivity that society really has very powerfully internalized and its politics of exclusion that seem to be dominating. We have this norm of transparency, yet we talk -- and Nuala's is among the clearest voices on this -- we all talk about our privacy. We have this norm of reciprocity right? Equal rules for all of us, it is a level playing field and our market still rewards first mover. We have a norm of accountability, yet we're moving inexorably towards globalization where -- which really confounds fixing responsibility. So

I think you're asking a question about partisanship. I'm setting that aside just because we have quite enough of it, thanks very much. You asked about what is the President's first task in the next administration? It is to lead the global recovery from the past six months because we're all effected by this. And so it is not to say that these issues are not politicized. They are, but they don't have to be partisanized. Is that a word?

MR. KERRY: It is interesting what you described in terms of norms sounds an awful lot like some of the rules of governance and digital space, leaving aside perhaps accountability which who is accountable when everybody is accountable which is a problem for the system. So let's go to the other side of the room, also in the back.

MR. BOHANING: Mark Bohaning currently with (inaudible). My question comes out of my own experience in government, being yet another graduate of the Commerce Department. Cam, I'm really struck by your first principle because it is something I've been thinking about. Actually Nuala and I have been having this discussion. I'm reminded that President William Jefferson Clinton's first act – one of his first acts was to set up the National Economic Council when he became president. Its first executive director was Bob Ruben. He was followed by Laura Tyson. I sense that we're still -- and even listening to this discussion -- we're still seeing the national security and actually a very narrow definition of national security, which is wrapped up in cyber, affecting the economic discussion. How do we get the cyber policy, the security policy reflecting what was happening pre-cold war where economics was an integral part of DOD? It funded our national highway system. It helped get our science and engineering grad schools going. So I sense that we've got to think through in a much more aggressive way. And I agree. I can't use the word balance with Nuala, but we've got to figure out how to have these parallel integrated fashion and I feel like the structures are broken down and that it is really that we're only at the beginning stages of thinking about

how we do this. So I commend you on your first principle. I think we have a lot of work to do to put some meat on those bones.

MR. KERRY: Well thank you. I think the paper addresses some of this. The resources, the energy, the institutional weight. All of those are on the National Security Council side. And yes President Clinton in 1993 created the NEC, created the Domestic Policy Council, issued executive orders for those and for the NSTC, the National Science and Technology Council. I bet you know some percentage in this room didn't know that that council existed. We need to elevate those executive orders that would give them the same status and the same access that would help to give them greater access to agency resources.

MR. GARFIELD: Is that possible? That's what I was asking you before we started.

MR. KERRY: Sure.

MR. GARFIELD: It's the first mover advantage that Jane spoke about. I don't know if no matter what we do, whether the National Economic Council is going to be able to compete with the NSC.

MR. KERRY: Well yeah I don't think you can completely rectify that balance. I think some of this has to be done within the NSC, so I think changing the presumption as to who is at the table -- institutionalizing the deputy national security advisor for international economics. I think it should have a broader role than just the sort of international economics trade multilateral G20's, G7's et cetera in a much broader strategic economic roll within the NEC, with more resources there as well. So these I think are things that would help to address that balance provided of course you've got a president and people around the president and cabinet officers et cetera who also get these issues.

MS. LUTE: I think one of the most important innovations is to restore the word "staff" to the end of NSC. This is NSC staff, this is not the National Security Council, this is staff. When I first joined the NSC staff under Brent Gocroft, Bob Gates was his deputy there were 53 professionals including Bob and Brent. There are now seven times that number. It is humongous. And that growth coincides, I mean it is not as though the world has been standing still. I mean that was the end of the Cold War, the post-Cold War period through 9/11. And today, I mean, massive shifts and growth in expectations of the presidency not just as an identity point of reference but as a performance point of reference. That enormous pressures exists on any administration to do things. So you can allocate things out. I mean, I spent four years in the provinces in the Department of Homeland Security. You certainly feel the effects of an activist White House. And Washington really, really understands policy departments and regulatory departments. Washington doesn't really understand operating departments. So we need to sort of sort through the difference.

MR. KERRY: Let's go to the middle over here.

