

THE BROOKINGS INSTITUTION  
FALK AUDITORIUM

INTERNET POLICYMAKING: NEW GUIDING PRINCIPLES

Washington, D.C.  
Monday, December 6, 2010

PARTICIPANTS:

**Welcome and Introductory Remarks**

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

ANEESH CHOPRA  
U.S. Chief Technology Officer  
Office of Science and Technology Policy  
The White House

HOWARD SCHMIDT  
Special Assistant to the President and Cybersecurity Coordinator  
National Security Staff, Executive Office of the  
President

VICTORIA ESPINEL  
U.S. Intellectual Property Enforcement Coordinator  
The White House

**Users as Regulators: The Role of Transparency and Crowd Sourcing as a Form of  
Oversight**

PHIL WEISER, Moderator  
Senior Advisor to the Director for Technology and Innovation  
National Economic Council, The White House

MARK COOPER  
Research Director  
Consumer Federation of America

CYNTHIA ESTLUND  
Catherine A. Rein Professor of Law  
New York University School of Law

KATHY BROWN  
Senior Vice President  
Public Policy Development and Corporate Responsibility  
Verizon

\* \* \* \* \*

## P R O C E E D I N G S

MR. WEST: Good morning. I'm Darrell West, vice president of Governance Studies and director of the Center for Technology Innovation here at Brookings. And I would like to welcome you to this forum on Internet policymaking in its third decade.

Since its inception in 1991, the Internet has come to play a very powerful role in commerce, communications and entertainment. It is a vital part of job creation, innovation and long-term economic development. There's virtually no part of any of our lives that are unaffected by this digital revolution.

In the early years, the government took a hands-off approach to the Internet. In 1997, for example, the Clinton Administration took the position that the private sector should lead and government should avoid any undue restrictions on electronic commerce.

When there was to be government involvement, the Clinton framework argued that it should be "predictable, minimalist, consistent and simple." Now, those are tough standards to meet. Today, though, people are very concerned about spam, privacy, cybersecurity, copyright and accessibility issues. What seemed to be a straight forward innovation several decades ago that would unite all of us in digital bliss has become much more complicated during that time period. There now are competing arguments over what role the government should play.

Last week, for example, the Federal Trade Commission proposed a "do-not-track" rule that would allow consumers to opt out of Internet search ads. And in the recent wake of the WikiLeaks document dump, there is renewed concern about security and confidentiality of government information.

To help us understand the issues related to Internet governance and

policymaking, we have organized a spectacular set of speakers for this morning. We're going to hear from top White House officials about their views on Internet policymaking. We will have a panel regarding the role of transparency and crowd sourcing as a form of oversight. We will discuss governance through multi stakeholder bodies. We will look at how the government can encourage Internet best practices. And we will hear from the American ambassador to the OECD about what is happening internationally.

For our first session, we are pleased to welcome several distinguished leaders from the White House. Aneesh Chopra is chief technology officer for the federal government. He serves as an assistant to the President and associate director for technology within the Office of Science and Technology Policy. In that position, he advises the President on technology innovation and ways to encourage new approaches.

In a *Daily Show* segment last year, Jon Stewart highlighted Aneesh's great sense of humor and actually called him the Indian George Clooney. And, Aneesh, there obviously could be no higher praise than that.

Victoria Espinel is U.S. intellectual property enforcement coordinator. In that position, she is charged with implementing the President's strategy on intellectual property. Previously, she was a professor at the George Mason University School of Law, where she taught courses on intellectual property and international trade law. While there, she also acted as an advisor to the staff of the Senate Judiciary and Finance Committees, as well as the House Judiciary and Ways and Means Committee.

Howard Schmidt is the White House cybersecurity coordinator. His task is to coordinate the many cybersecurity activities taking place around the government. He is a leading authority on computer security and has more than 40 years of experience in government business and law enforcement. He's the author of the *Black Book on Corporate Security*, it sounds like a very intriguing title there, and also the author of

*Patrolling Cyberspace: Lessons Learned From a Lifetime in Data Security.* And I should point out, I think that book came out before his current job, so clearly, after your current position, that book is going to be ready for a second edition.

Howard serves as a member of the National Security Staff and also works closely with the President's economic team on cybersecurity issues.

So we're going to hear from each of them, and then we'll give you time to ask questions. Let me start with Aneesh. You advise the President on many technology issues. What is the role of government and what should be the guiding principles for the future Internet?

MR. CHOPRA: Well, thank you for the opportunity, Darrell. And let me begin by thanking all of you for your participation today. And I want to set the stage up front by saying we're excited about your convening of a number of thought leaders that will help contribute to a conversation. And I want to set the stage, as well, Darrell, by suggesting that this is a conversation that we're very much actively engaged in. Just over perhaps a month or so ago, the dates keep missing me by, we announced the formation of an interagency White House led policy effort designed to extract that very question, surfacing opportunities for engagement within the federal government, and clearly in forums like this to engage with the private sector and the academic community.

So, broadly speaking, this is a conversation that we are actively engaged in and one where we're hopeful that your input will be much valued. My particular emphasis on this question began with the President's Strategy for American Innovation, which was released in September of 2009. And in that strategy, he made three broad points about the future of the American economy with particular emphasis on job creation. And he referenced this topic in the following ways.

First, he highlighted the fact that digital infrastructure is increasingly

critical to the nation's long term economic success. So before we get into the question about the role of the Internet from a policymaking standpoint, there's a base threshold question, which is, do we have sufficient capacity coverage access and so forth, and the President outlined very clearly that we view this infrastructure as a key building block of the economy.

The second element is exactly the topic that we're asking here, which is how do we foster open and competitive markets that promote productive entrepreneurship? We were very careful with our words in highlighting the importance of entrepreneurship, which is a key part of the success in the story of the Internet. And we will see, and you will hear wonderful opportunities today to engage on some specific conversations about how we're working to foster that.

And then third and related to that second, but certainly not least, the President said there are a few areas where we need to catalyze breakthroughs for achieving the kind of gains we want to see in areas that hadn't yet seen the kind of benefits. You outlined in the beginning, Darrell, the success of our commerce, our entertainment sectors and so forth, but what sectors have not yet seen the benefits? And two that were tantamount at the top of our list clearly were health care and the energy sector.

So why do I bring up those three components in the answer to your first question? Well, they're all very interwoven. I'll share with you an example about the ways in which this all comes together.

Almost a year ago today, Darrell, and then I'll wrap with this story and then we'll get back to the other questions, almost a year ago today, a physician testified at one of our public forums on the question about health care exchange and health care records, and he was a family physician in Northern Virginia who shared with us the story

of how one of his patients moved to Arizona and asked that a copy of her medical records be e-mailed to the doctor in Arizona. And coincidentally, the physicians both shared the exact same software platform, so the sense was, at a minimum, they should be able to facilitate this type of exchange, but he raised some eyebrows. You can't really use the public Internet for sharing medical records because of concerns of patient privacy and so forth.

In fact, he did say we got patient consent. We ultimately did because there was no button on the software that said e-mail it. We literally exported the file, attached it to the public Internet for e-mail, sent it over, imported it and it worked. Now, as this physician is testifying to this effect, the audience had like a collective (gasp) because the concern was the system, as wonderful as it is, is just not technically designed for that level of secure communication, at least in the context of our health care system.

So you raise the question, Darrell, what's the role? Well, in that case example, we took a very thoughtful approach in the sense that we have a long standing tradition of private sector led innovations on the Internet infrastructure. And so we did what we always do in this domain, we challenged the private sector to engage. We gave them 90 days for the development of technical specs. They produced those specs on time, 80 organizations under the banner The Direct Project.

We then got the group together to share a reference implementation, over 25,000 lines of codes written, and the first commercial product was announced almost a year ago to the day when Share Scripts announced that they would enable secure point-to-point health care messaging to trusted providers.

So, Darrell, in that case example, we, yes, relied on the private sector, but in the role of government as convener, engaged in a way that advanced or unlocked

some of the potential that we would see in our Internet infrastructure, and you will see that play time and time again in energy and so forth. So a very long answer to your simple question, how do we engage within the broad framework that's been in place, but to do so in a manner that encourages continued innovation in migration to open up opportunities in sectors that hadn't seen it.

MR. WEST: Thank you, Aneesh. Victoria, you coordinate intellectual property issues. How do you see intellectual property issues in relation to the Internet?

MS. ESPINEL: So first let me say thank you very much for inviting me to be here today. I'm very happy to be here with Aneesh and Howard, and hopefully the three of us can tell you a little bit about what we're working on at the White House.

My job is to make sure our intellectual property laws are functioning properly and that they're enforced. The Internet, as we all know, is an extraordinary platform. It has transformed traditional commerce, millions of businesses use it to reach their consumers, it has collapse barriers to entry, we have small businesses that are now on the grid, and we have billions of people that use the Internet just to say in touch with one another.

There are lots of ideas out there about how to enforce intellectual property on the Internet, and many of those ideas envision a top-down command to control model of authority. As I hope has been clear in the work my office has been engaging in over the last year that is not the approach that I think we have to have.

I think, in my area, there are three things the government needs to do. There are a few things we definitely do not need to be doing. We do not need to be picking winners and losers, and we do not need to do anything that messes up the Internet.

But there are three things that I think we do need to do. First, we need to

make sure we have good laws, and then we need to enforce those laws. Second, we need to make sure that we are engaging with the private sector. And third, we need to create voluntary solutions to this problem through productive conversations, and I'll just speak briefly to those three.

In terms of law enforcement, some of you may know the Department of Justice and the Department of Homeland Security cracked down on illegal websites last week. You should expect more of that. We are going after the pirates and counterfeiters. These are not legitimate businesses and they are a direct threat to our consumers and to the jobs that support our communities.

Second, in terms of engagement with the private sector, I have taken the open door policy one step further, as have Aneesh and Howard, and we have gone on the road to talk to people directly. So I have knocked on the doors of scientists, artists, engineers, entrepreneurs, I have talked to CEOs of Fortune 100 companies, I have talked to Internet success stories, some of them very, very big, some of them very, very small, in one case a two-person Internet success story company, and I've talked to manufacturers in middle America, so that I had a chance to hear firsthand what America's artists, scientists, entrepreneurs, big companies, small companies, what they need from their intellectual property system in order for them to continue to innovate and create.

The third thing, creating voluntary solutions through productive conversations, we should not need to mandate or regulate new rules for companies that interact or benefit from Internet commerce. We should not need to have new penalties for consumers. But we do need to find solutions.

So my office has taken what I think is an opposite and what I hope will be a more effective and efficient solution, which is to get a group of very smart, engaged people in the room and start talking to each other. We have been working over the last few months



with Internet service providers, with search engines, with advertisers, with domain name registrars and registries, with credit card companies and payment processors, for the whole host of companies that interact with the Internet to see if there's a way that we can come up with solutions that are balanced, that will effectively address what are repeated acts of infringement which need to stop, while protecting legitimate uses of the Internet, and protecting the policy principles that are so important to us, such as free speech and fair process.

So just to give you one example, over the last few months we've hosted a series of meetings with a number of companies, including Google, Go Daddy, American Express, Microsoft and others to see what we can do to reduce online pharmacies. And you should stay tuned in the weeks ahead for developments that we may be able to announce.

I think the conversations that Brookings is providing a platform today are extremely important. The panels on multi stakeholders processes, the panels on what the government can do to encourage adherence to best practices, these are exactly the kinds of conversations that we need to have, and I want to thank Brookings for providing a platform for those conversations. It is extremely important to President Obama that the United States be a leader for our citizens and to the government of other countries, as well. The United States must continue to lead by example in this area and in others. And I believe we are at our best when we are working together to come up with creative, productive, efficient solutions that will promote innovation, but also protect the foundation of the Internet that lets it fulfill its promise.

MR. WEST: Thank you very much. Howard, you are Mr. Cybersecurity. How should we think about the overall government role on the Internet in regard to cybersecurity?

MR. SCHMIDT: Well, first I would like to add my thanks to Victoria and Aneesh on you and Brookings for pulling this group together and the opportunity to speak here. The nice thing about being the third person to speak amongst the three of us, I just get to say what they said.

Seriously, though, when you look back to what we did in 1997, and that was sort of the precursor for PDD 63, Presidential Decision Directive Number 63, that laid down a number of things relative to the innovation strategy when it comes into security and critical infrastructure protection, and it's really important when we've seen and watched this evolution, the dependency we as a society had, what at one point seemed to be just something used by those of us in academia and research to just sort of bounce around and be able to collaborate and never thought for a moment that we would see it turn into what it turned into today.

But one of the things when you looked at the aftermath of PDD 63 and cybersecurity subsequent to then is we have to be very cautious to make sure that we really hold to those five tenets you mentioned from 1997 when it comes to the innovation and to technology itself.

We have a tendency to vilify the technology as opposed to those that misuse the technology. And Ernie Allen and I were talking just before we came in here, a million years ago, when I was going through the police academy, one of the instructors was talking about the use of technology in the law enforcement community, and cited an Arizona effort, I guess back around the turn of the century, where they were trying to make it illegal to have automobiles personally owned. And the concept was, if bad guys had them, and the law enforcement is all on horseback, they would win, instead of making sure the law enforcement had the technology and the ability to do their job. And I see a lot of correlation between that today. You don't vilify the technology; you vilify

those that are misusing it.

So with that, we've built some guiding principles that my office operates by. And once again, to reaffirm Darrell's comment, I'm dual-hatted, so I have the responsibility of the National Economic Council and the National Security Council. I think that's key to make sure you don't get lost in that vilification versus the innovation discussion.

But when you look at the four guiding principle we have, the first one is deterrence. And when people talk about deterrence, one of the first things they throw out is sort of the Cold War days, and, you know, mutual assured destruction, of course, we now call it mutual assured disruption. But basically the concept is, when you look at deterrences, you've got to make the cost of doing something to effect our innovation and technology and use of the Internet cost more than it's worth to them, whether it's a cyber criminal.

If they're selling a patient record, or if they're selling credit card information for 1-1/2 euros or for a couple dollars, you want to make sure it's costing them at least 5 to get that. And then notwithstanding the financial cost involved, if, indeed, which we're doing a better job, and Victoria has talked about some of the things in the IP world, but overall, we're doing a better job of actually holding people accountable, and that translates into catching them and prosecuting them.

And so when you start seeing people with sentences of 20 years in prison for doing some of the things against the benefits we get from the technology, that's pretty good deterrence, and we need to continue to work that way.

The other thing is resilience. And whether, you know, we spend the first hour of a sun spot cycle, and our BlackBerrys and our mobile devices don't work, generally I think the one hour is the threshold where it's like, hey, it's not work, no e-mail,

this is a nice day that I'm having. And about the second hour you get into what's going on, you get the phantom vibrations, and you wonder, you know, what's going on in the world, you feel so disconnected.

You wind up understanding we really need to have resilience built into this as well. And resilience, not only thinking for a moment that things were always going to work, but if they stop working, there's a gradual failover that we have the ability to recover from in the shortest period of time and with the minimum amount of impact.

The other guiding principle, and this is the one that overarchingly covers on both the things my distinguished colleagues have mentioned, and that's the issue around privacy. Without security, you have no privacy when it comes to data protection. We need to build that into it. But with that privacy protection, we also have to build the privacy enhancing technologies as well, because, once again, there are no absolutes when it comes to security.

So the issue becomes, if, indeed, something bad takes place relative to my data and someone gets a hold of it, they should not be able to do anything with it that benefits them, because I have to be able to control that as the end user. So when we look at the data points, and let's say for the sake of discussion me buying something online, the information that's necessary for me to do that should be minimized and also be there for the shortest duration to validate the transaction and move on. So when my new X-Box 360 with Kinect shows up at the door, I get the item, it's paid for, and that's all that we have to do out there. So when we look at the things we're doing relative to cybersecurity, we have to make sure that we're building privacy enhancing components into that, as well.

And the last one, once again to say what they said, is the partnerships. Private/public partnerships are so key. If you go back and look at the five key principles

from the Clinton Administration in 1997, all those point back to the partnership.

The partnerships, we're in the process of redefining partnerships, because partnerships in the early days were about sharing information on threats, and vulnerabilities, and what are the best practices, and that's changed, because the partnerships, we now have a greater dependency on them than ever before.

So it's no longer just sitting in a room and saying, gee, we're going to talk about issues we're running into, we're going to talk about identity theft, we're going to talk about exploitation of children, and come out of there with the concept of what I oftentimes refer to as the typical D.C. meeting. And the definition of a good meeting is, hey, we had a good meeting. But we need to move beyond and actually look beyond admiring the problem and get some solutions in place to solve some of these oftentimes challenging, but nonetheless solvable problems.

So out of these principles, we have four basic goals that we look at. I think the first one is something that all of us as citizens really would hope would happen sooner than later and that's protecting government networks.

I mean, we have a solemn responsibility. I don't know that there's any bigger repositories in a single location of data on citizens than with inside the U.S. Government. So it's incumbent upon us to make sure that we're doing all we can to protect bad data.

But as we always talk about, that data rides over a public network. And so the idea to protect that public network so we can still do what we need to do, free from interruption from cyber criminals or intelligence agencies or people that are doing theft of intellectual property, we need to make sure that the public networks are being taken care of as well, once again, keeping in mind that the government has got to recognize unique qualities of the Internet and look to do it in partnership with the private sector.

The third thing is building through the future. You know, my friends have this great R&D agenda over at OSTP. We're looking at workforce development, education. We're looking at sort of what have we learned over the past 20 some odd years and where we're going to be 20 years from now.

And that's another thing from the government we really have to focus on, and that's the issue, this is not a what's it going to look like in two years down the road. As we've seen with technology and networks, I remember some of the early networks I was involved in; we'd build it because it was cool. Then we'd say, oh, gee, we can build one over here, then we connected those two, and we constantly grew it without much thought about what it's going to look like 20 years, what the needs are going to be, what the resiliency requirements are going to be, so we have to build for the future from work force development to the innovation itself.

And the last one, and this is probably the most solemn of all these, and that's we have to make sure we strengthen as law enforcement, intelligence and diplomatic efforts. I've said many times that progress in the international realm is not standing in opposite ends of the room and yelling at each other. You know, we have to sit there and talk about people are very competitive against the United States, people are adversarial in some cases, but we all depend on that same level of technology. So as a consequence, it's incumbent upon us to sit down and have those diplomatic discussions.

But at the same token, we need to make sure that there are no safe harbors for the cyber criminals, whether they're stealing intellectual property, whether exploiting children, or whether they're just disrupting some of the things we're trying to communicate with from our desire to have free speech and open and secure communications over the Internet.

So when you look at sort of the principles and the goals together laying

on top of what we saw in 1997, I think we're clearly on a path where we're moving forward. And I have three of the four legs of the stool right here of Vivek Kundra, who is the CIO for the federal government, is sort of the fourth of this group that I just am tremendously privileged to work with. Thank you, Darrell.

MR. WEST: Thank you, Howard. And it's funny that you mentioned the controversy over cars when they first came in and whether people should be allowed to own them. I'm writing a book on technology innovation. One of the most intense battles took place in 1930, when, in the U.S. Senate, there was a motion to introduce dial telephones into the Senate as opposed to going through human operators. And the older senators were saying, wait a minute, I can't see the dial, or if you don't, you know, put the dial all the way around, you're going to get a wrong number, like they were absolutely and very intensely opposed to this.

