THE BROOKINGS INSTITUTION

COMBATING BOTNETS: STRENGTHENING CYBERSECURITY THROUGH STAKEHOLDER COORDINATION

Washington, D.C.
Friday, December 16, 2011

PARTICIPANTS:

Introduction and Moderator:

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

Presenters:

ARI SCHWARTZ
Senior Advisor to the Secretary on Technology Policy
Member of the Internet Policy Task Force
U.S. Department of Commerce

BRUCE McCONNELL
Counselor to the National Protection and Programs Directorate Deputy Under Secretary
U.S. Department of Homeland Security

SAMEER BHALOTRA
Deputy Cybersecurity Coordinator, National Safety Staff
The White House

Panelists:

MICHAEL KAISER
Executive Director
National Cyber Security Alliance

BRENT ROWE
Senior Economist
RTI International

JAMIE BARNETT
Chief of the Commission's Public Safety and Homeland Security Bureau
Federal Communications Commission

* * * * *

P R O C E E D I N G S

MR. FRIEDMAN: So if I could ask everyone to have a seat, particularly if you're supposed to be seated on the dais. So I want to thank you all for coming out on Friday afternoon. I know there's a lot of exciting things going on both on the Hill and in the Christmas party department, so thank you for spending the afternoon with us.

We've a very interesting event today and before I get to it, just a brief announcement. We have our new hash tag should you decide to Tweet or otherwise engage in all sorts of fun things, or start your own botnet and you want to build it into the code.

So this is a fascinating topic from Brookings' perspective. The challenge of how we think about cybersecurity in general and botnets in particular, has been clearly of great interest to many in the past few years and even for many of us even long than that. And it really does require some novel thinking not just on the technology side, but in terms of the governance and organization side.

And there are couple of key themes in this challenge of how do we look at botnets and how do we engage the ISPs or the intermediaries. So, first, we may need a new form of governments or new types of organizations that allow both the government to look after citizens and create good public policy, but at the same time be able to work with industry, not as a target to be regulated, that is something that is trying to, you know, change a profit margin, but essentially create good public policy in a way that is sustainable and cooperative.

Second, there is the theme of approaching information security as an economic problem, and it is very gratifying to see that this is a dominant trend recently, that we must understand this from a market perspective. My colleague at Brookings, Noah Shactman, has looked at ISPs as sort of a inefficient choke point or an intervention

point where we can look at this problem. But we also need to look at from the perspective of, you know, the incentives of the company and the perspective of the user incentives. So botnets might be seen as one of the core externalities where my failure to secure myself makes everyone else less worse off.

But, at the same time, how do we map that back into sort of a marginal cost approach for the user? The challenge of understanding botnets from a governance perspective ties into other efforts that are going on in the broader cybersecurity space. How do we think about liability in terms of assigning responsibility? Information sharing is something that everyone is in favor of, but as soon as you start saying, well, what information, with whom, and how, you start to get into some fun problems to solve that are closely tied with this.

And then finally, the challenge of sort of user responsibility campaigns. How do we increase user awareness to see this as something like pubic health, or public safety, or other areas where we see this? This is not just a technical problem, this is a social problem.

It touches on some of the more thornier aspects that are going on, so there are privacy concerns -- or not. This may, according to some people, touch on the rather controversial topic of network neutrality. And, in fact, some might argue that, listen, as long as we're intervening in ISPs for the public good, can we do something about this infringing content as well? But that's going on at the other end of Mass. Ave. right now.

So, to discuss this, we're going to focus on the Department of Commerce and the Department of Homeland Security's approach, which is, listen, we think that this problem is solvable. This is something that we can actually get out hands around. This is a challenge of an approachable unit that once we move in this direction, we can

actually keep the ball rolling. So the Department of Commerce's green paper on cybersecurity focuses on voluntary codes of conduct and multistate codeword processes to advance efforts to protect the Internet from growing security threats.

And to that end, they issued a Request for Information, or RFI, at the beginning of October that looked at how can we have a voluntary industry code of conduct to address botnets from an ISP perspective, or a service provider perspective, or any intermediary? So they posted 30 questions, and I'm assuming now they have the answer to all 30 of those questions and they've achieved some good responses.

And so now we're here to discuss the outcome of this RFI and explore the path forward. So to do that we have a great program for you today. We're going to start off with discussing the RFI and the responses and then we'll move into a panel which is going to talk about the direction forward and some of the issues that we need to keep in mind, both in the market perspective and the government perspective.