MR. REDDER: Hi, thanks for this. Tim Redder from the German Marshall Fund. I want to thank you for highlighting this cyber internet divide. I'm still concerned that we don't actually know what we're talking about in Washington or more broadly. Cyberspace and internet are not the same thing. The GPS signal coming out from satellites is not connected to the internet, and it better not be because that is dangerous. Your smart phone uber business model this is -- but it's all considered cyberspace. Until we start talking about the difference between internet and cyberspace, I think we're going to be confused. And just as an example at the Washington Post the other day, Juan Zarate, and there was someone there from the Federal Elections Commission -- they highlighted the fact that our election voting machines are not

connected to the internet. They are inherently secure because of that, the decentralized non-connected nature. But the online voter registration is connected to the internet, and that makes it more dangerous. And Swift network is not part of the internet, and Jane I know you know that Sipper is not part of the internet, but it is still all cyberspace. So how do we talk about different networks, which networks they should and should not be connected to as a matter of policy? Because until we start talking about whether the internet of things is a fundamentally dangerous proposition we're not going to have a real debate in this town.

MS. O'CONNOR: I'm so glad you brought that up, and thank you so much for that question because I was just at another event this week and someone described them as the internet fabulous or the technology fabulous. The internet and new tech is going to solve every problem, and it is all going to be fine, and don't worry about it. Then there are the fearmongering on the other side, which is everything should not be online and this is terrible for individual freedom and there are all these risks. And the truth of course is somewhere in between. The internet, new technology, hardware, software, name your thing; these are tools that can be used for good or evil. The hammer can be used for good or evil, but we have overstated both the potential perhaps and also the risk.

You're right and Cam's paper brings it up as well. Language matters, and it reflects a perspective where you sit in the organization and the government wherever also reflects your perspective. And we do need to get a little harder and a little more precise on the difference between, what is the internet, what are we talking about? Even the debate about whether it is capital I or lower case i has been a roiling debate with the "inter-nutters" that I associate with. I think these are important questions, and the first step is obviously having real technologists. I was thinking about our last

conversation and the importance of the NEC and the importance of elevating. I do think internet security and cyber security are national security issues, and there needs to be expertise at the NSC, but the NEC also needs to play equally and pull equal weight and be a big voice. But we do need to ratchet down our rhetoric on both sides of the conversation and talk about what is really realistic to have happen.

I'm so glad also you just touched on internet voting because we have one of the preeminent experts in the country on internet voting or on technology and voting on our team, and we are delighted given what we've learned from him that our voting machines are not connected to the internet and shouldn't be any time soon until we really get some hard work around this. The other internet fabulous or technology fabulous thing I've been talking about this week is Blockchain and Bitcoin, also great, great, potential in financial services and elsewhere. Not something we necessarily want our voting technology to be organized around, and we need to get really hard yet about the questions about what is anonymous, what is identifiable and especially in the voting space and citizenship spaces.

MR. KERRY: I agree with the question. The title I refer to – "Digital Policy Making" -- to try to move it away from internet or cyber. And I recall the drafts of the Consumer Privacy Bill of Rights talked about the internet economy and changing that to the digital economy precisely so that we try to look at this more broadly, and it is not just about the internet. Let me go to the right and I'll come back to you.

MALE SPEAKER: Thank you this is very interesting. I actually wrote my thesis for Jay Shue about this topic. So I find interesting researching is that everything was changing. So I was working on this thesis for several months and then at some point have to update everything because the whole scene had changed. With that in mind --

MS. LUTE: Find the period and hit the period.

MALE SPEAKER: With that in mind, we talked about having government and business at a table, can you really reach consensus when everything is changing so fast? Five years ago phones weren't a vector for attack; in five years' cars will probably be hacked regularly. Is there a way to really get enough principles in place when that is the situation? Thank you.