Fortunately, the phone company came to the rescue and said, hey, we can do both the dial phone and the human operator. That resolved the conflict and allowed the innovation to move forward. So hopefully, on some of our current controversies, we can find win-win solutions.

We have just a few minutes for questions from the audience. What I'd like to do is just take two or three questions and then we'll give the panel a chance to react to them and then we'll move on to our next panel. So if you could give us your name. Okay, there's a question over here. Your name, your organization, and we would ask you to keep your question brief just so we can get to as many people as possible.

MR. McCARTY: Hi, it's Mark McCarty with Georgetown University. How do the different aspects of what the three of you are talking about cohere with the global Internet freedom initiative that's being undertaken with the U.S. State Department?

MR. WEST: Okay. If you could hold onto that, let's take a couple more

questions. Right there.

MR. JOHNSON: David Johnson, New York Law School. My question is whether you think the government should, insofar as federate an identify, offer some approaches for secure accountable transactions. Should the government be setting minimum standards for the activities of identity providers or should that be done by the competition among the private sector to build trust marks?

MR. WEST: Okay. Mike Nelson has a question, too, and then we're going to give the panel a chance to respond to these.

MR. NELSON: Mike Nelson, Georgetown. I worked at the White House about 13 years ago and worked on the magazine reports. I'm always happy to hear that brought back. The toughest issue I worked on was encryption, and I thought by now we would really have that all worked out and that we'd have end to end encryption and that we'd actually be able to use these powerful technologies to secure our networks. But unfortunately, some people don't want to see strong encryption everywhere, and particularly Hollywood and the IPR community would hate to see encrypted technology used by pirates. So I'd like to hear where the White House is going on encryption.

MR. WEST: Okay. So we have great questions on global Internet freedom, identify management and encryption.

MR. CHOPRA: I'll start with Internet freedom. Actually, it's a good segue, all three one by one. Let me begin by saying that Secretary Clinton absolutely laid a very strong foundation for Internet freedom that is deeply a part of this process, this inner agency process that I'd outlined in terms of getting the policy answers. But I would also highlight not just the policy questions, but the actual implementation of this.

During the President's trip to India, one of our key deliverables was the launching of a formal open government dialogue with the government of India specifically focused



on empowering democracy through technology. As we actually opened up that dialogue, we convened with Samantha Power over at the National Security Counsel and the Indian counterpart on innovation and entrepreneurship, Sam Patroda, a roundtable of democracy advocates who are actually using technology as a manner of both holding their own government accountable, but also empowering people to improve their living and their daily lives.

That expo, by the way, included case studies all the way from grassroots crowd sourcing of regulating water quality, all the way to text messaging for criminals in the future elections, to getting a sense for the criminal history of any of your candidates, and you literally text in a week before your election cycle.

So in the philosophical and policy arena, it's part of this Internet policy principles conversation that we're having, and in the context of implementation and execution, we very much have been demonstration and celebrating those projects, and I have the pleasure of helping to assist in that effort with the Secretary's team.

MR. SCHMIDT: Yeah, I think it goes without saying that there's a strong desire across the administration to make sure that we do have those Internet freedoms and our ability to really play out through the Internet the very democratic principles that we hold very close to us. One of the challenge that we roll into, which as Aneesh mentioned the dialogue, and that's how do you wind up doing that in a manner that protects intellectual property, that protects children online, while still giving the ability to have that expression of freedom over the Internet? And, unfortunately, like in many of these things, there's no simple binary answer that says you just switch it over here, and we have this, and then you switch it over here and it's the Internet freedom.

And I think a lot of this comes down to a balance on the side of Internet freedom, but that means also then we have to ensure certain levels of security, because

the same technologies give us the ability to communicate openly and freely. Criminals and people that do child exploitation can use the same things to do what they're doing. And it's a real challenge to make this work, which is why we have this coordinating roll working across all sides of government and the private sector to strike that balance.

MS. ESPINEL: I would -- so now I get to go third, it is easy to say what these guys said, so I'll just echo their comments. The open Internet freedom, as Aneesh said, that's something Secretary Clinton has made very clear, that's something that the President -- that is very important to the President. I think open and free does not mean anything goes under any circumstances, I think we're all aware of that, and that is why I think it is so important again that the United States be a leader here.

There will be solutions to these problems that other governments come up with, and I think the United States needs to be out there first in terms of coming up with solutions, because we hold principles, like the openness of the Internet, like fair process, like free speech, these are policy principles that are -- that is important to us, and they are fundamental to the United States, and that's why we need to make sure we are out there first coming up with solutions that fully take those into account, so that we can be, not just an example to other countries, but the kind of example that we want to be.

MR. WEST: Okay. I think we have time just for one or two more questions, then we'll move on to our next panel. Leslie.

MS. HARRIS: Leslie Harris, Center for Democracy and Technology. I've got a two-parter for Victoria. So --

MR. WEST: But that just counts as one question.

MS. HARRIS: It's one question, it really is. So when you're doing a process that's a process with companies, how do you sort of maintain some level of

transparency in some of those sort of procedural things that, if it were being enacted into law, would allow for broader input in debate?

And I think the second one goes to the nature of private agreements. There are a lot of very difficult issues, and IP is one of them, and graduated response is one of them, and how do you do a process that actually includes some of the other stakeholders at the table so that when you finally announce a solution, you have some buy-in from those who may be critics?

So, you know, I'm asking you that specific about that process, but I think it is a core question about what we call multi-stakeholder process.

MS. ESPINEL: Yeah, that's a great question, and I totally agree with you. And, in fact, I didn't talk much about some of the overarching strategy that my office announced in June, but one of our sort of fundamental principles that we laid out that the administration needs to be following is transparency in terms of policymaking and all the processes that we've engaged in. So, generally speaking, you know, that is something that's very important to your specific question. I also totally agree with you, we have been -- my office is new and it is very, very small, but within the resource limitations, at least in my opinion, we have put a huge amount of effort in terms of reaching out to stakeholders.

You know, there is a wide divergence of use here, we want to make sure that we not only know what everyone is thinking, but that we are taking that into account, so that we're coming up with ideas and ways forward that are the best possible.

So hopefully the communities have felt that because it has been a real concentrated effort out of the office and it will continue to be, not just because of our sort of overarching principal transparency, but because I truly believe that is the only way that we're going to make sure we come up with good solutions.

MR. WEST: Okay. Howard, you wanted to address the federated ID question?

MR. SCHMIDT: Yeah, just real quick. There was a question about the federated ID. You'll be hearing, if you've not already heard about it, this strategy called the National Strategy for Trusted Identities in Cyberspace. And that's specifically looking at what sort of an echo system can be created using the talents and the technologies of the private sector, being some of the unique requirements that we have within the government, not only for the government to government work, but also citizen to government work, and so you'll be hearing more about it in the future. But I didn't want to let that opportunity slip by when the question was asked about federated identity, because it's got to be an echo system driven primarily on the back of the private sector. Thanks.

MR. WEST: Okay, thank you very much. We're out of time on this panel, but I want to thank Aneesh, Howard and Victoria for sharing their insights with us and taking time out of their busy schedules, so please join me in thanking them.

(Applause)

And then I want to introduce Phil Weiser, who is going to be moderating our next panel on Users as Regulators: The Role of Transparency and Crowd Sourcing as a Form of Oversight. Phil, as you know, is senior advisor to the director for technology and innovation at the National Economic Council at the White House. And he will be having Mark Cooper of the Consumer Federation of America, Cynthia Estlund of New York University School of Law, and Kathy Brown of Verizon. So if those people can join us, thank you.

MR. WEISER: Thank you, Darrell. I want to start by acknowledging Darrell's leadership. For those who are not fully appreciative of what an impact he's

making here at Brookings, I can recall it was only in April that Vivek, Aneesh and I were here at what I think was the inaugural event of this institute. And since then, he's been at the forefront of facilitating valuable conversations that bring together communities of theory, policy and practice, and this one is a tour de force event. Thank you so much, Darrell, for doing that.

I also acknowledge in another related project the Aspen Institute Idea Project. We'll hear from Gary Epstein later today on a panel. This is another complementary effort that is essentially part of the same enterprise, which is working out a new model -- it has to be international, too -- about how do we think about Internet policy. And this project is one that's been, you know, really now in its second decade or third decade, depending on how you count, because I guess, you know, it started in the '90s, so this could be the third decade, but it really got going in the mid-'90s. And some people deserve some acknowledgement from that, among them Peter Swire, who's here, who will be on the next panel, was one of the people in the White House in privacy during this process. Kathy Brown on this panel was also at NTIA during this timeframe. Mark Cooper, who has been in the consumer community, sort of the great rabbi of how to practice policy in the best possible way, and others, I could go on.

But I think that we are humble to this administration by both the depth of the challenge and by the need to be attune to not just history, but other fields, because although Internet policy was once aspired to be sort of an exceptional thing that didn't have anything to learn from anything else, people have come down a little bit from that to say, well, there's actually a lot that we have to grapple with. And that's one reason why we've invited Cindy Estlund on this panel from New York University Law School, where she is a scholar of labor and employment, but also one of the best of breed in what law professors sometimes call new governance, which is thinking about the basic question

that we have set out to think about in our subcommittee that Aneesh talked about. Aneesh and I, along with Howard, Victoria, are critical in sort of the Executive Office of the President oversight of that, but the people who are most focused on Internet policy principles: Gene Kimmelman from the Department of Justice, and Danny Weitzner, who'll you meet on the next panel.

Danny testified last week, and in his testimony set out what could be set as a broad theory of the case, which is a legacy role of government, and many government institutions was prescriptive before-the-fact rulemaking. That was the quintessential construct for the Administrative Procedures Act for the New Deal agencies.

But we are in the midst of inventing and implementing two new models of how regulatory agencies operate. One is identifying principles that are to be enforced after the fact. That's, indeed, what's being talked about at the FCC on neutrality. That is also what Danny's testimony last week talked about, and I would commend that to all of you as valuable reading, and that is something that we are thinking about in all these concepts.

But there's another point, too, that Aneesh outlined which has probably had less said about it, which is the government role of convener, facilitating best practice, enabling disclosure information to be accessible in terms that are usable. And we're going to talk a bit about that on this panel because there is a role as information gets out there and as conversations are happening to enable what someone calls normative communities to help develop, again, a sense of norms and, in some cases, shame, in other cases, pride, about how policy is made in the Internet space.

So with that, by way of background, let me get into our panel. I've woven introductions in, but I want to give them a little more formally. Mark is not formally known as the chief rabbi of the consumer community, although I personally view him in that role.

He is formally the research director for the Consumer Federation of America. He has been center in lots of these policy discussions. It's fair to say he's seen it all and brings an enormous amount of intelligence and integrity to all these discussions.

Cindy Estlund, to my left, is a professor at the New York University School of Law. She has authored a book recently, I'm going to get the title wrong, but -- the title, what's --

MS. ESTLUND: *Regoverning the Work Place: From Self-Regulation to Co-Regulation.*

MR. WEISER: *Regoverning the Work Place: From Self-Regulation to Co-Regulation*, those are concepts that we'll get to in this context. And she is really one of the finest scholars in new governance and very good to come down and join us today, thank you.

And Kathy Brown, who, as I mentioned, had been in the Clinton Administration, at NTIA, and then at the FCC, has now been at Verizon for almost a decade.

MS. BROWN: Well, eight years.

MR. WEISER: Well, going up to a decade. And she -- there as senior vice president, not only is involved in public policy, but also a corporate social responsibility. So let me start off with a basic question and then we can have a conversation amongst the three of us, and the first one is this concept of transparency and disclosure and how that can be a regulatory tool.

The challenge that is, for example, in the privacy concept is how does disclosure happen in ways that people understand it? So as an academic, let me start with the academic. If you might start, Cindy, just the broad contours of disclosure, when it works, how it works, and then we can go from there.

MS. ESTLUND: Thanks very much for inviting me. I'm a little bit of a fish out of water here, and you know what happens when fish stay out of water too long, so I better get off the stage pretty quickly.

So transparency plays a key role across the range of regulatory areas, and it's worth stepping back to think why that's so important. The field of governance, one of the kind of defining principles or features of the field of governance or governance based regulation is the recognition that good regulatory architecture has to be triangular or tripartite. So you have the -- if you picture a triangle, with the government being at the bottom, the basic level, you've got the regulated actors, and then you have the stakeholders, the beneficiaries who need to be able to enter the process both to guard against cheating or cosmetic self-regulation by those regulated actors, and to guard against capture of the government agencies, the regulators.

So transparency is absolutely crucial to opening the door up both of government and of what's going on inside the regulated actors and enabling both individual beneficiaries. Of course, in the Internet field, the beneficiaries range from very large corporations in some cases to individuals. So people need to be able to both watch what the government is doing and watch what the regulated entities are doing, as individuals and as intermediary organizations.

We are fortunate to have a very diverse and vibrant civil society in which people are constantly forming new associations and new forums through which to speak and exercise their voice and express what they need, and transparency is simply fundamental.

And as far as when it works, how it works, that varies enormously from one field to another, and I'm going to be the learner here rather than the teacher as to what works here. But obviously the Internet has become an enormously important



vehicle for disclosure for other fields. My field of employment and labor law, for example, the Internet opens up possibilities for using transparency as a regulatory device.

But I think it's critical to have sort of layers of transparency, some elements of which can be understood by, you know, an ABC rating system, for example, something that individual consumers can understand and can see. But there also has to be transparency for everything that goes into that, so that the intermediary organizations, the more sophisticated actors, can actually see whether those simple grades make sense. I think I'll stop there.

MR. WEISER: I think you set up Mark very well, so I'll let Mark go next.

MR. COOPER: Phil always uses that rabbi line to remind me to be on my best behavior. And it's interesting, people have said it twice, as someone who used ARPANET in 1971, we're in the fourth decade, not the third decade. And I actually started talking about crowd sourcing for enforcement 18 months ago in the context of network neutrality, which is sort of how I got roped into this, and my answer is that transparency can be an effective tool for regulating behavior only if it exists in a structured context.

So I haven't yet given up the notion that we need enforcement. It's ironic, last week the Federal Trade Commission used an expression, "robust enforceable self-regulation." WTF are they talking about? Wait a minute, folks. Enforceability involves some third party, I think. You can think that doctors and lawyers are self-regulatory in terms of de-certifying and de-licensing people, but it's not very robust. And so it's that external force that I really worry about. And in order to have a good external enforceable regime that uses crowd sourcing -- and Phil knows I'm a consumer advocate, so even if he won't let me make an opening speech, I'm going to get my agenda -- the institutional structure has to answer four or five critical questions that every institutional

structure has to answer: Who gets to complain? Which behaviors are objectionable? What are the consequences for violators? How do people register their complaints? And most importantly, how do they learn about the success of their complaint?

In order to have a system that works, you have to give people that structure. In that context, transparency and information become critical, but the information has to be available, accessible, accurate, and actionable. And those requirements, I firmly believe that we can use those requirements for getting the crowd to help us regulate.

I believe government doesn't have a prayer in this environment of having the auditors and the cops to go out there and police this marketplace, it won't happen, they have lost control. This is the 35th anniversary of a wonderful book, a little bit geeky, with the title of *The Mythical Man Month*, and the technologists and the crowd will appreciate that. The hypothesis was that 35 years ago, IBM, the great software writer of the first part of this century had simply lost the ability to write code because it had become too complex. And the notion of throwing more man or woman hours at it only made things worse, not better, because it was impossible to organize that complex a process in a centralized manner. And the solution was decentralization modernization.

The same thing has happened to government. It is simply impossible for a central institution to manage the complexity of the economy, the Internet and everything else going around it. So what we need is a set of principles from above, a set of structures in the middle, and then the crowd on the bottom really doing the policing work.

And I do believe that the era of writing detailed rules is over. And the faster we learn that, the better form of regulation we'll have. I think I answered the question.

MR. WEISER: Two great answers. Kathy.

MS. BROWN: It's always wonderful when I can start agreeing with Mark, not disagreeing with Mark.

MR. WEISER: Give it time.

MS. BROWN: Good morning, and thank you, Phil, for inviting me on this panel. Just to -- before I answer, a little context on what we're talking about. So I, too, am a disciple of the five principles of the Clinton Administration, and I probably have lived that in world the longest and have really developed my own policy thinking from those principles.

At the same time, I also agree that what was the Internet in 1995 -- 1992, '95, '97, now has grown into a very new vibrant marketplace, one that is evolving all the time. So the Internet itself is a marketplace.

Within it, of course, are very discreet markets, the medical market, the energy market, the financial market, but there's this thing called the Internet that has changed the way markets are functioning. And what is probably central to this debate is the crowd's access to those markets through this thing called the Internet.

That ecosystem now is much larger and much more complex than that ecosystem was in '92, '95, when we started to think this through. Nevertheless, those principles have taken us very far. It has allowed this evolving innovation to keep happening, to happening more and more and more and more, so that what we could even imagine in those early years is actually obsolete already. In that kind of marketplace, I guess I'm probably with Mark, and maybe a little bit not exactly with you, Cynthia, that bottom layer really is the crowd, or for a company like my own, the consumers, it's that great consumer base out there to which we owe everything we have to do.

Maybe on either side of that triangle, I would put the government, and I

would put the advocates who are watching and watching and watching in the company, okay. So the company is over here in my mind, that's my world view.

But this notion that the consumer is at the center of this ecosystem I think is one that I suspect we are all going to agree with. The question then is, what power does the consumer have to exert its control in this complicated marketplace? And the notion of transparency, it seems to me, is enormously important.

We have been saying at Verizon I think now for almost two years that our laws are antiquated, they are obsolete, they are not now robust enough to understand and operate in a very different marketplace, in a different place where relationships are much more complex than they were before. So we object to asserting old-style regulation on a new market. We are very much in agreement that the day of rulemakings are over and that we absolutely do need high principles of which we have to enforce to make sure the bad guys don't take control. So there's lots of agreement here on this panel.

How you get to transparency and the layers that were discussed I think is enormously important. I am in agreement that on this thing called the Internet, consumers need ABC like clarity about what it is they think they're getting. They should - I always say, you should get what you think you bought.

In other words, if I buy this thing that's supposed to do these things, how do I know that it's performing, whether it's the network, whether it's the device, whether it's the operating system, whether it's the apps that are on it? How do I know that? What is the transparency that is required of all of the actors on this thing called the Internet, all of the actors in the market that allow folks to actually access other markets?

And the role of government there, it seems to me, is that of convener, and it may well be that, in a democracy of setting norms. And I don't disagree at all that

government processes will allow folks to come into a process where otherwise they might feel outside of it. That said, this complexity demands that the players in the market themselves have clear policies for their actions, their business case, and how they treat their consumers, and that we are responsible as the private sector market to developing those norms, to ourselves be discussing what those norms are and how we go forward.

And thus, this bad word called self-regulation can also mean that it's a normative process that can inform the greater democracy. So transparency I think is at various layers, and how we get there, it seems to me, is the debate we're in the middle of.

