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 adversarials 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 aps 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.

* * * * *