MS. LUTE: Yeah I think that is a great question, and the answer is, I mean, I come from the philosophy that you don't have to sacrifice decisiveness for inclusivity. I mean we can build as big a table as you want, and what organizes people is purpose and pride it turns out. People will come together for purpose. I mean that is really one of the founding insights of our forefathers here that people will come together from highly, highly diverse backgrounds for purpose. And when you articulate the principles, what principles are we trying to preserve here? What principles are we going to use to guide our work and what do you have to do in that kind of environment? You have to organize, right? And prioritize, right? And then unify. These words sound abstract but not in a setting like that, where you can bring together members of the business community and government officials together for a common purpose. What you find very interestingly is not unlike, I mean, in my other life I spent all my work in international conflict and conflict resolution and conflict prevention. Why are some fights prolonged? Why are they generations long? Is it because side A and side B don't understand each other? No, they understand each other perfectly well; they don't like each other, and they're willing to kill each other over it. And what you discover is persisting conflict exists not because of the differences between sides but because of the differences within sides. So the government is not monolithic on this question. Even the national security is not monolithic. The business community is not monolithic here but with the ingredients of a good meeting. A strong chair, the right people and a good text --

a lot can be achieved.

MR. GARFIELD: If I may add one other thing: I think your language and focus on principles is important. I think one of the things we need to begin thinking about is agile policy. So rather than always thinking about nailing down statute with precision of language, all contours well-defined, is thinking about the fundamental principles that we want to advance, recognizing that the world is incredibly dynamic and things are going to change and you need to have some flexibility.

MS. O'CONNOR: I just wanted to chime in because it is such a great question. It really highlights the issue, the age-old issue we all have in tech which is, when the world is changing so fast, how do we put a stake in the sand and say this is it? And I think we have some shared principles; they are in the U.S. Constitution. We really do know what the right answers are here, and again it is back to the tech fabulous idea that we suddenly invented these issues. There is really not that much new here. There is new technology…

MR. GARFIELD: I disagree.

MS. O'CONNOR: Okay, there's lots of great new technology, but I do think perhaps scale and speed. But other than that, we know what we feel about our relationship to our government. We know what we feel about our relationships with each other. These are new hypotheticals that we need to discuss, but I'm absolutely the ultimate optimist that not only industry and government that academia and civil society do come together. They come together at CDT's table every single day. They come together in great spaces like this and elsewhere. And that with the discord you see on each side, there also come different voices. What I worry about is the voices that are not at the table. Who is not getting a seat at the table? I'm wracking my brain to come up with another Hamilton reference because you threw that down at the beginning and we've all

failed you on that Cam.

MR. GARFIELD: I was in Germany last week with folks from the German Marshall Fund and speaking to the dynamic of a current situation. We're dealing with issues around ethics and machine and machine-to-machine communication, neuro learning, distributive ledgers which is very different then cryptocurrency. The issues that are raised are different and new for us. And so how do we begin to organize ourselves so that we can take advantage of the principles that Jane mentioned to begin to solve for them. There are models out there, but there are also new questions that we have to confront as a society. I don't think that we need to run away from that; I think we need to confront it.

MS. LUTE: But this is why Cam's point is so essential. That there be other voices and issues present at the table because we don't want to make the Christopher Columbus mistake: failing to distinguish what is new from what is new to you. It might not be new to everybody who has ever had to deal with the issue. There are tactical ways to address timus fugiting (phonetic) and also to address trust. One is to build into your process a redress mechanism that is available to everybody. Here we're going to make this set of decisions, here is a redress mechanism if the decisions we're making have unintended consequences which are confounding our core purpose. The other thing to build in is periodic review. We're going to look at everything in six months. We're going to look at this whole thing in a year. So we can't allow that and you don't have that luxury in a policy environment to just sort of say this is too hard, things are moving too fast. I had this extraordinary conversation with a number of colleagues regarding the cybersecurity profession. They said, well we need to wait for this field to settle before we make a move in professionalism. Thank God the doctors didn't say that. Okay they were prying open our craniums with stone tools, but I mean at least they were

engaging and learning. For cyber security we're going to wait for everything to calm down. No.

MR. KERRY: So we have time for one more short question but we're going to go to the wait, wait don't tell me ending here and ask each of you while that question is on the table. It is January 21, 2017; you have been appointed by the new president as the Digital Policy Czar. What is going to make in your recommendations to the president this is what we have to do right away. Over here on the aisle.

MR. SPARAPONY: Hi Tim Sparapony: concerned citizen. Quick question. My experience really does mirror Jane's in that when I talk to people internationally especially leaders abroad they really do feel that the U.S. has militarized the internet. I think that was your phrase. Here is my question: When we stand up a U.S. individualized cyber command as a new branch of the military, which is seemingly likely for the next administration and maybe before the end of this administration -- that announcement will come -- that is going to confirm people's suspicions around the world that we've done exactly that. And I wonder to Nuala and to Dean who deal with businesses who have to operate abroad how that is going to effect, maybe deepen the suspicions that people have internationally as businesses work to capture market share and provide goods and services around the world and what you think of that.