MR. WEISER: So just to review, we have the pyramid with three critical parts, and obviously that could be three pillars. You can reconceptualize it, but it's, again, the stakeholders, it's the industry and government. We have the need for a set of principles, a structure in the crowd, because, as Mark Cooper said, the government -- before the fact, rulemaking is over, and you have to have the five As, which Mark will remind us of later.

And then Kathy Brown, the players themselves have this normative role that transparency helps to facilitate and enable. I want to go to one context that is a test case to talk about, among other things, what Mark said is the need for structure disclosure and oversight, again, as Kathy said, the disclosure would have to be accurate, and that would be Gramm-Leach-Bliley, which was one of the privacy regulatory regimes that govern financial services.

There were at least two dimensions one can judge this on, one which was I think explained very well by Peter Swire in an article called "The Surprising Virtues of the Financial Disclosure Law," is that right? And that is that the law force companies themselves to ask themselves the question that some of them had, which is, hey, I'm a

financial services firm, what should be my privacy policy? So that sort of gets to Kathy's point about, you know, prodding or nudging private companies to think about what norms they ascribe to.

The second goal, most people would say this law probably didn't do so well, Tim Yuris called it government-mandated spam, because you people got these very thick privacy policies. There was no structure for disclosure under Gramm-Leach-Bliley. It was all -- many people were unable to judge them. I think it was Cindy said if you want to have a successful regime for transparency disclosure, you need some form of a structure, I think FDA nutritional labeling that people can understand. Gramm-Leach-Bliley, I think by all accounts, didn't do so well on that. So Gramm-Leach-Bliley, the lessons from it, I want to go in reverse order, Kathy, how do you see both those two principles in general? And if you have particular thoughts on Gramm-Leach-Bliley, that's great.

MS. BROWN: So I won't discuss financial disclosure just because it's not my area, but I can certainly discuss disclosure in our sector. But let me start again with the tension I think between rules that have an A, B, C, D, E, F, G section to them, and principles, and what the consequence is, and that is what I call the tension between a compliance structure and culture and a culture that is actually trying to respond to what the consumer needs.

I'm not saying by this that there ought not be laws and lawyers, but I am saying that laws and lawyers beget privacy principles that are unreadable, because the lawyer's job, inside any organization, is to protect the organization from liability and to make sure they are complying with the letter of the law.

The job of those of us inside a company is to communicate with our customers about what it is we're doing for them, with them, and where they can get

redress if they're not happy. And sometimes these things come into conflict. And the government itself, in my view, the agencies that are promulgating these extensive regulations ought itself to sit back and think about those unintended consequences.

I'm not suggesting that these aren't good faith attempts to make sure everything is buttoned up for the consumer. I am suggesting that they sometimes work against you, and that what we really need to understand is what consumers want. What do they want to know about their service? What do they want to know about the way a company operates?

Most consumers, and I do a lot of polling for my company, actually don't really give any credence to what goes on internally, they just want the output. I'm not suggesting that the intermediaries don't want some transparency into processes, and that can be provided, as well, but it seems to me we have to get to a culture, particularly in this complex Internet space, where things become easier for the customer, not harder.

Today's privacy principles, it seems to me, are going to be a test of whether and how with different, again, different markets operating within the Internet market space, think medical privacy and financial privacy as opposed to Facebook privacy, how overall there is an ease of use for customers as they operate in this very new world.

MS. ESTLUND: I guess one thing I wanted to introduce into the conversation is the notion that not all stakeholders are customers. Not all those who are affected by regulation and its success or failure are customers. And so when they are the customers, I think the market does an excellent job, and sometimes the answer is just to empower those who are forward looking and who have internalized the norm of something like privacy.

I think the idea of relatively generalized or sometimes even ambiguous

norms that are enforced ex post is an excellent strategy, especially when you're operating -- when the regulated actors are responding to the interest of their consumers.

But if we think more broadly, and I'm sure there are analogs in the present Internet context that you all could think of immediately to pollution, where the effected constituencies are not the customers, who can't rely -- and we can't rely on market mechanisms. Even forward-thinking progressive market mechanisms may not be enough to respond adequately to those external needs. So transparency beyond what your market constituencies may want is crucial to allowing those constituencies to have a voice.

I think the one critical challenge, and again, I retreat to a more general framework here, one challenge here is always how to empower the high road actors to get out ahead of the curve, formulate and improve upon best practices, figure out what the next horizon is, how to do things better, how to have a regulatory architecture that both does that through generalized norms and constituencies that have internalized those norms, while at the same time having a capacity to reliably discipline the low road actors, those who are acting opportunistically, who you really do need. You need to have that deterrent threat. And whether the same -- whether you have to have multiple regulatory tracks or whether a single ex post standard is sufficient to regulate those low-road actors, I think the answer to that is going to vary somewhat, you know, from one area to another.

But it's worth keeping in mind that not everyone, not all the actors out there are motivated by market forces to do the right thing, get out ahead, internalize the norm, and figure out how to do a better job.

MR. WEISER: So I don't know if Cindy meant this, but we've had a number of cases of cyber bullying recently. In an article on the front page of the *New York Times* the other day, that's a form of a negative externality, if you will, that isn't



really about sort of the industry and consumers, but it's how the technology can be used in ways that public policy obviously has concerns with.

The third panel will address some of that user education, because obviously one of the true things about the Internet is, everyone is both a user and a producer. Being such an open platform has certain responsibilities and risks that have to be grappled with. Mark, why don't you take us home on this? And then after crowd servicing, we have to let the crowd offer some of its wisdom and thoughts and we'll go to the audience for some questions.

MR. COOPER: Well, the way you justify public policy in America is demonstrate market failure. If you can't demonstrate significant market failure, you cannot move policy forward, that's a fact of life. There are other countries where that's not the case, but we have to govern the country we live in. The simple fact of the matter is that the extent of market failure in the information space is immense. High-road actors can't discipline low-road actors if there isn't competition between them, and if consumers can't understand the difference and act on it, and this is the fundamental problem in financial markets, in technology markets. The average consumer is simply outgunned.

There is no way that that consumer is going to be able to comprehend the technological arms races that go on in the back office and be able to act on that kind of information, even if they get it. And, frankly, there's a tremendous advantage, an asymmetric information problem, so that people who produce goods and services have the information, they have no interest in giving it to anybody, and then, of course, when they give it to the poor consumer, the consumer can't possibly understand it anyway.

In answering -- addressing the market failures, you can and have to design principles. And I'm going to agree with Kathy, we need some principles, although she talks about old-style regulation, I talk about traditional values. We need some

principles about what consumers should deliver.

And I exist in a different space. We're having a great debate about the fuel economy standards for automobiles. The National Highway Transportation Safety Administration has decided to give a letter grade to each vehicle. They're going to write the 25 miles per gallon or 35 miles per gallon, but then they said we're going to put an A, B, C, or D on that vehicle, and they've done it arbitrarily, just, you know -- but it's fairly transparent. I mean, more transparent than the way your kids get their grades in school. You haven't got a clue about how that teacher gave your kid an A or a B, right? Here they've got 120-page regulation which describes which category they fell into.

The automobile industry is absolutely furious about having a letter grade on their vehicles. Why? Because no one wants to get a C. And even if 22 miles is really crummy, somehow or another they think it's better, well, 22, because the consumer doesn't understand what 22 means. The C they understand because their kids get Cs and it bothers them.

It has to be really simple. And the claim, the expectation that consumers will be able to use that information in the financial services space or in the technology space just doesn't wash. So we have to work really hard to get some principles now.

And Kathy talked about the great mass of the crowd, but there's a different set of people known in the marketing literature as the mavens, right. Mavens can understand stuff better. So, in point of fact, what we need to do is design stuff for mavens who can then educate the rest of the crowd. But I thoroughly reject the idea that merely making information available is sufficient, it has to be in an actionable form.

MR. WEISER: Two quick comments and I'll go to the audience. One is what Mark says, sort of relates to one of the real opportunities of the Internet which is trusted intermediaries. Another one of the organizations Mark works with, Consumers

Union, Consumer Reports has achieved legendary status there. That's something in the Internet era that is out there, and there's an aspiration that you can have that done by technology alone, a la Amazon's rating system or eBay's, which is you have individual people and then technology figures out who to trust and how. I'm sure that'll be something we'll talk about more.

Another on the later grades that's worth adding is a really interesting study about L.A. Health Department, where they use grades as opposed to some other incomprehensible system, and they graded just, you know, objectively, not on a curve, whether you're A, B, or C --

SPEAKER: Restaurants.

MR. WEISER: Restaurants, yeah. And the restaurants, what happened was, people were more willing to try restaurants they hadn't been to before when they saw they had an A, because, you know, the way people historically protect themselves in restaurants is going to places they know. Part of the fear was that if you don't know the place, what could it be like? Well, this helped allay that fear, so that's another one of the positive benefits of understandable information disclosure.

Thoughts and questions from the audience? Yes, I'll start in the back. And are there microphones, Darrell? I can repeat the questions, too.

MS. KRIGMAN: Hi, Eliza Krigman, *National Journal*. This question is for Kathy. Why does Verizon think that Congress, rather than an expert agency, is better suited to create the rules for net neutrality, and is this because you think you have a better chance of lobbying Congress to get a sunset provision into the law?

MS. BROWN: So it was inevitable, right? I think I opened by saying we firmly believe that the current law is not up to snuff for the new marketplace, that we need a new framework, and we've said this fairly consistently. We, I think, are -- Tom Tuckey

was out a year ago saying we need to upgrade the laws. We've laid out what we think the principles ought to be. In the net neutrality context, which, let's face it, is a narrow -- it's a narrow piece of all of the policies that are being looked at in the Internet space, we think that the law is not written for the Internet age.

I, myself, as Phil said, I was at the FCC when we were putting into effect the rules under the '96 act. I think, again, if you take a hard look at that statute, the word "Internet," it's just not there. We're talking about advanced technologies, and the Congress really was not thinking of this very complex marketplace.

Interestingly, as I listened to Cindy, and she talks about regulated industries, I think this is a great example of one. In the Internet space, of course, there is government oversight either by the FTC or by the FCC, but that oversight is very different depending on who you are in that space.

It's not been brought up to date to give consumers clear rules, to give clear guidance to behavior, to have clear transparency, and it's our firm believe that the agency has a very difficult time acting under law when the law is not written for the age. So that really is the basis of our position, and I think we've been quite consistent on that.

MR. WEISER: Others, yes, the back, also.

MS. MARSHALL: My name is Julia Marshall. I'm with USAID. Every time I hear the word "crowd sourcing," I get a little disturbed and very skeptical because history in the past, there have been numerous examples of crowds being manipulated, and manipulated into doing very heinous things like genocide, lynchings in the South, et cetera. And, you know, every time I hear this word, I just want to say, so how are we going to prevent somebody from coming along and manipulating a large group of people into doing something that we look back on and are really ashamed of, you know, sometime years down the road?

So I'd really like to hear how that would work, you know, or what kind of ideas that you would have on protecting minorities or other people who are a little different.

MR. COOPER: Well, it's a fascinating question, and I've been around long enough to have participated in these great debates among progressives, who really were very concerned about highly sensualized media, you know. They were concerned, you know, broadcast TV, cable TV is very concentrated markets, and they always wanted more open speech. And then the Internet came along, and they suddenly discovered the cacophony of the masses.

And you get the answer, it's such junk, right. They thought the people were going to produce PBS, which has a less than 1 percent market share. So the problem is that democracy is an ugly space. It's a beautiful space, too, but I would answer that anything you do to try and prevent people you don't want to speak from speaking will end up more likely preventing the people you want to speak.

So you have to take the good with the bad. And there's absolutely no doubt, in a world where 60 percent of the people on this planet have a cell phone, which is a remarkable accomplishment, the entire race can speak to each other. You have to have confidence, I used to say faith, but now I say confidence, in the democratic process.

So more speech is better in the aggregate, and efforts to try and control speech will always work to your detriment. And ironically, I think that is a place where the left and the right can agree, more speech is just better.

MR. WEISER: Let me add one point, which is, Louie Brandeis was probably one of the greatest American philosophers ever and had a couple concepts that are on point, and it's fascinating that, you know, we need sort of who's the Brandeis of today's Internet age, because he had the insight that sunlight is among the best of

disinfectants, and the Internet and disclosure is an extraordinary approach for sunlight.

And if you think about how the Internet has actually done the opposite of what you just said, it's called out some of the ugliness in ways -- I mean ask, you know, Trent Lott literally, you know, lost his position because people on the Internet were talking about the Strom Thurmond statement he made wasn't a one-off, there was lots of times he had said that, apparently like people on the Internet figured that out.

Dan Rather may well have lost his job because people on the Internet figured something out. So it actually -- sunlight is the best disinfectant is not simply a philosophical idea, it actually does have some resonance.

The second apropos of more speech, you know, in *Whitney v. California*, Brandeis has a very, you know, pointed concept, which is the cure for speech is not to try to stop it all down, but to have more speech, and the Internet, again, is a powerful medium. So you're right when you put out the sort of scary vision of what the Internet can be used for, and I guess we are conducting an experiment. I'm probably with Mark on this, I'm optimistic of how it goes, but not to say your point isn't important. It is.

Other questions? We have one up here.

MR. SMITH: Bruce Smith, Brookings and George Mason University. I have a little trouble with some of what is being said here, not that it's necessarily wrong, but it's just meaningless, it's just quack-quack policy, wonk-speak, buzzwords. Without making a long speech, let's just look at -- just take the IRS, for example.

The IRS is still there. It issues five categories of rules. The era of rulemaking is not over. It has a preliminary rule, a final rule, a this rule, that rule. You're still paying your taxes, it's still enforcing people who don't pay their taxes. If you file on the Internet instead of filing in hard copy, this doesn't make the slightest bit of difference in the real thing of what it's up to.

Now, you're saying, gee, there's something that should be totally different about government when it comes to the Internet. We don't like traditional rules, we don't like traditional this or that. Well, the government is still going to be there. That's what government is, it issues rules and laws. What is it that you're actually talking about? Do you want something that is different from democracy, different from how government has always operated, and what could that possibly be? What are you talking about?

MR. WEISER: Good to get questions from first principals. So it would have been good probably to begin the panel on that question, but I think let's end the panel on that question. How is this regulation of the Internet something different in the nature of how government should proceed than let's say the IRS?

Yeah, Cindy, why don't you start with that?

MS. ESTLUND: OSHA is still there, too, but the question is whether OSHA can -- how far OSHA can get in prescribing safety rules that are based on the technology that was in place when the detailed rules were written and how much they have to move to a general duty, which is enforced mostly ex post, and through empowering those internal actors who are in charge of safety inside companies to get out ahead of the curve, both the curve in technology, the curve in ergonomics. So we're talking -- it's not that the Internet is completely different, it's that across areas of regulation, we need to move to -- technology affects every area of regulation, pollution control technology, for example, and so it's a shift toward a new kind of regulatory strategy that can keep up with changing technology.

MR. WEISER: Kathy.

MS. BROWN: I don't disagree with you. I think I started by saying there are different sectors that now do business on this thing called the Internet. Those sectors are regulated, overseen -- I hate the word "regulation" because some oversight is not rule

regulation, but it's enforcement regulation even now, so all of those sectors have a rule of law that is enforced by the government.

The question that has come up, and what we've wrestled with are twofold: One, how do we ensure that people have access to this new marketplace called the Internet, and what rules apply with respect to that access and use in this new market, this new marketplace? That's one way it's come up.

And the other way is, what are the cross effects between sectors of entering this new marketplace where business is done differently, thus, the privacy issues? That's how you share the security issues we heard earlier. And that's I think a right thing and not nonsense to be grappling with. It's as if you have established a new marketplace, a new city square, and you have to figure out, well, how do we -- how does civilized human beings operate in this place.

I think that this is a fair question, and it is the question that I'm suggesting has not really been understood well enough, thus, that the imposition of law is still fuzzy.

MR. WEISER: And to close us out, Mark Cooper.

MR. COOPER: The best definition of democracy that I have ever heard is people get to write the rules under which they live. Now, you don't actually have to have government to write those rules. Frequently they will organize themselves into common resource and management and so forth. But in a nation of 300 million people and a globe of 6 billion people, you're going to get institutional government and representative democracy, we hope.

And so you have this representative democracy in which people are supposed to participate in the writing of the rules, and you've described the process we have from the 20th century, or actually from the 17th century, of proposing a rule and



notice, et cetera, and comment. That's, unfortunately, the problem of having to live -- of living in a society as big and complex as ours.

What we're talking about here is, A, facilitating the participation in that process. The Internet has really inundated the government with huge numbers of comments and so forth, and people really do seem to like to participate, they'll send in millions of e-mails.

The fundamental change here is going one step further. What crowd sourcing may enable people to do is participate in the enforcement of the rules under which they live, and that hasn't been the case before.

The notion that individuals can, in fact, identify abuses, bring them to the attention of the government through this process, and influence the actual enforcement of rules is actually a much more potent possibility now. It's always existed. You could go down to the cops and complain, et cetera, but here, this is a very much more powerful way, and, frankly, I believe a major improvement in the democratic process, albeit in a representative type of democracy.

MR. WEISER: That's a good note to end this panel on. Thank you all very much and thank you to a wonderful set of panelists.

\* \* \* \* \*

MR. WEST: So, our next panel is going to discuss Internet governance through multi-stakeholder bodies. The moderator for this panel is Danny Weitzner. Danny is the associate administrator for the Office of Policy Analysis and Development at the National Telecommunications and Information Administration. Danny.

MR. WEITZNER: Darrell, thanks so much. And let me just add on

behalf of NTIA our thanks to Brookings for pulling together this terrific discussion.

So, I'll introduce the panelists in just a moment. To give us a little bit of context here, I think that you can see from the opening panel we have a bit of a framing of the substantive policy challenges that face us, the issues that at least we in the administration feel are really, really leading questions that we have to address in the Internet environment; copyright protection, cyber-security, the global free flow of information, and commercial data privacy. It just so happens that the Department of Commerce's Internet policy task force is working on all those four issues, and so these questions are very much at the top of my mind.

From the second panel, from Phil Weiser's panel on transparency, what you heard was the institutional challenge. You heard from Rabbi Mark Cooper that the era of detailed agency rulemaking is over. There's a lot of Clinton Administration resonance, it seems, in this room. But I think we have to take that awfully seriously from someone like Mark at the Consumer Federation of America, whose lifeblood, in many ways over the last 20-plus years, has been to engage in just that detailed agency rulemaking at both the federal, state, and sometimes even local level on behalf of consumer interest.

And so I think that leaves us now with the question, now what? If we don't have this -- our normal process, the traditional process that we're all used to of legislative authority given to expert regulatory agencies around which we have lots of advocates clustering to develop rules, what do we do?

This panel is an effort to begin to answer that question. And I certainly subscribe to the notion that we're not getting rid of that traditional regulatory style altogether, but that the Internet seems to call for some additional mechanisms.

I want to just frame a bit of the motivation of this panel by citing another

Clinton Administration official, the chairman of the FCC, Reed Hundt, who when we were all first starting off looking at our policy agenda at NTIA, Reed Hundt came and gave one piece of advice that I've really taken to heart. He said if you're looking at how to have a long-run impact on the direction of policy, you have two choices, basically: You can make rules, or you can make institutions. And what he pointed out quite simply was rules change. Administrations come and go, policymakers come and go, but institutions actually have a way of sticking around. And that's sometimes a good thing, sometimes a bad thing.

But we're really here to look at on this panel is the question of how we can create a new set of institutions that can allow us to make progress in a balanced manner on the substantive policy issues that we've talked about.

We have an extraordinary panel. It's a panel full of people who I've looked to for guidance over the course of my career and who have tremendous accomplishments in this area. I'm going to introduce them very briefly and then turn to each of them for a short framing statement.

To my immediate right is Peter Swire. Peter is a professor of law at Ohio State University. He's both a scholar in the privacy area and the cybersecurity area, and in housing finance, as it happens. That's why he ended up as a policymaker at the National Economic Council at the beginning of this administration, where he provided me personally tremendous guidance.

To my immediate left is Ernie Allen. Ernie is the president and CEO of the National Center for Missing and Exploited Children. NCMEC is a congressionally-chartered organization whose mission is to protect children who -- both online and off -- in a whole variety of context to be a little ecumenical. I think it's fair to say he's a godfather, really, of this multi-stakeholder model and the effort to advance important public policy

goals in complex global environments. His organization, as you'll hear, really pioneered a style of working with law enforcement, working with industry, working with technology companies, and working with advocates towards a really vital goal. And we'll look forward to his thoughts.

In some sense, the simple question for this panel is how do you bottle and replicate what Ernie's been able to accomplish.

To my right is Joe Waz. Joe is the senior vice president for public policy at Comcast. Joe has seen the evolution of his company and of the cable industry from being just the cable company to being the triple play to big companies that's in a wide variety of information and communication businesses. And he's now wrestling with questions of how to build a new governance framework in the Internet environment. We'll look forward to hearing from him.

And then finally, to my left, Leslie Harris. She's been -- who is the president and CEO of the Center for Democracy and Technology. Full disclosure, I was a founder of CDT. But Leslie's been a leader in the Internet civil liberties arena from before there was an Internet at the ACLU. (Laughter) She was a teenager at the time when she started. (Laughter) But what that means is that she brings really extraordinary perspective and an extraordinary range of accomplishments in the area of building coalitions to advance civil liberties and other important public values in very complex and rapidly changing technology contexts. We're going to turn to Leslie to hear about her efforts in the global free expression environment.

So, I want to begin by asking Professor Swire to give us perhaps a little bit more with his scholarly hat on, a perspective on how we ought to think about the process of creating institutions in this Internet policy environment. So, Peter?

MR. SWIRE: Thanks, Danny. And thanks to Darrell and Brookings for

hosting this.

The structure of what I'm going to try to do, in a lot of ways, comes from work that people did in the 1990s. Again, I wrote an article on self-regulation markets and legal enforcement in 1997 back when the Department of Commerce was trying to figure out how to do self-regulation and markets for privacy. Of course, they're doing it again and there's a lot of reason for that.

There's this area of constant technical change, but the underlying intellectual structures don't change nearly as quickly, and so I'm going to try to put out a couple of ways to think about when multi-stakeholder groups are likely to succeed or not succeed.

The first frame here is market structure, market concentration. So sometimes we have monopolies and sometimes we have a few companies or entities, and sometimes we have lots and lots and lots of companies. And the chances of getting the industry to do something varies with the market concentration.

So, in the privacy area often is the question of whether there's been a set of promises that are enforceable. If you promise a set of things, then the FTC will come after you if you break the promise for a deceptive trade practice. And we've seen that happen sometimes when there's one company.

So, about 10 years ago Microsoft had a product called Passport. And it got into a tussle on enforcement with the Federal Trade Commission. And the answer out of that was a consent decree. One company can say, okay, here's the promises, here's what we're going to do going forward. And it's pretty easy to imagine a government agency with one very big leading company being able to negotiate that out. You don't need a law for that, you don't need a regulation. You get a series of promises from the one and it pretty much can work because you can really, really see that one company if it doesn't do

a good job, and there'll be publicity enforcement.

Sometimes there's a few or several companies. In around 2000 there was something called the Network Advertising Initiative. And the biggest company in that was a company called Double Click. And at that point you could get three or four of these ad companies in the room and they had more than 90 percent of the market share.

You can have a meeting with four people in the room. You can have them all sit there, they can have meetings at the Department of Commerce, in the White House about what should happen. They can have different meetings with the FTC. They can have different meetings up on the Hill. But it's a manageable size, and if you have a market structure like that you can imagine getting to something like what happened there, which was basically an agreement among the 90+ percent. Here's how we're going to do cookies, here's how we're going to do things. And that can be negotiated out in a pretty understandable way.

But sometimes you don't have one or a few, you have a bunch of companies. An example here is the Direct Marketing Association. So the DMA had a series of self-regulatory efforts over time. They used to run the telemarketing Do Not Call list. They had a series of privacy promise programs about Internet privacy and the number was a few thousand. So the DMA could have a conference and you could have all the few thousand people at a big conference in a big hotel.

It's much harder to get it in an office in Danny's building to meet with a few thousand people. I mean, Danny's got a nice office, but it's not that big. You can't have several thousand people.

And so when that happens, you need to have a series of intermediaries and you, over time, can get that industry to gradually get to a series of promises. And it can then actually apply to all the members of the industry.

But at that point you start to notice who's in and who's out. So, who's in are what Cindy Estlund, I think, called earlier today -- I hadn't heard this term -- the high-road companies are in, the ones who are willing to make the promises in public, and the low-road companies -- the little ones out there -- probably haven't made that promise.

In some earlier writing I used to call the big companies that were visible the elephants. It's very hard to hide if you're an elephant, right? But you have a thick skin, you have lawyers to protect you, but you're very visible. And so when it comes to the Internet and these multi-stakeholder things, the great big elephants have to play. They have to be part of the conversation.

But on the Internet, and for the direct marketers, also, you have what you can call the mice, the little ones who scurry around, who breed annoyingly quickly. Lots of new sites pop up, right? And they hide in the woodwork, they hide overseas where our enforcement isn't so good, and Howard Schmidt then says we need international, you know, strategies to go for cybersecurity.

So when you have a lot of these many players who can have a big effect and there's many, many of them and they're good at hiding, then it's hard to imagine that your multi-stakeholder process is going to do very well. Or at least you're not going to do very well at closing down the spam kings or closing down the spyware providers, if they're coming from far away, et cetera.

So this market structure is just one simple way from one to many for when you're likely to succeed. I'll make two other quick points and then let other folks go ahead.

What I just talked about is when a set of enforceable promises is likely to work for the industry or the stakeholder group. There's at least two other reasons that are prominent for why you'd want the stakeholders to gather together.

One of them is they might have a lot of expertise. You might have something called the Internet Engineering Task Force. We have a lot of really smart people all over the world who try to have some process to get smart people to agree on things. And for that, that's not particularly a government strength. They might or might not have people from NIST or something there, but basically it's getting those smart people to do, and that's going to have a lot to do with the community norms of when that works or doesn't.

And then the last point is, sometimes you have what economists and lawyers and the states like to call network effects, where you're worried about interoperability. And the more people you can hook together, the better the whole thing works.

A great example of this in the history of the Internet governance is the domain name system, which started out in a professor's basement out in California. Then he had a bunch of buddies around the world who, like, worked together on the domain name system. And then it got really big, because domain name is how you get to the right URL, to the right WWW, whatever it is. And if it doesn't work it's extremely frustrating for the companies or for you or for anything like that.

And that evolved into something called ICANN, which almost nobody loves, but at least it's sort of been there for 10 years now or more, and it sort of works. And the point there is, when you have to actually interoperate in a way that I really have to get to the right web address. Over time, that expertise group and that let's-see-how-we-connect-it group tends to evolve towards more formal regulatory enforceable things, because having the route directory go down is just not a good option.

And so when it gets important enough to interoperate, then the multi-stakeholders off on the side isn't going to work and you tend to evolve more towards a



government structure.

So that's what I have to say.

MR. WEITZNER: Peter, thanks very much. So, Peter's given us two scales on which to think about this question of what kind of institutions we need. A scale that has to do with size and accountability, and then kind of another scale that has to do with expertise and perhaps competence and ability to implement.

I want to turn to Ernie Allen now. Ernie, as you'll hear, works on what is clearly among the more pressing problems just in the world that is protecting children, and works in an environment where accountability is awfully hard. There are a huge number of actors here and there, and it's also, paradoxically, to be an environment in which we tend to assume that law enforcement has this covered totally, right? I mean, this is -- if the police are not protecting kids all by themselves, what are they doing?

But I think that what Ernie has learned is that it actually takes a much more complex structure to work with law enforcement to enable them to be effective.

So, Ernie, what do you have to tell us about how to build institutions such as yours?

MR. ALLEN: Well, I think, Danny, first, thank you for the opportunity to be a part of this panel.

Much of what, I think, we have learned we've learned through evolution. You make the point about the role of law enforcement. Law enforcement is doing extraordinary work in attacking the issue of child exploitation, child pornography on the Internet. Light years from where we were a decade ago.

Yet it became quickly apparent that, like the war on drugs, this is a problem you're not going to be able to arrest and prosecute yourself out of. There's simply far too much of it, far little capacity of government.

And so what we evolved to -- and a little bit of history. In 1998 -- as Danny says, we're a government-chartered nonprofit with a series of very specific tasks that we perform on that side, one of which is to operate the National Missing Children's Hotline. In 1998, we were asked to do something similar for the Internet. The then-Vice President Al Gore announced that the Center was going to become what he called the 911 for the Internet. We created a cyber tip line to take leads from the public.

Same year, Congress mandated electronic service providers to report suspected child pornography to that cyber tip line. So, we became sort of the central repository, the clearinghouse of data and information about those kinds of crimes and that kind of content. We worked, over the years, to try with law enforcement. Our primary role is to take those reports, try to identify where they're coming from so that we can identify the appropriate law enforcement jurisdiction, and then hand it off to that agency -- federal, state, local, or international -- for investigation.

But it was clear that wasn't enough. In the first place, child pornography images are really not pornography at all, they're crime scene photos. They're images of the sexual abuse of a child. And even when you successfully prosecute the offender, the photos stay out there forever, the photos of the victims. So, it was clear that like the war on drugs, you can't just attack the enforcement side. You also have to attack the demand side, and you have to figure out other kinds of approaches to at least minimize the re-victimization of the children featured in those images.

And so what we evolved into is a -- and whether this is self-regulation or co-regulation or where that fits, I'm not sure, but because, by historical accident, the Center was sort of the primary repository of data and information about this kind of content, what we tried to do was develop a system that provided, in a voluntary way, for electronic service providers to receive daily lists, daily feeds, regarding URLs containing

the worst of the worst images. And by worst of the worst, the goal was to identify content that nobody thinks is protected speech: images of prepubescent children in the most egregious kinds of settings.

Now, we have critics who say, don't you care about 13-year-olds? Well, of course we care about 13-year-olds. But the goal here is to help companies develop a mechanism for identifying the worst of the worst images in their system so that they, on a voluntary basis, can take action under their terms of use.

So, today there are 82 companies representing about 80 to 85 of the U.S. Internet industry who receive a daily feed from us of content, of URLs of the worst of the worst. And it's reviewed every morning at 3 a.m. If the image comes off, the URL goes off the list.

About six months ago we began to try to -- even though it's voluntary -- to track what companies were doing with the list. And the participants include companies like Google and Microsoft and Yahoo! and AOL and Comcast, the major players in the space.

What we found is over the past 6 months, 6,400 URLs have been communicated to these participating companies; 6,400 URLs have come down. Search engines are using the list to block this kind of content appearing in search results. The web-hosting companies, companies like Go Daddy and others, are using to block it upstream. So, it -- I think it's a process that is working, it is voluntary. We are playing a role of central clearinghouse, central resource.

One other quick example, Danny -- and I see my friend Mark McCarthy from Georgetown in the audience. Mark was at Visa four years ago, when we began to notice that commercial child pornography sites were containing credit card logos. And that purchasers -- in one case, 70,000 purchasers of a child pornography site that

included, among its options, something called "Baby Rape," 70,000 purchasers were accessing that content and using their credit cards. I called the former FBI director, who was then at MBNA Financial, the largest issuer of credit cards in the United States at that time, and said how is this possible? And what he told me was we don't know what these transactions are for. I mean, they're not using a transaction code for child pornography subscriptions. If you can identify for us in a timely way where these sites are, who the merchant bank is, where the account resides, this is an illegal use of the payment system.

And so because of Mark, Visa and the other major credit card companies, major banks, major Internet companies, third-party payment companies came together in a coalition using our center as the clearinghouse, as the information clearinghouse. As we identified the sites, we would alert the companies, they would review it, take action under terms of use, stop payments.

In four years, this problem has gone from a multibillion dollar industry -- based on the estimate of one of the participants of our coalition, an Asian company that hired Mackenzie Worldwide to do an estimate -- to a problem that the Treasury Department's Office of Terrorist Financing told me two months ago in an e-mail is effectively zero. And that's because these companies, using existing law in a voluntary way, sharing information through a central clearinghouse, effectively eliminated the ability of these people to collect.

Now, I'm not sure it's effectively zero. I'm sure Russian organized crime and others have come up with some creative way to collect money out of this that we haven't discovered. But, Danny, I think my view, from these two approaches is that in a voluntary way companies coming together to share information -- and maybe this is Professor Swire's high-road companies. Because, as I say, we have 82 participants, not

hundreds. And they're primarily the largest companies. But the impact this kind of voluntary collaborative effort can have in addressing these kinds of problems that are clearly unlawful, and clearly violate nobody's rights of free speech, we think is working and is something that certainly should be examined.

MR. WEITZNER: Ernie, thanks very much. I think you can hear in Ernie's description of his really extraordinary work and an extraordinary accomplishment - - as Ernie said, number one, the clearinghouse role, which -- but I think also a prioritization role, which really comes out of the kind of expertise that Peter talked about. It's the question of understanding what's going to have an impact, how the collective action of the voluntary participants can actually come together to achieve a particular goal, to know to go to Mark -- I would have gone to Mark anyway. But -- we always go to Mark. But to know to go to the payment processors reflected a deep engagement with the problem, obviously, and the ability to mobilize that kind of action.

I think -- so again, I think there's the theme, really, of the collection of expertise in one place that can really help a very large group of entities function in a smarter way.

I want to turn -- and I guess what I would suggest is that between what we've heard already from Peter and from Ernie, there's clear examples of models that show that multi-stakeholder processes. We're going to turn to Joe Waz to talk a little bit about a new organization that he's been very involved in putting together that's designed to meet a very politically challenging and sensitive issue, response to this issue, the net neutrality issue. And then we'll turn to Leslie Harris, who's going to talk about how it may be possible to bring these kinds of models into the global environment, which has its own set of challenges.

So, Joe, please.

MR. WAZ: Great. Thank you, Danny. About a month ago in this room David Cohen of Comcast gave a speech, a keynote, where he talked about Internet self-governance and the evolution of Comcast's involvement in the space. And the thing that really drove -- the event that really drove, precipitated our deep level of interest in this was the issue we had before the FCC, the so-called BitTorrent complaint back in -- starting back in 2007. And what we learned from that process is, you know, we were faced with a network management decision that we had made about how to manage certain P-to-P protocols at the time.

It was objected to at the FCC. We wanted to find a way to resolve the question, not litigate the question. And -- but there was nowhere to go, to have that dialogue in the United States. What we wound up doing, at the time, was going to the IETF that Peter referred to earlier, the Internet Engineering Technology Forum, and brought our ideas of alternative approaches to network management, ways to manage the bandwidth consumption of certain protocols or by certain users to a broader international dialogue.

As a result of that dialogue, we came up with a system called Fair Share, which does not manage bandwidth based on protocol -- or it's protocol agnostic, but rather based on individual user's consumption. And we vetted and went through the IETF process and then announced we would implement this plan. We actually announced we would implement this new plan some six months before the FCC, under previous management, decided to condemn us for the plan that we had chosen earlier.

But the thing we learned -- I think our main takeaway from it was, in the U.S. there really wasn't a formal, or even informal, domestic venue to go to to have these sorts of dialogues about network management and the interaction between networks and applications and services. We continued, over the years, to bring our questions and

some of our solutions and our new network management ideas to IETF.

I think many of you may be acquainted with something called Constant Guard, that we launched in -- piloted last year and have launched broadly now, that is intended to deal with bots and viruses and other threats to your Internet experience and the security of the network. We actually brought our ideas on that to IETF as well to have a dialogue.

Why IETF? It's an international engineering-focused, consensus-based institution. You can go to IETF, everybody has standing when you go to IETF, provided you can bring the engineering expertise and the capacity to engage effectively in the dialogue there. And it is a normative body. It gave us a place to go and say we are thinking about doing X or we have implemented Y. What does the Internet community think of this idea or of this innovation? And in our interaction with IETF, we actually were able to refine a number of our ideas.

So, the beauty of it from a -- as it relates to policy is, instead of a situation where you implement or practice and the only way to have a dialogue about the practice is a legal complaint process at the FCC involving lawyers and advocates and politics, you have a forum where you can go to and engage among engineers, among experts, and look to build consensus and develop answers together.

So, our -- in various dialogues with people like Phil Weiser, other companies in the industry, with academics, and others over the years -- over the last couple of years -- we began asking, how do we bring the best of IETF back home? How do we make this -- how do we create the equivalent of a domestic IETF?

And the notion that was developed is something called BITAG, the Broadband Internet Technology Advisory Group. Its existence has been announced. Its board will have its first meeting this month. I believe it's going to -- we've already had expression of interest from about 40 organizations. And the idea is to have a cross-

section of the Internet community: Internet service providers and network providers, technology companies -- the Silicon Valley companies, for example -- equipment companies, content companies, and representatives of the Internet community at large, academics and NGOs and advocacy organizations in the room. And have those organizations be able to take questions or present questions for the BITAG to consider.

The BITAG will work by empowering working groups, technology working groups -- engineers and technologists are welcome, lawyers like me are not -- and try to frame the question, develop consensus, and come back with recommendations, answers, ideas, alternative approaches in a timely fashion.

It's -- the point of the group is also to try to educate policymakers generally about network management issues and other technical issues and to serve as a sounding board for new ideas and practices. So, you don't have to go before BITAG with a complaint, you can go before BITAG with a question or an observation and try to tee up the dialogue.

What I think is going to make BITAG work, what gives me hope is that, number one, the great expressions of interest across the board from the range of organizations I mentioned. Number two, we had to find the right convener. And to paraphrase an old Sarah Lee commercial, everybody doesn't like someone, but nobody doesn't like Dale Hatfield. (Laughter)

And Dale Hatfield has to be the most respected engineer in our space who, whether you've been with him or against him on any given issue, you can never doubt his integrity and his capabilities. And, fortunately, even with all the other obligations he's taken on, working at Silicon Flatirons and so on, Dale's been willing to step up to this challenge.

So, what I hope will be the case is that BITAG will build on our



successful history with IETF, with MAAWG -- actually, quick show of hands, how many people know the acronym MAAWG? Okay, maybe about 10 or 20 percent. Messaging Anti-Abuse Working Group, which is a global -- another global organization, it represents about a billion e-mail boxes across the globe. And they're focused on all forms of messaging abuse online, from spam to viruses to bots, denial of service attacks, and so on.