MR. GARFIELD: I think you're right, Tim, that it will. I do think that there are things that we can do including all of the things that Jane mentioned to begin to address that. So as it turns out just personally, I think to the extent that we can explain in common language why that is good policy and not intended to undermine the integrity of our global cyber systems that we can make a lot of headway. So these challenges, whether it is that or others, I think will continually come up, and as businesses I think were becoming increasingly prepared and able to speak them through and talk through

them. I think one thing that is important is the point that Cam made at the very beginning of his presentation about the early language that President Obama used during the Snowden disclosures. I think our government and the next government can learn from that and be thoughtful and how they articulate and explain shifts in policy or structure like that.

MS. O'CONNOR: Well I think we certainly haven't done ourselves any favors, right, in our global dialogue on privacy not just post Snowden but even before in seeming to not want to play in the sandbox that others created, which is understandable. I think to Jane's point, increasingly collaborative structure, so to the extent that we recognize cyber security as a national security threat, it is also a global security threat so partnering with others and not appearing to be acting unilaterally would certainly be one solution to the hypothetical you posed Tim. We've still got a long road. We've been having the same conversations around data and technology and privacy and security with the Europeans in particular for a long time that don't seem to have made a lot of progress in opening minds on either side of the Atlantic, frankly, and I would put the blame on both sides not just ours. But we need to keep pushing that forward and realize that the global internet is a global resource certainly not a U.S.- or an EU-only question. So the real question on my mind is, where does the dialogue go past U.S./EU in global norms? Global -- I love that story about the cyber security professional because I heard that in a conversation I had with a European official: you all need to just wait and slow down while we figure out this issue, and I said the internet waits for no man, no country and no region. I think is going to move fast to the previous question's point, and we definitely are scrambling to create structures in this country and elsewhere to accommodate.

MR. KERRY: Okay well we need to wrap it up. January 21, 2017 Digital Czar Jane Lute, what are you going to recommend?

MS. LUTE: It is not even a close call. If we're going to change the game in cyber security, we need widespread adoption of basic cyber hygiene. People need to know and be able to tell what is connected to their networks and systems, what is running on those networks and systems, who has access, administrative privileges to wander around the networks, and do they have a system in place to alert them automatically. Those four measures will prevent or help rapidly mitigate 80 to 90 percent of the problems we're seeing. We're not even making it hard. We've got to change the game in cyber security and basic hygiene is the way to do it. I would make that my first priority that the government puts it shoulder behind that message. It is very consistent with the NIST framework; it is a way to implement the NIST framework. It has been adopted by Etsy, by the Brits, by a number of other leading governments around the world as the core of their cyber security approach. The government needs to become a major megaphone and platform for innovation and tools and messaging on that subject.

MR. KERRY: Dean?

MR. GARFIELD: Two things. One, bring Jane back to be Chief Advisor. Two is to develop a G20 for the digital age that is a group of countries, global leaders focused on these issues that also include the business community in a real and meaningful way.

MR. KERRY: Thank you.

MS. O'CONNOR: There was a digital G8 a few years ago. Well I can say in addition to all that, that all sounds great. I may be shooting higher and lower at least domestically in that my president will make a clear announcement that – I was going to use the gender, and I'm going to just not – that the administration and the country stands firmly behind the idea of the strong end to end encryption but while recognizing also the important national security and law enforcement concerns on that issue and will

really move that conversation forward. But also dealing with the global norms around security and surveillance in 702 reform and our other concerns around just getting ECBA (phonetic) done. We couldn't even get that done in the last few years, and that seems like a simple fix to me. And we'll disengage from this blame game with the tech industry and the internet community and move forward the conversation around extremist content and community and dialogue online in a more constructive way.

MR. KERRY: I want to thank all of you for coming this morning. These are such wonderfully thoughtful panelists. I certainly appreciate their being here and the opportunity to have this conversation. Jane Lute, Dean Garfield and Nuala O'Connor, thank you very much.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

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