Another example of a global organization -- and Danny, as time permits, here, I would like to be able to come back to a conversation about how official Washington interacts with a number of these global organizations. But another important global organization that I think provides a model for developing normative behaviors that we have to learn how to better leverage for domestic policy purposes.

MR. WEITZNER: Thanks, Joe. I want to just highlight from my own experience one point that you made, Joe. You know, the -- identifying Dale Hatfield, who we do, indeed, all love. If you're out there, Dale, hi.

I think that from my own experience working with organizations like the World Wide Web Consortium, the Internet Engineering Task Force, other organizations. These organizations -- and you see them represented on this panel. These organizations depend, on the one hand, on broad, multi-stakeholder participation for their legitimacy. But significantly they depend on individuals, both as participants, but also on leaders. And I think if you look at the history of the Internet, what you see is a surprisingly small number of individuals who have had extraordinary leadership roles. I spent many years working with Tim Burners-Lee, just one example, the founders of the Internet Engineering Task Force are another example. There are people in this room who've been involved in organizations like this.

And I guess I would just make a plug to all of you out there. Don't

underestimate the vital importance of individual leadership, both in running these organizations but also in participating. Because we are still at a point, notwithstanding the global scale of the Internet, where I think individuals actually can have huge impact.

So I want to turn to Leslie Harris. And hope that you'll help us with two questions. Number one, the question of how to make the multi-stakeholder process truly multi-stakeholder. We've heard -- some of the organizations that we've heard about do tilt a little bit in the commercial direction, and there are good reasons for that. But I think that we all recognize, going forward, that for a multi-stakeholder policy process to have legitimacy and also sustainability it's going to have to really reflect a broad range of interest, both commercial and non-commercial.

And second, the question that I think Joe also wants to come back to is the question of how do you get this to work, globally. So, two simple questions for you.

MS. HARRIS: Two simple questions. I think it's interesting you asked the first one, because I had written down during the other presentations, what do we really mean by multi-stakeholder? Because rarely does that mean true and equal participation and decision-making by the non-corporate participants, unless the stakeholders are government and participants.

And I think I've got some lessons learned from GNI. I don't think I have anything remotely resembling final answers.

So let me talk a moment about the Global Network Initiative, which I'll refer to as GNI, which is a multi-stakeholder initiative that's intended to help companies in the Internet and technology sector chart an accountable path forward when they are faced with demands from countries around the world to take actions that may violate free speech or privacy rights of users; and sort of the iconic cases of, you know, China requiring censorship on the part of its online providers or countries without fair process

seeking information to unmask a blogger or a user from the companies who may be holding that information, things that may actually happen in democratic countries where a rule of law process has set some norms about when and how that should occur, but that increasingly happens, particularly in non-democratic countries. But these rules apply to all, where companies are faced with the possibility that they are engaging in something that could aid and abet a violation of human rights.

The center of the initiative is a set of principles and guidelines that were developed over several years of consultation. My years of living very dangerously among a very diverse set of stakeholders. And that included Internet and telecommunications companies in the room at the time, social investors, like the Calvert Group, for example. A wide set of NGOs, human rights organizations, free expression organizations, Internet civil liberties advocacy groups like my own, and very prominent academics and academic institutions.

And the commitments -- and I think this is significant -- in the principles and guidelines are backed up by a real accountability regime. That includes company reporting and some independent assessment, and the ability of outsiders to file complaints.

There are three companies -- and we are calling them today high-road companies, so I will -- Google, Microsoft, and Yahoo! -- who stayed in the room for the whole process and are now implementing the guidelines. And we'll be doing a first reporting back to GNI and we'll allow in some independent third parties in the next year.

GNI is now an independent nonprofit. It has a director and a board of directors. And I think that what is significant for purposes of this question of multi-stakeholder is there is equal participation in governance of GNI between the industry and non-industry participants. We're certainly beginning to develop a global brand. There's a

lot of interest from governments, enormous interest from other third parties around the world, even from the United Nations, and a lot of ongoing discussion with other companies.

So, what do we learn from this process? My lessons learned have to be very, very preliminary. Ernie talked about the evolution of these kinds of models, and if you are now a full, stood-up human being we have recently crawled out of the -- onto the land for the first time. (Laughter) So -- yeah, out of the muck. We're very -- but I think lesson one that applies across the board, if you're going to do this seriously, is that not everybody in the room starts with the same knowledge base with respect to technology. So, if we're talking about Internet's issues and solutions, or access to the same facts. And people in the room do not have the same resources to participate.

So, GNI spent the time -- we've gotten a lot of criticism. Why did this thing take so long to get stood up? One reason is that we spent an entire year in what was in some way a pre-negotiation dialogue on the technology, how it worked, who collect data, who had access, how it operated in a system like the United States, so that people could get if not on a level playing field at least a playing field where you could rationally participate. So, I think, you know, we talk a lot about multi-stakeholder. You have to take this into account, and there are going to be some things like the ITF or CDT is one of the few NGO participants that there are, you know -- there are some kinds of processes where the price of entry is deep technical knowledge. But it all can't be.

Lesson two is, technologists and companies don't know everything. And I think one of the things that happened over time in this process was that people opened the space to understand that the non-company stakeholders had their own facts and knowledge, and that that informed and enriched the process. They introduced the companies to human rights norms and thinking. They brought significant experience with

earlier processes and models for corporate social responsibility initiative. Some fit, some didn't, but they also knew where the crash and burns had been in the past.

There were rich bodies of work on the concept of human rights risk assessment. We know privacy assessment, we didn't know this. They understood the human rights landscape in a different way, and I think that those two bodies of knowledge being brought together created a richer, more credible product that reflected, at the end of day, expertise and knowledge and facts from all sides. This is really hard to do.

The other lesson, which certainly precedes the nice lesson about the product at the end of the day -- real multi-stakeholder initiatives bring people into the room for very different reasons. So the agendas, you cannot ignore how far apart, why people are in the room. And there were people in the room with one goal. We're holding companies accountable. There were people in the room -- we really got to, you know -- this is really complicated. We've got to bring all these people together so we can learn and share best practices. There were people who wanted to create a formal initiative, there were people who did not. And if you're going to stand up something like this, you can't gloss over that. You can't just say we're doing it this way. And I think that when consumer groups participated principally industry initiatives, it's very easy to say, here's the goal, give us your input and you're at the table. But your other agendas can easily get swept away.

So, lesson four, because of lesson three, is if you're going to do this you have to be prepared, all stakeholders, to lean very far forward in order to get to yes. And I will say that everybody in that room -- and certainly the companies who, at the end of the day, are the ones in the spotlight here, leaned very far forward to get to yes. And I think that is an opportunity, but I think if you're going to be serious about what it takes to do this, you've got to understand that.

The last one that I'll mention is, that leaning forward in compromising has its plus and it has a potential minus, because everybody who is not in the room does not have the two- or three-year benefit of very rich dialogue. And very hard-fought compromise, and they will very quickly start throwing things at you. And from the human rights perspective, those human rights groups that chose never to listen and hear continue to be, perhaps, where they were years ago, which is companies should just leave these places or you should always store your data out of the country or all kinds of binary, this is the answer.

And companies not in the room are faced with looking at agreements on some very hard things, like accountability, that they were not privy to the dialogue. And that leaves, I think, a very complicated question is, do you rent a stadium to try to reach this kind of consensus? It was hard enough to do what we did, and some companies at the end of the day did not stay in the process. And I think that that's a very -- an interesting question for GNI going forward.

Here's the open question that puts it sort of in the context of what we're talking to. What ultimately will be the right role for government, whether it's a role with respect to GNI specifically, or more about norm setting in this space? The United States Government does not have a formal role in GNI. They have been very, very supportive. Not everybody's happy about that, but they have, as have some European countries.

There was a rationale for not having the government at the room at the time. You know, number one, after we've seen from sort of efforts to right those deep regulatory rules that Mark was talking about, we had proposals like GOFA in Congress that tried to create sort of black letter rules in a situation where those who understand something about this space understand it's not black/white, yes/no. And it just doesn't lend itself to those kind of binary solutions. So that suggested to us the private

governance solution.

We were also concerned that it would be viewed as United States initiative, when our aim is to cede a global standard of care around the world. And -- but to be fair, I think there's a question about what that's going to be sustainable over time.

It is not clear that this should be entirely outsourced. You know, if you were to ask me where I am on the line of government action to totally private action, when rights are involved, government has a role. Secondly, companies step up and do the right thing when government is either setting norms or threatening norms. And, you know, even BITAG, which I support -- the CDT intends to participate -- certainly got legs from the net neutrality debate, even though we may not all have come out on the same place on that.

And so I think there's still a question about whether truly voluntary initiatives that may have some carrots, but very few sticks, like GNI, will be able to attract new companies or whether, at the end of the day, some degree of high-level norm setting -- and, again, enforcement -- some kind of more co-regulatory model may emerge.

MR. WEITZNER: Leslie, thanks very much. I have a zillion questions for the panel, but actually think I want to open the floor up to questions from the audience.

And I think we have a microphone. So, please.

Could you stand up? Thanks?

MS. KING: Sorry. Robin King with USAID. I am actually wondering if -- there's a couple pieces to this question. And I'm not representing the free speech group, but I am wondering about a couple of the stakeholder groups that -- for instance, in processing the porn sites, the child porn sites, for instance. In my experience, there have been legitimate organizations who have been victimized by hackers and others who may have gotten caught up in those types of, you know, stings or caught.

So my two questions are really about due diligence in verifying all that information. And due process for those who are victimized but are doing legitimate business. A lot of us have heard about hacking sites. The CIA, for instance was at once hacked. And also small businesses who may not have the resources to put in place some of the regulatory or compliance things that may come up in these norm setting groups. So, just my question is about --

MR. WEITZNER: Thanks. And I think we'll take maybe two more questions so that we can think of them together. This gentleman right here, and then over on the side.

MR. ALTMAN: I'm Fred Altman. And I wanted to go back to something that Mark Cooper differentiated between the policy setting and the enforcement. And I'm wondering what are the differences that organizations that set policy, the companies and the government regulators need to do in terms of responding to consumers terms of enforcement versus policy.

MR. WEITZNER: So the question about different roles for enforcement functions and policy setting in these organizations, please.

MR. MEEHAN: My name is Josh Meehan with Romulus Group, a consultancy firm. Mr. Allen, your group is obviously phenomenal, but I feel like one of the reasons it's very obviously phenomenal is that it does incredible work on an issue that people can widely agree really needs to be handled.

But the model that you're talking about, in particular, of aggregating data through kind of clearinghouse and bringing stakeholders together. I have a question about that kind of model. Because if you apply that to, let's say, something as maybe more controversial, less agreed upon, let's say abortion issues or maybe something related to terrorism or what have you, I just wonder, so what are some of the legal issues



that you've seen just kind of come up when you're dealing with this kind of aggregation of data? And do you think that the model really transfer that well, just generally to all issues? Or do you really feel that there needs to be sort of a social agreement beyond a legal one that you're dealing with something that has to be handled directly?

Thank you.

MR. WEITZNER: Okay. So those are, I think, four important sets of issues. The question about how transparency and due process works in these multi-stakeholder environments, especially when there's some enforcement or action-taking component.

Questions about whether everyone will have the resources necessary to comply with the rules that come out of this process. The question about how enforcement functions will work, and then I think really underneath the last question is a question about where do we get the principles that drive the multi-stakeholder agreements? Do we expect those to arise out of the multi-stakeholder process or, as was suggested on the previous panel, is there a role, perhaps, for government in establishing some broad guiding principles?

Who would like to start? Ernie, go ahead.

MR. ALLEN: Shall I? Okay. Let me start with the last and then pick up a little bit of the first.

Absolutely. I mean, the issue will define how replicable the model is. And I think what we have learned from the process, what these companies have said to us is, there needs to be some central clearinghouse that provides them expertise or information that allows them -- because most companies are not going to have major enforcement staffs. Are not going to have the capability to do it themselves. So, social values, clearly, need to be an element of that.

But I think there are lots of other issues where it is replicable. To the point about due process, at least from our perspective there are two levels to this. The first priority in all of this is law enforcement. Law enforcement investigation. So, that's where the primary due process issue resides. And, of course, law enforcement -- whether it's federal, state, local, or international -- has got to do the necessary investigative approach to make sure that the person who is being pursued is, in fact, responsible.

As it relates to our voluntary effort with electronic service providers, the premise is not that someone is being held criminally or otherwise legally responsible for what they're doing. The question is, is the presence of that URL, of that image -- Microsoft and Google are helping us develop even more surgical tools that enable us to focus on very specific images instead of larger URL content. But the whole premise is, is the presence of this content on that system a violation of their terms of use? Companies remove content all the time. The due process is really between the person whose content is removed and the ISP or the content hoster or whatever.

So all we're doing is alerting them to apparent content that meets the worst of the worst criteria with no instructions other than, they take that and use it in the most appropriate way within their company, whether they're scrubbing their systems and making sure they're not hosting it or whether they're blocking it from coming up in search results. So I think they're really two separate pieces.

MR. WEITZNER: Thanks. I want to turn to Peter and then Leslie on the question of source of principles. Peter, you talked about a variety of different voluntary multi-stakeholder environments. What's your view about where the guiding principles ought to come from?

MR. SWIRE: So, that's more general than I have any answer for.

Where do guiding principles come from in life is a very broad question. (Laughter) But I'll put that into a manageable regulatory frame in a second.

I think that in the privacy debates, where I spend a lot of time, there's been a lot of talk over the years about self-regulation. And a great deal of confusion around that term. And so, one part of self-regulation is where do the rules come from, or the principles? You can think of that as sort of the legislative function, where do the rules come from. And in a lot of privacy policies, the companies have written their own rules or whatever.

But then there's another thing, you might think of it as the enforcement or judicial function is, how do you enforce against it? And there there's been a government that steps in. For instance, the Federal Trade Commission. There's also the press and the advocates who step in, and this was in the last panel talking about how crowd sourcing can help us find out violations. And so the self-regulation and privacy has been where the rules come from for companies' practices. Self-regulation has not been in the United States at the level of enforcement. So, that's just a confusion people often have.

Let me just also make a quick question on the small business. Over time in the privacy debates we didn't used to have a threshold for when the small businesses kicked in. And that meant, for instance, selling customers lists is prohibited under a lot of privacy proposals. But does that mean the Girl Scout cookie list can't go to next year's Girl Scouts? And if we thought that you had to give a privacy policy out when you sold Girl Scout cookies that would pretty much end the privacy efforts in America, right? Because that's just over-regulation.

So, the new versions of bills that -- the Rush bill that's out this year, and other -- have thresholds. Once you have a certain number of records in, then you kick in. But the Girl Scouts and the people that cut lawns in a neighborhood and the small businesses don't have to. So you have to find ways to make it workable for people who,

incidentally, are in the space. But if you're big enough to really be having an impact, that's when the rules kick in.

MR. WEITZNER: Peter, thanks. Leslie.

Ms. HARRIS: So, to the extent I understand your very broad question, I - you know, I think there isn't one answer about where the rules come from. I mean, if you're talking about an issue that there is either societal agreement or there is societal obligation -- the government has an obligation to protect our rights, it has an obligation to keep us safe. Then I think you have to tilt towards processes that inform the government solution, or processes that lead to government norms with some kind of an enforcement.

So, for example. You know, in the privacy space, no. I don't think companies get to just make up those rules. But I think that what they've been doing in self-regulation, what the consumer community believes is the correct answer, can together create the set of norms to guide the space. And I think that's where you can think more about co-regulation. You know, you create a baseline for what people need to do, you encourage the sectors to engage and go further in some kinds of outside processes.

But I do think it depends on the subject matter. And I think it's correct that a process like NICMIC's does depend on there being an absolute societal view on the content. I mean, people keep bringing up NICMIC as, well, can't we do a NICMIC for copyright? That's the discussion right now. Can't we do a NICMIC for a variety of other things? And you always run into the question of either, there is no societal agreement or -- as the woman in the back of the room said -- you're dealing in an environment with a subject matter which you don't know it when you see it, and therefore there are some First Amendment and other kinds of implications.

So, I'm a great admirer of this model. It's how to extend it and where to

extend it is more difficult than I think I would like it to be.

MR. WEITZNER: So, Joe, being near the front end of the creation of a new institution, leave us with some reflections about what do you think got the various players to the table and what do you think is going to constitute success such that it looks good both from the perspective of those who are sitting around the table and from the public at large, who I think your intent is to feel a sense of confidence and trust in the process going forward.

MR. WAZ: Right. Well, the debate about the preserving an open Internet has been around for the better part of a decade now, in one form or another. Probably longer. But the FCC actually did give us an articulation of principles of an open Internet arguably on two prior occasions.

One was Michael Powell's speech, I think at Silicon Flatirons in 2004, where he stated a four freedoms formulation for maintaining an open Internet. And then the following year, the FCC articulated principles of an open Internet as well. So we've been operating for five or six years now under some notion of what the appropriate principles are, not as a function of legislation, not as a function of a formal FCC rulemaking proceeding, but sort of the acquired wisdom articulated by the FCC in a policy statement.

Our interest in giving more shape to these principles predates the current effort by the FCC to turn these principles into rules. And in fact, the whole conversation about BITAG dates back to well before the notion that the FCC might even consider rules. If there are rules put in place, as the FCC is now proposing to do sometime this month, I think BITAG will play an important complimentary role to that effort and hopefully will be a place where issues can be discussed and resolved and put in the context of Internet norms before they become a matter of complaint.

If those rules were not put into place, I think BITAG would still move forward with the same goal, which is to provide assurance that stakeholders can get together and, under the principles of the FCC previously articulated, be able to try to address questions and resolve issues before they become the basis of complaints.

Danny, I'd like to tap one other point. We talked about the issues of resources a couple of times. I think that's important to come back to, because especially for the NGOs, like Leslie's organization and others. In the context of BITAG, we've had that conversation. And the question of how -- we're now asking people to bring engineers to the table. Not every advocacy group has an engineer. There need to be perhaps more engineers than there are today, perhaps some more economists, and perhaps a few less folks like me, law graduates.

But I think it's going to be important for those funders of the NGOs to take seriously the need for NGOs to have the capacity and have the capability --

MR. HARRIS: Your lips to God's ears. We've been trying for years to get them to understand that it -- for NGOs to participate seriously. I mean, we can't be the only one on the table because Rabbi Cooper's daughter works for us.

MR. WEITZNER: Joe, thanks. I think that's a terrific note to end on. We're going to transition to the next panel. Mike, I'm sorry. But you could probably ask the same question to the next panel is my next guess. Because you're very clever.

But let me just close by observing that I think that what we've learned is that there's a lot of learning here about how to make these multi-stakeholder processes work. That people have put a lot of time and effort into them, that we understand a number of the piece parts that are necessary.

I think one thing that we understood just from the last round of discussion and the last round of questions is that guiding principles are really important. In some

cases we have those guiding principles because they're just understood in our society. We protect children, as an example. In some cases, those principles arise out of the collective expertise of these organizations. That's the case in some of the techno organizations, where -- and in the case of Ernie's organization, where the knowledge that's contained in these multi-stakeholder organizations really helps society articulate just what its values actually are. And that's a very valuable contribution to make.

And in some places, there's a role for government in helping to crystallize that awareness and articulating a set of principles, as in the case of the net neutrality principles or perhaps some others that will be coming down the pike.

So, join me in thanking this panel and we look forward to the next panel.

(Applause)

\* \* \* \* \*

MR. WEST: Okay, our next panel is going to deal with user education and net citizenship, how the government can encourage adherence to best practices. And we are very pleased to welcome Christine Varney here with us at Brookings. Christine will be moderating this panel. Christine, as you know, is the assistant attorney general for the Antitrust Division of the Department of Justice. Christine.

MS. VARNEY: Thank you so much, and it's a delight to be here and be back talking about a subject I used to know a lot about. Let me start by emphasizing, pointing out disclaiming any professional responsibility today. I'm here solely in a personal capacity. I am not here as a representative of the Department of Justice or the administration, so I'm just here as somebody who used to work on these issues and has

followed them with keen interest.

Now, the people who you can hold accountable for what they say today include Alan Davidson, who is the head of U.S. Public Policy for Google. Prior to joining Google, Alan was the associate director for the Center for Democracy and Technology, and an adjunct professor at Georgetown University and a computer scientist.

Also joining us is Gary Epstein. He's the managing director and general counsel of the Aspen Institute International Digital Economy Accords Idea Project. Before joining the Idea Project, Gary was the founder and global chair of the Communications and Practice Group at Latham & Watkins. He has also served as a team leader of the Economics International Trade Team on President Obama's transition, executive vice president of SkyTerra Communications and the digital television coordinator and chief of the Common Carrier Bureau at the FCC.

Pamela Passman is here. She is Microsoft's vice president and deputy general counsel, Global Corporate and Regulatory Affairs. Prior to serving in that position from October 1996 till April of 2002, Pamela was the associate general counsel responsible for Microsoft's law and corporate affairs groups in Japan, South Korea, Taiwan, People's Republic of China, and Hong Kong. Prior to joining Microsoft, Pamela was at Covington & Burling.

Also with us is Rey Ramsey. He is the president and chief executive officer of TechNet, the bipartisan political network of chief executive officers and senior executives of leading U.S. Technology Company. Rey was previously CEO of One Economy Corporation, president and chief operating officer of the Enterprise Foundation, an officer to the cabinets of two governors of Oregon as the state's director of Housing and Community Services, as well as practicing law.

So welcome to everybody. What we thought we would do at the panel is



just start with some questions which we hope will provoke a conversation among ourselves, and then turn it open to questions from all of you. So what I want to start with, given the title of our panel is: Do voluntary best practices work? For example, in unchartered or rapidly changing areas such a privacy, net neutrality, can we and should we rely on best practices, or do we need legislation and regulation? And why don't all of you take a crack at that, and then we'll dive deep.

Go ahead, Alan.

MR. DAVIDSON: Now, I'm not being --

MS. VARNEY: Easy one to start.

MR. DAVIDSON: Here we go, a simple question. First of all, let me say thank you for the organizers for putting together such a great set of presentations today. It's really tremendous, and this is a set of issues we really do need to make progress on, so congratulations and thanks

I think a starting point might be sort of are there good examples out there, best practices or user education initiatives that have had traction? And I'll just speak a little, give a couple of the examples from Google's perspective. We've heard, for example, about GNI and BITAG, but even looking a little more granularly at some of the products that we've created, so Google owns YouTube. YouTube's a very popular video-sharing site. Every minute, 35 hours of video is uploaded on YouTube. That's our latest statistic, so, you know, since our introductions began, you know, almost, you know, several days' worth of video has been uploaded upon YouTube.

It's very, very difficult to imagine how, one, how a government or even a single, you know, entity could go out and prescreen all that content, try to police it, but what we have put in place instead of community standards that our community is very aware of and a set of flagging mechanisms where they can flag content that's

inappropriate. And what we've seen, and this was -- it was not known that this would work when we began, but what we've seen is actually this is a mechanism that can work very well, so, for example, we don't allow pornography on the YouTube. It's a violation of our community standards. It's not illegal, but it's a violation of our community standards. And actually we've gotten, I think, pretty good -- not perfect, but pretty good -- at catching it because what happens is when you have literally hundreds of millions of people watching videos and they know that the standards are in place, they will flag content that they know violates those standards. And then, very quickly, we can intervene and take content down.

I think there are a lot of examples of innovation in the space where the Internet itself allows users not just to be educated, but empowered. That's a good example. Another example is the work that we've been doing on Internet advertising where recently Google got involved in trying to do what we call intraspace advertising, targeting based on interest. And we were able to do something new which was to place on every ad that we put up a icon where people can find more information. We created an ads preference manager that lets people select their -- see what we know about them and try to tweak it themselves.

I'm not saying that these are perfect initiatives but I do think they are examples of how we can, if we educate users, we can empower them in some of these areas.

There will be areas where we do want and need the bully pulpit or the backstop of government, but anyway my point I think is that there's a tremendous amount of innovation, and we can do more on transparency and empowering people as a start.

MS. VARNEY: Well, Pamela, I mean, the bully pulpit of government can

mean lots of things. It can mean people pounding the table and say you need to do this, it can mean legislation, it can mean regulation. What do "best practices" mean to you and when do they work and when don't they work? And when you want the government involved, in what way?

MS. PASSMAN: Great question. I mean, this morning's been all about, you know, when is regulation the right appropriate vehicle versus self-regulation, and I think the answer is yes, you know.

MR. DAVIDSON: Right.

MS. PASSMAN: There are appropriate times for both. You know, Microsoft has advocated for comprehensive privacy legislation since 2005, and for a variety of reasons, I mean, the speed of technological change is the debates that are happening of various levels of society, that hasn't happened yet. But, nonetheless, we have felt very strongly that we needed to put some stakes in the ground in terms of the way we developed our products, the way we conducted our business, and, over time, you know, those have become best industry practices, and we have very much felt a responsibility to provide that kind of information to the industry or the ecosystem, if you will.

An example is the Microsoft security development life cycle, which is a mandatory way that all of our product development, all of our architectural or engineers develop our products to improve the security of software code. It's been very successful for us, and we have made this information broadly available to software developers around the world.

Another example is our commitment to privacy by design, something that the FCC is very much focused on as well as the European Commission. Here again, we are committed to designing, developing our products with privacy front and center, and all

the processes that happen around that as a company need to take that into account.

We just released Kinect Xbox 360 which takes -- this is fabulous, it's my first gaming experience, actually -- it takes facial and body pictures as you are doing these fabulous different kinds of games. And we recognized early on in the development of that product that we needed to design privacy from the ground up. We are sharing all this privacy by design know-how with others in the industry.

Again, two examples of best practices -- I think we've heard a number this morning -- the Global Network Initiative, as Alan also mentioned and Leslie very articulately laid out for us; you know, the work that Arnie does is just phenomenal creating best practices that are shared around the world and creating incentives for companies to work together, to develop technological solutions in the hopes of advancing the response to very, very challenging situation.

MS. VARNEY: Well, Gary, that's, you know, from the American perspective all very interesting because when you look particularly at jurisdictions like Europe, I don't see a lot of best practices; I see a lot of regulation legislation. So government is clearly taking a different role in other parts of the world.

How do you see that? How do the roles that government can take both in the U.S. and internationally, and how can government be effective without sort of the heavy hand that we all, you know, fear could retard innovation, but yet maybe put the safeguards in place that some feel are lacking?

MR. EPSTEIN: Thank you, Christine, another easy question. I get --

MS. VARNEY: I'm known for this.

MR. EPSTEIN: I did want to note, as you listed my title, I somehow feel that the length of the title is inversely proportional to the staff and the power that I've had

over the years in my various jobs.

I can answer that question by maybe describing just for a second this project which I'm involved in now which is the Aspen Institute Idea Project. And what this is, is I learned an awful lot today from these really excellent speakers both on multi-stakeholder, governance, and on the aspect of setting principles. What we're trying to do is we have 19 -- and I think I'm going to coin a new term, "a high-road elephant" in the consortium right now -- 19 of the major companies. And we have important NGOs, including Leslie Harris' organization, and that is an important part of the venture that we're trying to go forward.

And what we're trying to do right now is develop these principles that you're talking about, Christine, in order to see whether from a U.S. perspective we can reach some kind of accommodation or some sort of consensus. And we have the full support of the U.S. Government who has been extremely helpful. Both members of this panel have are also -- have been extremely helpful in getting us to the point where we are now.

And so we recognize that in order to have the appropriate nonregulatory role that you're talking about, we probably have to achieve consensus here in the U.S. first, but we can't be U.S.-centric. And so the idea is to take these concepts and these principles, see if over the next six months to a year we can actually develop them in the open Internet area and then see if we can reach consensus overseas.

I will listen with great interest to Ambassador Kornbluh's advice and speak and direction on how to make this perhaps an easier sell in Europe than we think it may be.

MS. VARNEY: Interesting. Well, in all of this, right, what's the responsibility of the NetiZon? How do we, as citizens, get our government to do what we

think they need to do or -- it sounds like the companies are being pretty responsive, what's the role of the NetiZons?

MR. EPSTEIN: Other than prayer? Let me -- I want to take a slight take on that question because I think it's important to sort of look at this as an ecosystem and that includes government, the public interest groups, the nonprofits, the companies. And then when you get to the citizen, the challenge that I think we still have is how do we create a process and a means for citizens to actually participate? And so before you can answer the question of the responsibility of the NetiZon, the question is how do we ensure that people have both the capacity and the means to be able to participate in the ecosystem?

So some can and do and many others don't. I mean, you do have some net tools out there, you know, the way Alan was describing that Google makes available the people where the citizen herself can actually just engage and be involved and take advantage of things. But in some cases we have so much more to do in terms of making it possible for people to participate, so I think it's a difficult question. When you say "responsibility," well, yeah, there is some responsibility to yourself to your family, but a lot of people don't have the ability to participate.

I mean, look at broadband and how we spend money, how we try to get people involved in broadband. The big issue is still adoption. We still have a huge percentage of the population that even when they're exposed to broadband don't adopt broadband. So they're not even in the system; they're not even in the ecosystem.

So I think we've got some of those things to look at before we can say that they have responsibilities.

MS. VARNEY: Well, let's drill down a little and it looks like two areas that are very topical and talk about best practices, privacy best practices, net neutrality. Is

that enough or do we need something more? You know, the FCC has articulated principles for net neutrality for quite a long time now, and the Federal Trade Commission and others have articulated principles for privacy on the Internet for quite a long time now.

And what's wrong? Why are we having this conversation if best practices work? Alan?

MR. DAVIDSON: I think I'd start by saying that the pace of change is incredible, and I think we have to recognize that that's part of the difficult here, and it's part of the challenge that Rey talks about, right? I mean, you know, it's very if -- you know, we recognize it's bewildering out there. So, you know, I don't -- I think a lot of people have said it's not -- it's not an either/or, it's exactly what Pamela was saying: We have actually joined this great initiative that Microsoft I think was one of the pioneers of saying that there ought to be baseline privacy protections because even if you have wonderful actors out there like Google and Microsoft, you will still need probably some baseline protections to deal with others who may not be consumer facing and who may have different businesses that actually lead them in directions that we think are not appropriate.

So it's not to say it's an either/or; it really is an event. But I think the tricky part of this is, as I say, the pace of change and why I think we are continuing to have this conversation that, Christine, before the panel that you were saying we've actually been having for quite awhile --

MS. VARNEY: That does need released.

MR. DAVIDSON: -- that you've been part of for quite awhile, and it's, you know, if we were having this conversation 12 years ago, Google wouldn't exist.

MS. VARNEY: Undoubtedly.

MR. DAVIDSON: You know, six years ago Mark Zuckerberg was in college and most people didn't know what Twitter was or that Twitter even existed. YouTube didn't exist, you know, so I think, you know, we have to -- with the mobile revolution, Internet, you know, Internet through mobility, then really within a reality. So if you look at the pace of change, I think we are going to continue to have this conversation because it is a struggle, and I think that fear in some ways, and I think is that we have to be very careful about when we bring government in, in the regulatory capacity. It's not that it shouldn't be there, we know we need it in some places; it's just a question of how do we do it carefully.

MS. VARNEY: Well, and, Pamela, that's the reason that in the '90s we didn't regulate privacy on the Internet because things were moving so fast and we didn't want to retard innovation and we wanted to be careful. So the idea was, okay, let's articulate best practices and see where things evolve and have a light hand.

And some would say, well, you know, time's up. It's now time to move beyond that.

MS. PASSMAN: Well, I think the process that the Federal Trade Commission, and you could say the same of the FCC that have used in the past year and a half, two years to bring the various stakeholders together, and then they, you know, both agencies took broad views of stakeholders. So I mean I commend both processes. I think they have been very strong processes to bring in different groups.

And now industry, you know, needs to respond, and needs to be very thoughtful in how they respond. You know, the threat of regulation is quite powerful.

MS. VARNEY: Mm-hmm.

MS. PASSMAN: It is still an incredibly dynamic industry, you know. The EU data protection directive is under review, and, you know, lots of activity right now. But



a new directive would not be in place for five years.

MS. VARNEY: Mm-hmm.

MS. PASSMAN: So today we're discussing how to amend change the EU data directive, and, you know, who knows what the environment's going to be like in five years?

So I think -- again, I commend the process here and, you know, the next 6 to 12 months are going to be very interesting.

MS. VARNEY: Gary, how about on net neutrality? Same deal? Go slow. Things are evolving, we don't know what's going to happen, let industry lead? Or is it time to put some regulations in place?

MR. EPSTEIN: Actually, I think it's a fascinating contrast. I won't tell you where I was 12 years ago or 18 years ago; probably in the same place I was now. But the net neutrality debate really is subject to the same issue of rapid technology change making old style regulation obsolete. But it's not because the issues are so new: The issues have been around for 20 or 30 or more years, you know. Net neutrality in some sense is a descendent of the computer 2 and computer 2 and computer 3 inquiries of the FCC, and those were, as panels earlier today have talked about in a fascinating series of discussions, is the old command and control notice of proposed rulemaking, comment, and you should have seen the rules that came out of computer 2 and computer 3. Many of you did.

I was the computer chief who has to implement computer 2 at the FCC, and that was a full-time job for the entire agency and in the end turned out not to be a particularly productive job because even then the pace of change was overshadowing what was happening.

And so the discussions we had earlier today I think were extremely

instructive and I commend Danny Weitzner's speech, testimony on the Hill the other day, where he laid out the construct of the three kinds of regulation that governments could be involved in,

One of them was the old commands and control type regulation which I think by consensus today it has its values, and I wonder whether the FTC will adopt that in its most recent proceeding. But it doesn't really seem to work well anymore. And the other two is the government is a convener construct and then we wound up having major discussions about a multi-stakeholder process coming as a result of that, and then the general policies with after-the-fact regulation, and that's a long way of saying I think that's where we're going with the net neutrality type regulation. Like technology involves; regulatory policy should evolve also and we know that the detailed rules of the computer inquiries in all likelihood are just not going to work in this new environment.

This seems a very interesting and creative and really worth trying compromise for government involvement in rapidly changing technology.

MS. VARNEY: How are you, Rey? You've got a view on that, and then we'll got to you, Alan?

MR. RAMSEY: Yeah, let me say this about net neutrality. You know, if, when Julius Genackowski, the chairman of the FCC, laid out three basic ways that he wanted to operate the FCC, and I would say this: That if that is adhered to, we will handle this situation really well. He said we want to be transparent, we want to be open, and we want to be data-driven. And if those -- those are three very significant values, and if we adhere to those values, we'll have good policy.

And, as I've said to him personally, one of the most important things is, in policymaking, is a level of humility. If we're humble, we'll recognize that change is rapid, that we can't resolve and solve every issue. And what we need to do is have a

framework and that framework needs to be elastic and evolve over a period of time while we remain transparent, while we're open. And in terms of openness and transparency, it's not only waiting for the sophisticated to come to you but it's also taking it on the road to seek other ideas, to seek other issues and other points of view.

So if we had that balance with the humility, I think we'll get there. I think this framework that was articulated last Wednesday is a good start. We'll see how it evolves over the next couple of weeks, but I think it's a good start.

MS. VARNEY: Alan, do you want to come in on that?

MR. DAVIDSON: Actually, I was -- actually, I wanted to say something a little bit broader than --

MS. VARNEY: Okay.

MR. DAVIDSON: -- about net neutrality. I'm happy to talk about that, too. And I think Google's made no secret of its belief that there are parts of the network infrastructure that need to have government involvement, and we expect in the spectrum space, and we saw it in the narrow band world. And we expect in some ways that there ought to be some baseline rules, and there's been good progress in that area.

But I think, what I was going to say sort of to our broader discussion, that, you know, we're sort of treating the involvement of government as kind of a binary thing, right?

MS. VARNEY: Mm-hmm.

MR. RAMSEY: You know, that it's sort of either -- this is what exactly Pamela was saying, you know, regulate or not regulate, yes, right, you know. I mean, you're going to need -- but if it's really a continuum -- and there are a lot of things that we've seen that government can do. Government has a role as a convener, the bully pulpit of government. I think what you've seen, something in the last panel was saying,

you know, some of the -- a lot of progress has happened at the end of the barrel of a gun maybe, but also I think that also there has been a bully pulpit that the Federal Trade Commission has used very well here in the U.S. to convene these -- and other parts of the U.S. Government. The Department of Commerce is doing this now with the series of inquiries, to convene people in workshops, to get people talking about these issues.

It's happening internationally. Like the Internet Governance War on this property is a very good example of places where we can pull people together in multi-stakeholder groups and get them to talk about this. Government has a role itself as a modeler of those practices, right? Security standards, IPv6 adoption, we can look at lots of places where we need government and where government can use its purchasing power and model these best practices itself.

Government is a regulator of last resort in some cases, or maybe in some cases it will need to be the decider of some issues where it's about government behavior. So we need government engagement on issues like how we're going to deal with censorship and free expression online. How are we going to deal with surveillance rules? These are inherently government functions, and we need government out there protecting the model of a free and open Internet as well. So there is a continuum engagement.

MS. VARNEY: Pamela, do you want to come in on that?

MS. PASSMAN: We also need government reaching out to its counterparts around the world. I mean, the issue of harmonization of these rules, it's great to have the U.S. ambassador to the OECD there to close the session. It is absolutely critical, you know, as we see more and more of our services going to the cloud, and I know many others in our industry are very focused on the cross-border transfer of data and the fact that, you know, many -- multiple governments are trying to

regulate the same data. So we need, certainly, the U.S. Government to be a leader in interacting with its counterparts.

And I don't know that we can wait five years or ten years. You know, the technology and the interest of small, medium, large enterprises' governments moving to the cloud. They're getting ahead, if you will. And so we really need to get the whole legal framework in place for that.

MS. VARNEY: So let me speculate that there is probably complete agreement on this panel that government can and should be a convener. They should model their own best practices. They should enforce existing law fairly and reasonably. They should make sure the international playing field is level.

Now let me ask the audience, is that it? Does everybody agree that government should stop there and not go the next step? And it's a binary question, it's a yes or no question. Should government now in these areas that we've identified -- for example, start with privacy -- should government legislate privacy in the U.S. in the way -- let's pick an example, for the example the way the FTC has proposed -- do you all think that's a good thing? If you agree with that, raise your hand. Okay, not many.

Okay, how about network neutrality? Hands off? Leave it alone, let the companies continue to deliver and build out broadband and do what they need to do? Or do you agree it is time for the government to step in and legislate in order to protect the openness of the Internet? Raise your hand high so we can see it. Okay.

SPEAKER: (inaudible)

MS. VARNEY: Well, that's not binary. It's hard to -- so I'm taking off everything short of legislation and seeing where people stand.

Well, you're hearing a lot about what we're thinking. What are your questions? Do you have some questions for us? Yes, David? And please identify

yourself when you stand up.

MR. JOHNSON: David Johnson, (inaudible). Earlier (inaudible) and we also have heard about steps that those elephants can take to use their technical power to simply take off from that sites that infringe widely-shared norms or, in some cases, not so, you know, some controversial electrical property norms.

What I'm not hearing is anything about whether the relationship between the elephants and their constituents can change institutionally. Should we be talking about new ways to give users the opportunity to have a voice in what the large technical companies actually adopt by way of policy? Or is it just a matter of whatever their terms of service said?

MS. VARNEY: And how would you give them a voice, David, before you pass off the --

MR. JOHNSON: Well, I think there are a few examples of ways to pose questions and get a sense for the online community. It's never going to be a representative democracy, and it's going to be a small number of users participating. But that's an area where we haven't done much innovating, so since this is about net citizens, I'd like to ask if we can innovate in that range.

MS. VARNEY: Okay, Rey, do you want to kick it off? Then we can ask the elephants.

SPEAKER: We always think of ourselves more as puppy dogs, actually, maybe a Labrador, but.

SPEAKER: Please, high-end (inaudible).

MS. VARNEY: Okay, go ahead.

MR. RAMSEY: Basically, what you were bringing up, David, was exactly what I was alluding to, sort of looking for some of these models. And there are some

small things, you know, that are out there in terms of, you know, listening to consumers, listening, you know, to customers. And so I think this is room for a lot of innovation, and it's something that at TechNet we're very interested in from a policy perspective. And what we're looking at doing is setting up an apparatus so we can hear from a wider array of individuals.

I've been saying that if you had to bring together 5,000 really smart thinkers, you know, onto a subject matter, we're still doing it in a 20th century way and making phone calls and convening people. So it's something that we're working on, and you'll see something in the coming year on that where we want to open up more of Washington in terms of the debate on issues like net neutrality and other issues.

But I've been living that for the past 10 months that I've been in this job sort of seeing that it goes slow and we need to open that up now. The companies, I'm sure, have got some other things they're looking at, but I'm looking at broader policy issues.

MS. VARNEY: Well, it's interesting when I throw it over to the companies because suppose you get 5,000 incredibly sophisticated NetiZons who say, you know what, Google, Microsoft? Absolutely you should not under any circumstances ever track any individuals. I think you got obligations to your shareholders, and these 5,000 people might not be your shareholders.

So how do you reconcile the competing interests of multiple stakeholders, including your shareholders, including the NetiZons, including consumers?

SPEAKER: Great question. Great question.

MS. VARNEY: No, you got -- and maybe Gary wants to take it first.

MS. PASSMAN: It's a great question, and companies have to be more transparent. I mean, just in the environment that we live in and, you know, every day you

-- it comes closer to home. You just have to be more transparent, you have to be in a dialogue, and we are in a dialogue. I mean, consumers, our users are telling us exactly what they think. The challengers are a very diverse group of use. They're, you know, the recognition of the roll that your advertising does play on the Internet, you know, content is free, but, you know, there it is for a reason.

So I think, you know, our view is we must give consumers choice so that they can make an informed choice so there's a huge amount of education that goes into that, but we have to understand that users have very different perspectives, the technology has to provide choice, and there has to be significant dialogue with our users.

MS. VARNEY: Well, maybe we should put a question up to the 5,000 NetiZon panel to say would you like to continue to receive all your content for free or would you like to not get tracked and have to pay for all your content? A binary question.

MR. DAVIDSON: So I would say -- first of all, I would, like, in a lawyerly way reject the premise of the question. No, I'm not sure that we believe that there is this strong tension between these interests. I think a lot of us --

MS. VARNEY: It was a hypothetical, Alan.

MR. DAVIDSON: Oh, then I'm doubly rejecting it. I don't answer hypotheticals in Washington. But that we -- you know, I think we've all taken this kind of long view that actually, a lot of us in the interest of taking this long view, that actually doing what's right for the user community and the Internet communities ultimately are going to be what's good for our businesses.

We've actually had this experience on this very issue. We started this thing. I mentioned this thing called the "Ads Preference Manager," that Google launched which lets people actually go and see, think like on if you see an ad like Google, click on it, or you can search for "Ads Preference Manager" on a Google privacy, and it'll take you



this page. But if you're logged in as a -- it'll take your cookie, and it will show you what we associate with that cookie, what interests, right, and will let you change those.

First of all, you can opt out of it so that we won't -- this cookie won't be operational, or you can change your preferences so it'll show you we think you're a car enthusiast and you like knitting. You can change those things, right.

So say I actually don't like knitting, but I really do like interior design. So what we have found when people go and visit this, we thought people were just going to go all opt out, right? I mean, that's what the advocates said. That's what we actually thought. And what we have found is that the vast majority of people when they come and visit this, I don't know if they're fascinated, but they end up tweaking. They don't opt out. What they do is they change their preferences. That's a win-win.

Now we had, you know, people are getting ads that they would like to see. It makes our system more effective, so I'm not sure that we have the right model here, that this is a -- that there is this tension. But I think what's more important is that there is this possibility, right. The reason we think user education is so important is because we actually think there's a possibility to give users more control.

So David Johnson asked this very question. He wrote the great article with David Post years ago, late '90s, about Internet governance, right, and the possibility that you could create different rule spaces. If you gave people information, they could make choices, and if you gave them the possibility of choosing between different places where they could exist, they would vote with their feet.

I think we need to keep trying to do that. That is the thing, it's not just the old version of government regulation or nothing; it's like can we create new stuff. We're going to have regulation where we need it, but we also try and create these new things, the BITAGs, the IEPFs, the IGFs of the world, the global convening so that we can try

and take the advantage of what the Internet offers us. It's all to Deke Allen, but thank you, David.

MS. VARNEY: I think there are a couple more questions. Go ahead, sir. Get your microphone and tell us who you are. The microphone's coming. Thank you.

MR. KERN: Charlie Kern. I spent 30 years on Capitol Hill with the Senate Judiciary Committee and the House Judiciary Committee with Senator Hart and many others.

I used to write speeches when I was up there -- I'm now retired -- in which I said when the tide of regulation goes down the beach, the sand of anti-enforcement must appear. And I'm wondering whether there's any role for antitrust enforcement in trying to shape some of these policy choices

MS. VARNEY: Well, thank you for that question. I'll -- (Laughter) -- we've got a lot of staff people here. Anybody want to answer that? You know, I'm going to confine myself today to let the current experts speak on this. We're trying very hard at the Antitrust Division to fulfill our mission vigorously, and we'll continue to do so.

But let me talk to the experts about their panel. I'm not sure that -- I think that what we're talking about today for self-regulation and user education probably is not an antitrust issue. You know, we're charged with protecting the nation's markets from undue concentration and illegal otherwise agreements that could tend to restrain trade. So I don't see that as a role that I'm currently in.

Go ahead.

MR. BALKAM: Stephen Balkam with the Family Online Safety Institute. In an earlier panel, Phil Weiser threw out the issue of cyberbully, for instance --

MS. VARNEY: Right.

MR. BALKAM: -- as a curious or difficult case to have to handle. It's not

as straightforward as what Ernie Allen has to deal with at NICMIC, for instance.

The *New York Times* ran a very long article yesterday on its front cover trying to work it out. Isn't this a perfect example of where we need education, digital citizenship learning, or do we need what we're seeing is the states, not federal government but the states now crafting laws to deal with sensational, particularly suicides coming out of cyberbullying.

MS. VARNEY: Right. Where is that?

MR. BALKAM: We're not even talking about an international issue here, we're talking about state-by-state coming up with their own mosaic.

MS. VARNEY: Right.

MR. BALKAM: So how are we going to deal with cyberbullying in all of this?

MS. VARNEY: Who wants to take that? Go ahead, Rey.

MR. RAMSEY: One aspect of this, and not addressing the state law part of it, is the human behavioral side of it and sort of the training and the digital literacy and the support that a lot of people need.

One of the programs that I've been involved with, Comcast is actually a large funder of it, it's called Digital Connectors. And it's a training program for young people, and this is one of the areas where they're getting training in, so -- and they get lots of hours of training and they do community service going out training others. They're working in schools. So as we have a regulatory and legal framework that will likely grow because of the sensationalism of this, we've got to put as much energy on the behavioral norms and other things, and the training and to show young people, hey, it's not cool to do that and those sorts of things.

And I think we underinvest in some of those things, you know,

sometimes, but that's part of what I'm saying, the means and capacity to participate. There are a lot of people who say, like, oh, everybody does that. I thought everybody does that. Well, they don't. And so I think we need all of that.

MS. VARNEY: But, Gary, is that an area that we should be looking at legislation? I mean they've keyed up a pretty defined area, cyberbullying, terrible consequences. Should it be regulated, and should it be regulated at the state and local or federal level? And then I'll go to you, Pamela.

MR. EPSTEIN: Well, I, you know, I don't have first-hand experience like Microsoft and Google do in this, but I do think that before I would jump to 50 different state laws or political issues that were involved here I really do think that a heavy grounding in education and in bringing the issue to light and in publicity, and in those kinds of non-legislative solutions, we should attempt to put it on the table first.

You know, other -- I think here rushing to legislation may be problem as heinous and as difficult as the problem is.

MS. VARNEY: Pamela?

MS. PASSMAN: There are some very interesting conversation in your organization is quite engaged in really talking to school authorities and the school systems. I mean that they are very overburdened as it is today, but we have a history of health education, drug abuse education that happens at different points in time in the educational curriculum. And to the extent that we can begin to integrate some of these issues into the curriculum, getting more of the Parent-Teacher Associations involved, this has got to be a very grassroots, if you will, approach.

MS. VARNEY: Go ahead, Alan.

MR. DAVIDSON: Again, I think it's also an area where, you know, the pace of change is also incredible. And that's, of course, part of what is so difficult and I'd

say, as a parent if a nine-year-old who has not yet discovered social networking but I'm told she may any moment, that it is, it's going to be a difficult environment. But again, if we were trying to put a law in place about this, if we'd done it a couple of years ago, we would have missed social networking, you know.

It's not even obvious that those are the areas. I shouldn't pick on that because if your conference was great presentations about what's happening, it's about global, it's about texting, and so it's not obvious that this lends itself to an immediate legislative solution. I think it's exactly what the other panelists have said: We've got a giant challenge in terms of getting a generation of much more media-literate, and getting their parents much more up to speed on the tools out there. So it's a hard one.

MS. VARNEY: Yes, go ahead.

MR. HOWARD: Alex Howard, O'Reilly Media. One of the themes that's come out of this morning is transparency and multi-stakeholders, and certainly the Justice Department itself is a stakeholder in this in the sense that we know that you're working with elephants here and elsewhere to get information about the same citizens online and to follow us as well as part of our prosecutions, or certainly a great interest in other parts of the government are as well, well beyond Justice.

So with respect to the premise of this how can government encourage adherence to best practices, how will the Justice Department be more transparent about the request it's making regarding mobile technology and regarding tracking on social networks and other ways that citizens exist online?

MS. VARNEY: Well, as I said when I started, I'm not here on behalf of the Department of Justice today. I'm here in a personal capacity, but I am the assistant attorney general for Antitrust, and I can tell you in the Antitrust Division we try to be completely transparent so that everything we undertake goes up on our website as it

happens, and you get access to all of our filings.

We are very open on any of our matters to meet with interested parties, to talk to parties about what we're thinking about, but that's not the point of your question, and you're not going to get me today because I'm not here on that.

MR. DAVIDSON: Maybe I can help.

MS. VARNEY: So Alan can answer.

MR. DAVIDSON: I'll jump in for a second and just say that I think -- well, first of all, yes, and, by the way, the Trust has an excellent privacy policy, and I totally recommend it to you if you're looking for a good model. And but -- and very transparent - - but I think in this area we need more transparency for sure.

I'll just say something that we've recently tried to do, do the launch of this tool called our *Government Transparency Report*. You can go find it on your favorite search engine. I'm sure it comes up even on Bing if you search for Google in government transparency, and it -- but what we did is we've tried to, in aggregate, post all of the number of requests for information about our users from each country. It's very revealing. And if you -- and we've also posted the aggregate number of requests to remove information from our services that we've gotten from each country.

And I think if we can get more people to put that kind of information up, it would be very helpful because I think it gives you a good indicator of what's going on out there and what's happening relatively among countries. I think this is an area where we need our government to help, which is to be more transparent itself but also encourage others to show what's really going on out there.

And so I have to say these requests shouldn't happen. A lot of them are about real law enforcement investigations or real illegal content that needs to be dealt with, but there needs to be a conversation and -- this is an area where it honestly needs

to be a conversation between governments, companies, as much as we love the GNI and those kind of multi-stakeholder things, we can't do this. This is really about governments talking to each other.

MS. VARNEY: We have time for one last question, and this gentleman's been patiently waiting back here.

MR. MIA: Josh Mia, Romulus Group. So my question is about I guess how best standards, best practices really works when you're dealing with sort of irrevocable choices and irrevocable errors that happen on the Net. So best practices is something to me that evolves every time and says, okay, so these are things that we should try to adhere to, principally. But before that happens there are certain choices.

For example, a few months ago when Facebook CEO Mark Zuckerberg actually states that the future of the net is that people don't really want privacy that much. And then you have all these issues where people's information is just out there. You can't really take that back, but you can get past and try and get, you know, better practices. And at the same time, you also have younger people who would make choices on the Internet, maybe they would put their own information up there, and you can maybe tell them some of the precautions and what not, but it would seem that the role for government, historically, would say that we protect you against long-term bad decisions. So we have social security because we presume you may not safe properly.

MS. VARNEY: For the moment.

MR. MIA: Stuff like that. And so I guess my question is for anybody on the panel, and especially I guess for Google and Microsoft, like --

SPEAKER: I have the Kinect.

MR. MIA: I do. It's very ridiculous in the pictures, and I don't know what the privacy policy is but nothing against the Kinect, but it's that kind of thing where they

are just things that happen, and people either they can't know or just don't know and they'll make decisions. Maybe you could fix them, but it's out there.

So is there a role for law there? Thanks.

MS. VARNEY: One of you who goes on Microsoft? Pam?

MS. PASSMAN: I mean, that's why I talked about privacy by design. I mean, you need to build these concepts into the development of the product. Yes, bad things happen. People are imperfect and technology is imperfect, but, you know, how you build a product, the processes that you put around it, the compliance as a company that you invest into and ensure that you are meeting your commitments, all of these things, you know, are important, incredibly valuable.

But at the end of the day, you know, bad things do happen, and your ability to mitigate them, to respond to them, to be transparent about them are all very critical.

MS. VARNEY: Alan?

MR. DAVIDSON: Yes, I agree. We are not going to stop people from doing dumb things on the Internet, I'm afraid. And, you know, somewhere out there (inaudible) citizens talk that, you know, somewhere out there right now is an 18-year-old who 30 years from now will be President of the United States. And that person is probably out there right now posting silly pictures, sending silly text messages, putting things up on a blog or a Facebook page that might be embarrassing or we might view as embarrassing. And I think we are in the -- we have to recognize this is a moving target, right. The hope is, of course, that 30 years from now that we'll view this as very differently, right. But we all posted something dumb in our, you know, Facebook page back in the 2010, right?

So, and, you know, our notions of privacy and other things, our other



norms will change. But -- and it's going to be very hard to figure out how, so it's very hard for us to figure out how to stop people from doing those things, especially in this moving-target environment. What we can do is exactly what we were just talking about which is to try to give people as much information as possible, give them the tools to control things as much as we can, take advantage of the power that the Internet offers to give that control, try and keep the Internet this open place that allows that.

It's a huge challenge. It's a huge user education challenge, but otherwise we won't be able to stop the tide of people doing things, silly things on line.

MS. VARNEY: Well, in that spirit of the title of our panel, user education how can the government help, I'm from the government. I'm here to help, and I'll give you a parting piece of advice.

During this holiday season when I was driving home from work the other day, I got a text from my brother who has a seven-year-old and a nine-year-old, and it was the end of the day. It was for me 7:30, 8:00 at night, and the text from my brother said, hey, what did you get the kids for Christmas? And I assumed he was out Christmas shopping and didn't want to get the same thing.

I immediately pulled over because I would never text and drive, and I texted him a very long list because I love my niece and nephew -- the ambassador knows them, the one you had dinner with. I immediately texted back a long list of these wonderful things that I had gotten for my niece and nephew.

The text was from my niece on her father's phone.  
Be careful as you approach the holiday season if you are a gift-giver. Be very careful.

Thank you, all. (Applause)

\* \* \* \* \*

## P R O C E E D I N G S

MR. FRIEDMAN: As we come to the close of the event it's nice to have Ambassador Kornbluh here to remind us that the Internet is, in fact, not just American, and lots of other people use it as well.

With just a very brief introduction, Karen has done an incredible amount of work on both making policy and also framing it intellectually. She has worked for then Senator Obama as his policy director. She was at the FCC in a number of different offices, internationally and domestically. She's had fellowships at the Center for American Progress and the New America Foundation, and she's written extensively on broadband deployment international investment produce. So, Ambassador?

AMBASSADOR KORNBLUH: Thank you. Thank you, Allan. Good morning.

I just have -- before I get started, I just wanted to compliment and commend all the administration folks who are putting together this examination. I think there's this cadre of tech experts right now in the administration whose work is incredible important and really under --

SPEAKER: I can't hear you.

AMBASSADOR KORNBLUH: You can't hear me. Can you hear me now? Is that better?

SPEAKER: Move closer.

AMBASSADOR KORNBLUH: Can you hear me now?

SPEAKER: That's better.

AMBASSADOR KORNBLUH: All right. So I was just complimenting and commending the tech experts in the U.S. Government right now because I think the work

that they're doing is really making good on President Obama's promise to create a smart government. And I think what they're doing is also helping to lay this foundation he's talked about for a better economy that's going to have growth in the future. I think a lot of the work that they're doing, those of us who are sort of wonky can see the value of it in the work space. But I think in the much bigger space of remaking, reinventing government and also creating a foundation for a strong economy, I think it's undersung.

So I'm going to talk about the international component of what we've been talking about a little bit, and then I'd love to have a discussion. As you remember, the Clinton Administration framework for global electronic commerce listed as Number 5 of its five key principles, electronic commerce over the Internet should be facilitated on a global basis.

Today the U.S. has an enormous stake in the global, single, open Internet first in growth and jobs. I just want to talk about this for a second. The most recent OECD *IT Outlook*, which came out on Friday -- this is the 2010 outlook -- show that of the top 250 IT firms, 75 are U.S. companies. The U.S. has 8 of the top 10 Internet firms, 7 of the top 10 in software, 6 of the top 10 in IT services, and 4 of the top 10 in equipment and systems. And I could go on. This sector is obviously huge. Its already recovering from the recession, and the market should grow by three or four percent just in 2010 alone.

The number of jobs in the IT sector alone grew by 26 percent in the U.S. from 1998 to 2008, 4 times faster than the U.S. employment rate as a whole. But that's sort of understating the case because the Internet is, as you know, and as has been discussed here, not just another industry. It's a platform, it's a technology enabler. As such, it can drive productivity growth in jobs.

So I remember when I was working at the FCC in the mid-'90s, there

was a lot of talk about how companies had been buying computers, but it wasn't showing up in the productivity statistics when economists said computers are everywhere except in the productivity data. But then once the Internet took off that completely changed. And starting in the late '90s you saw productivity which had been stuck start to climb. You saw jobs grow, you saw incomes go up, and that was because these computers were connected and so suddenly people were doing things more efficiently.

According to the OECD again, the impact of the Internet on productivity may be greater than that of other so-called technology enablers, including electricity and the internal combustion engine. It lowers barriers to starting and operating a small business, improves quality and quantity of information available at a far lower cost.

The Internet also facilitates trade according to the OECD because it allows the expansion, aggregation, and globalization of markets as well as the customization of goods and services, and this is also important to innovation. There's recent research that shows that firms that are exporting are more likely to innovate.

So in addition to the economics stakes, we've heard a lot today about the social stakes in the Internet, but the U.S. also has a political stake in the Internet, and I'm sure a lot of you have been following the work that the State Department has been doing, incredible work, to support those who would use the Internet to empower themselves politically and to exercise values such as freedom of speech. So, internationally, we have a huge stake in getting this thing right.

And the same what I'd like to make is that the success of this global Internet and the benefits we've been able to achieve is no accident. Just as we set in place a framework in the mid-'90s for the domestic evolution of the Internet, this framework was adopted internationally as well. It had an international component. The U.S. principles were echoed by Europe which took a similar though distinct approach to

the EU's electronic commerce directive.

The U.S. and the EU developed a privacy safe harbor for data transfers. This allows data to be transferred to the U.S. as long as the company doing the transferring is regulated by the FTC or the Department of Transportation, and the company follows a less regulatory version of the EU data protection principles.

The OECD socialized this approach. It had a 1998 auto administrative which called for an industry-led approach. It created a framework through its privacy and e-commerce guidelines -- which I'll talk about in a minute -- of high-level principles, transparency, cautions against practices that create unreasonable risks of harm to consumers, and these helped e-commerce to expand by balancing protections as freedom of commerce.

The general thrust of these policy strategies was away from placing the onus and policing content on the entities that sit on top of the physical infrastructure, the Internet intermediaries, and the result was this ecosystem that we've been talking about that fostered openness, decentralization, and created a trust environment. It meant the Internet could be a conduit for freedom of information, and it gave rise to the participative web. It means everyone could be a speaker, a producer, and a consumer of information goods or services. So that's the good news.

The bad news is, Number 3, that today the need for a single Internet is increasing, increasing data flows, cloud computing, new applications. But the consensus that was agreed upon internationally is fraying on a whole number of fronts.

And I'll just take through them because I think a lot of you are really familiar with this and it's been in the liturgy before, so there's regulatory divergence, different rules and privacy, data retention, and law enforcement access in the liability intermediaries. And, as you know in Italy, three Google executives were thrown in jail

because of a video posting.

German regulators issued a resolution disapproving of the US-EU safe harbor and asking the EU to reconsider it. China has censored content of L-1 Chinese Internet portals, and on occasion ordered that access to major U.S. e-commerce platforms be blocks. So there's regulatory divergence.

There is also actual property infringement issues that have been rising up. German courts have ordered monitoring by Internet marketplaces after a counterfeit good has been found to be sold in their state. Neely Croyce, the EU Commission for the Digital Agenda, recently said that European copyright rules are out of date and require a major overhaul because they have given "a more prominent role to intermediaries than to artists," a censorship. As you all know, it's been in the news a lot.

Secretary Clinton has said that we in the U.S. stand for a single Internet where all of humanity has equal access to knowledge and ideas, and we recognize that the world's information infrastructure will become what we and others make of it when in the last few years we've seen unfortunate spikes and threats to the free flow of information. And then a lack of consensus, as you've heard about how U.S. companies should respond.

And then there are also a bunch of new fora that are coming into play, a number of entities in putting the ITU that are looking at the Internet and considering frameworks to regulate it. So the bottom line of all this is that this consensus that we had is fraying, and we run the risk that the Internet will be atomized, and that you'll wind up with state-by-state regulations, and that the growth of entirely legitimate Internet-related businesses will be chilled as intermediaries attempt to comply with the most stringent of the new rules.

And so I think what a number of people are talking about now is how can

we start to have a discussion to rebuild a consensus for an Internet that is on the one hand both safe, curbs illegal behavior, but is also predictable and safeguards freedom of expression and lawful commerce.

So how do we have that discussion, and I would like to submit to you that the OECD is not a bad place to have it. So what is the OECD? It's the Organization for Economic Cooperation and Development. It has 33 member countries. It has partnerships with the developing world with what's called "enhanced engagement countries" which are basically the big emerging economies, and it's not where you go if you want hard lots. It's not where you go if you want a treaty that's legally binding, that you can enforce with sanctions, but it is a place where regulators come to share best practices, develop soft lot agreements such as principles, guidelines, and conventions. It's starting to sound a little bit like that new governance model that we were talking about.

In the case of the Internet, the OECD is the home of the 10-year-old OECD e-commerce guidelines and the 30-year-old OECD privacy guidelines. It's also the source of the definitive data on the Internet, the broadband rankings which are being released today, actually; *The IT Outlook*, which I said, it was just released on Friday. The OECD has done extensive work on security, and then maybe most important, the OECD is a forum for multi-stakeholder dialogue.

So it works with volunteer groups and Internet intermediaries, child protection privacy and e-commerce. It has business in labor advisory groups that have a formal role, and, as I said, the nonmembers have a direct way to participate. And the OECD happens to be working on a study of Internet intermediaries that comes out of its last ministerial and so I was told to look at the role of Internet intermediaries.

So the Obama Administration has proposed working with other OECD

members to organize a high-level meeting at the OECD in June on the Internet economy generating innovation and growth, and we think this is going to happen, and we want you all to participate. The objective is really to just reinvigorate a conversation among OECD members as well as other key players about how to build trust and while also safeguarding these qualities that we've talked about.

And really, what's as important as the actual summit itself is what leads up to it and how much involvement there is. And then what we want to do at the summit is adopt some principles that are a little bit apple pie, but cutting enough, sharp enough to actually be meaningful in terms of the kinds of concerns that countries should weigh in terms of creating some kind of interoperability framework.

So the meeting would underscore the importance of broadband and Internet intermediaries to the Internet economy so that we could remind ourselves and the broader public not to take this medium for granted

Second, it would review the shared experiences of countries in promotion of broadband access and deployment, and agree to improve our metrics on that front.

Third, it would review the success of the existing framework and some of the new realities.

And fourth, it would come to some kind of political agreement, as I said, on principles to maximize the benefits of the Internet and create these interoperable regulatory schemes.

The specifics are still being discussed so I can't really tell you what they are yet, and I want you all to help us figure out what they are. But some of the things we'd want to see in the final principles are just what we've been talking about today. So empowering media institutions, due process, transparency, and education, government



as a convener and facilitator of best practice, government articulating principles and technology-neutral performance standards to be realized by the private sector rather than rigid commands and control regulations, creating rules that are predictable and understandable, finding ways to build trust in the Internet, and safeguarding freedom of expression.

So this is what we're planning to do there. Obviously, this is only one piece of a big hole that there's got to be a key role for the U.S. Trade Representative's Office in terms of looking at trade issues. In the EU, Bill Kennard, who's the U.S. ambassador there, is engaged in a dialogue with Europeans. Leslie Harris just talked about GNI, so there's the Internet. The IGF so there's a lot that's going on. This is one piece of the puzzle, but I would just hope that we could take a look at this idea of having a June summit where some of the like-minded countries that have been involved in building this consensus can come together and restate what a new consensus is on some principles going forward. And I hope that you'll all be involved in helping us think through what we want to get out of that, and then come to Paris in June and participate,

So I look forward to having a discussion right now.

MR. FRIEDMAN: So thank you, Karen. Ambassador, you highlighted as the cross of these issues there's sort of a different types of organizational models. You have direct state-to-state bilateral discussions, safe harbor. We have the official government body organizations, ITU and various UN approaches as well as to some extent the OECD. And then we have the multi-stakeholder organizations of ICANN and IGF, et cetera.

How well do you see them playing together, and what do you think are some of the main hurdles that we need to avoid as all of these different groups work together on Internet governance issues?

AMBASSADOR KORNBLUH: Gosh, that's a neat question. I mean I guess one of the things that we're hoping to do with these principles is, you know, state that the more the better in terms of entities that are involved, but that there should be some basic approaches that you take that you make this trade-off really clearly, and that principles that -- I mean, that regulations that governments come up with are clear and transparent, and there's due process and that they work together so that the company doing business can do business worldwide, and a consumer who wants to purchase can purchase easily on the Internet and at work speak easily on the Internet.

And so I think that's the main goal. I think the main goal is sort of the output and making sure that everybody can participate. But I don't think we want in any way limit the entities that are involved.

MR. FRIEDMAN: All right, we'll turn it over to questions. The one in the front there.

MR. SMITH: Bruce Smith, George Mason and Brookings. I think there's a certain boosterism for high-tech here, certain high-tech snobbery which we should really call attention to. Having experience now with undergraduates a little bit, the Internet has not fostered learning, it's perverse, and it's the enemy of learning because students seem to have a mentality that if they can't grasp it in six minutes, they don't pay any attention to it. They've diverted into narrow casting, to use that term of Cass Sunstein: Instead of broadcasting, look at common themes.

Is there a kind of -- and when we talk about here the need for a digital infrastructure and for broadband policy, this is Clinton era technology policy, industrial policy. Why do we need a broadband policy? Why don't we allow sort of the economy to develop without attempting to force it in one direction? You don't really promote jobs through high tech?

MR. FRIEDMAN: Sure you do. Let me --

MR. SMITH: There's only -- there's 5 percent of jobs in this country are high tech.

AMBASSADOR KORNBLUH: So what I was trying to say, and I guess I didn't -- maybe I said it too fast, I'm from New York so I speak quickly. But the Internet is a technology enabler. It's a platform for innovation and growth, so not only is it, you know, a huge industry globally where the U.S. has a big advantage at least for now, but also it allows small businesses to sell broadly. It allows, you know, it allows me to buy books easily from Amazon.

Before I moved to Paris, and I thought at the last minute, oh, my god, I have to get my kids a ping pong table, I went on Craigslist and, you know, was able to buy it. So it's really -- it's a nice place to -- for consumers. It's for efficiency, it's a great place for small businesses, it's as great place for innovation and, you know, what role did the government have in making sure that electricity got to rural communities and making sure that the railroad got across the country? Highways. I mean, it's -- broadband is equivalent.

And that data is there to show it. I mean I'll send you a copy of the *OECD IT Outlook*. The data is pretty compelling.

MR. SMITH: I'll send you some of my work.

AMBASSADOR KORNBLUH: All right, I'll read it.

SPEAKER: I just had a quick question in regard to a kind of composition that the -- of the conference. I think that the global aspect of this is incredibly important, and better we're focusing on it.

We have two kind of large players, one on the state side which is China, and another -- others on the side of industry, including (inaudible). And I just wondered

why the OECD is a place which could attract the interests that these parties represent as a forum for the type of work (inaudible).

AMBASSADOR KORNBLUH: I'm sorry, but I didn't quite understand what you were saying. Why not bring the industry in?

SPEAKER: Well, industry I think was the (inaudible) about industry.

AMBASSADOR KORNBLUH: Yeah.

SPEAKER: I'm really thinking more about China at this point.

AMBASSADOR KORNBLUH: Oh, I see. Well, that's actually one of the things that's interesting to me about this is that so China's not a member of the OECD but it has a partnership with the OECD. So one of the things that can happen with the summit is that we can engage them in a conversation, but they quite frankly don't have veto power over what comes out, that the countries that are part of the consensus-based decision-making process at the OECD are the membership of the OECD.

So we, to the extent that the countries of the OECD are the more developed countries -- and I mean that loosely -- I mean, Chile just became a member, so it's countries that really have adopted a market-based, rules-based economy. To the extent that they can agree on some principles that make sense, they can talk to China, talk to these other countries, try go get them involved. And at the end of the day I think it's a benefit that it's driven by those countries because we still, you know, for all our differences with Europe and elsewhere, we still basically have a similar approach.

What would be nice is at the end of the day we've got a set of principles out of this that says, no, this is -- this is important for your growth, this is important for your growth, this is important for innovation, let's educate you about why this approach makes sense, and also let's clear up any misconceptions about what it is that a free market economy does when it

approaches the Internet, and I think that would be very useful in this debate.

We're not going -- the OECD is a purely economic forum, so we're not going to talk about it from a human rights point of view. We're going to talk about it from the innovation, economic. The freedom of expression is important to that. If you have freedom of expression, that allows the development of the Internet the way it's been developed. So I think really, really clear to state what kind of approach countries that have been successful have taken and will take.

SPEAKER: You're not really including critical issues and human rights issues in the discussion at all, although those are extremely important such as China.

AMBASSADOR KORNBLUH: Yeah, I mean, to the extent -- I mean, freedom of expression is right at the heart of it, so I wouldn't say we're not including it. But the slant, the focus is more of the economic. And I think that's -- you know, there are the human rights conversations going on, and those are incredibly important. But I think to have this other conversation that says, look, in your self-interest if you want to grow an economy, if you want innovation, you know, you have to be a part of this world that says there's a single open Internet, and this is what it looks like and this is why it's been successful. And you start to vulcanize that and cut it up, it's just not going to be the same thing.

MR. FRIEDMAN: It's also interesting to note, by the way, that sometimes economics actually works quite well for promoting human rights. So, for example, efforts to legalize cryptography was, I think ultimately one to the benefit of the human rights community but for economic interests to create e-commerce.

MR. HOWARD: Alex Howard, O'Reilly Media. With respect to photography, of course, many companies are asking for access now to the servers, whether it's Blough Graham or any other company to get around that precise issue, right,

and so there does seem to be a tension to entering an economic market in terms of exceeding to the individual government's demands for the company itself, right?

And I suppose the question is with regards to vulcanizing policy, how are you seeing companies amend their terms of service or their standards to enter certain markets? Others are certainly, if you know in this news, Google made some real tough choices in China. To what extent are other technology companies changing the way that they operate, which in turn will have an impact upon the development of the Internet?

AMBASSADOR KORNBLUH: Yeah, I think that's a real interesting question. I don't know if our principals will get into that, and that will be part of, I think, the discussion we have, you know, in the U.S. and then with other countries about whether it should get into that kind of thing. But certainly, I think that's part of what GNI is looking at.

I think that Aspen Project is going to be looking at that kind of thing, what kind of norms should we expect from U.S. companies, you know, and other companies about what to do when those kinds of requests come in, what kind of procedures do you face? I think there's a lot of real interesting work and very needed work being done in this, that area. And companies are saying, you know, we need that.

MR. FRIEDMAN: In the back.

SPEAKER: Thank you. Ambassador, my question is a bit of a follow-up on the lady in the front and also perhaps a bit to the gentleman who just spoke. And it regards a dialogue that's been happening within the Council of Europe regarding the role of Internet service providers, the Council having defined them as critical to a participatory democracy in the 21st century, therefore the Council suggests that ISPs may be the best ones to assure fundamental and human rights.

So I'd like to ask from an economic perspective, from your organization's

perspective, any thoughts that you may have on that. Thank you.

AMBASSADOR KORNBLUH: Sure. First I should qualify and explain that I work for the U.S. Government, so I'm the U.S. representative to the OECD, so the OECD is not my organization, it's all of our organization. We pay a lot of the bills over there.

I think -- I mean, and that -- and part of where this -- you know, I think it's hard to sort of separate off human rights from the economics because, as I said, free expression is just so important to why the Internet works from all perspectives.

And, as I said, the U.S. has a big economic stake in the Internet, but it also has a political stake, and that's a sort of enlightened stake because, you know, what we get out of the Internet and what we want to protect is good for the rest of the world as well.

So the OECD has been doing these studies on the Internet intermediaries coming out of its sole (phonetic) ministerial. And part of what it's laying out is why Internet readers are so important and the role they play. And most people are not aware of them, you know, that this separation that there's this layered structure to the Internet with the fiscal layer and then the Internet intermediaries in the middle and the incredibly important role that they play.

And we think that maybe there's a role for education about the role of these different players, different layers, and that maybe that will help inform the regulation that's going on. Maybe if people start to understand that they could be killing the goose that lays the golden egg, not only economically, but in terms of free expression.

MR. FRIEDMAN: I guess I can dive in again and ask you, sort of prognosticating to the future, are there issues that you think we're going to hear a lot more about coming up that you think, you know, institutions and other organizations start

spending a little bit more time researching both, and so that we can shape up for the coming debates?

AMBASSADOR KORNBLUH: Yeah. Well, I just think that the issue that came up before about -- and that Danny raised in his testimony about, you know, what's the role of government, and I'm feeling that a little bit in this international realm. What's -- you know, where should you -- I just -- let me just tell you the story.

So I met with people from the American steel industry last week, and they said we'd love coming to the OECD. We have these wonderful conversations. We've talked to the Chinese.

And I said, well, do the talks lead anywhere? You know, how good is it to talk? Do you see change in the action?

And they said, well, yeah. I mean, we've educated them. They're -- they are talking differently. They do understand some of our concerns more. They do -- you know, we've educated them about how to use scrap metal, so they're more energy-efficient, and how they have to do this and that.

But then as it came out, what they've also done is the steel workers have filed a complaint, a 301 complaint with USTR, and that sort of helps the conversations if you have that threat hanging out in the background of a possible 301 violation and possible sanctions.

Now, you know, will the U.S. really put sanctions on Chinese to steel imports? You know, your guess is as good as mine, but having that threat out there certainly helps conversations. And so in this space, too, you know, I think these principles are great, a great way to educate us and to have a discussion and, hopefully, they'll create -- one of the things the OECD is really good at is creating, naming and



shaming. So it just had this big success with tax havens where it put out a blacklist of countries that weren't sharing tax information. And just the shaming factor of it made it made a whole bunch of countries -- so I think there have been 600 tax treaties signed since a year and a half ago when they put out this list. It's amazing.

So there is a big advantage to countries signing up to principles and then being held to account for them. But how much do you need behind that in terms of some kind of threat of trade violations or, you know, other kinds of a stick, as people were talking about at the end? How do you get citizens and stakeholders involved in holding people accountable?

So I think there's a lot of fascinating work to be done in that area that we've heard about all day. And, you know, I think this is a great conversation that's been started, and thank you to Brookings for hosting it and to the administration folks who organized it. I think it's been tremendous.

MR. FRIEDMAN: And I think on that note I would like to thank again all of the panelists and all of you for spending the morning with us. (Applause)

\* \* \* \* \*

CERTIFICATE OF NOTARY PUBLIC

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

/s/Carleton J. Anderson, III

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2012