So, starting off today we're going to begin with Sameer Bhalotra, who is the senior director for the cybersecurity programs on the National Security staff. He reports to the cybersecurity coordinator. He was the lead staffer in cybersecurity and tech issues for the U.S. Select Committee of Intelligence before joining the cybersecurity coordinator staff, and he also worked with the Comprehensive National Cybersecurity Initiative. He was a contributor to the Center for Strategic and International Studies' Commission on Cybersecurity for the 44th presidency. Previously he was an engineer at the CIA, worked as support staff for the CIA director, and on the Science and Technology staff inside the Office of the Director of National Intelligence. He has an undergraduate degree in chemistry and physics from Harvard and a doctorate in applied physics from Stanford University.

Talking about the DHS perspective we have Bruce McConnell. Bruce

McConnell is senior counselor to the National Protection and Programs Directorate in DHS. McConnell serves as senior advisor to a host of strategic and policy matters related to MPPD and its components. Prior to DHS he was in the Obama-Biden presidential transition team, working on a variety of open government and technology issues. He had a stint in the private industry when he created, built, and sold McConnell International and Government Futures, a boutique consultancy that provides strategic and tactical advice on technology. Before that he was strongly involved in and ran the International Y2K Cooperation Center. He coordinated regional and global critical information technology. He spent a long time in government IT as CIO of OMB, and before that he has an MPA from the University of Washington and BS from Stanford.

Finally this morning, to talk about the RFI and what we've learned, we have Ari Schwartz, who is senior policy to Commerce Secretary John Bryson. He helps to run the Department of Commerce's Internet Policy Task Force. He came to the Department of Commerce through the National Institute for Standards and Technology where he served as senior Internet policy advisor to the NIST Information Technology Lab. Prior to his work in government he served over 12 years as vice president and chief operating officer for the Center for Democracy and Technology. While at CDT he regularly testified before Congress in the Executive Branch agencies on Internet policy issues. So he's been strongly involved in a wide range of privacy and security issues, he was named one of the top five influential active thinker in 2007 by *Security Computing*.

So, with that, I turn the floor over to Sameer.

SPEAKER: There's lots of seats up here if anybody wants them.

MR. BHALOTRA: Thanks. That's right, we're not infectious. Come on up, guys. Thanks for the introduction. Great to see such a good crowd here. If we get more people you'll have to sit up in the front of us here.

Again, I'm Sameer Bhalotra. I'm deputy to the White House cybersecurity coordinator, and we've got a little staff over there of people advising the President every day on cybersecurity issues across the board, but, like he said, today we're here to talk about botnets and malware and what we can all do together to attack this problem.

I've got three main points for you today. First, I want to talk about why we're concerned about botnets and malware at high level. Second, I want to explain why and that the White House is taking this quite seriously. And third, I want to talk about how we believe in an industry-led approach going forward. So, let me just dive right in.

First of all, do you all know that botnets and malware are a real threat to Americans and U.S. commerce? The President himself has highlighted this when he came into office and many times since then.

Just a few data points that we worry about, you know. Millions of American computers have been compromised and are remotely controlled for a variety of malicious purposes via botnets. This malware enables online crime, aggression, and the potential for hostile actors to hijack our computers, servers, and networks for nefarious actions. With millions of computers controlled by botnets, the cost to consumers, industry, and government is far too high, unacceptably high. One report has sighted this as $500 million in losses in the Fiscal Year 2011. I don't know the exact number, but it's a lot of money and we need to do something about it.

Another data point, last month FBI and European police arrested the operators of a 12 million computer botnet faction. Botnets are getting larger and more dangerous every month. Today's adversaries we see tailoring their approach. Their tactics are increasingly precise, increasingly targeted, increasingly dangerous, so something we're quite worried about.

Now, obviously, our job here is to move beyond talking about it and implement solutions. What are we going to do about it? Now, many companies have done very good work here and I want to make sure that you know we know that. Many companies have done good work here, but we think there's still a gap in this country that we can address. Our country can do better to address this threat.

Now, in addressing botnet infections, we have divided up the challenge into six primary categories that we are concerned with -- and I think you guys have heard this six before. The first is awareness; second, identification; the third, notification and education; the fourth, remediation; the fifth, information sharing; and the sixth, last but not least, measurement.

Now, today here in this session, at least for our panel, we would like to mainly focus on near-term progress towards identification and notification and education.

Okay, second point; the White House takes this seriously. That's why I'm here. This is why the White House with the Office of Science and Technology Policy and the Department of Commerce and Homeland Security met with several private sector leaders as well as trade group and consumer advocates last week to explore plans for engaging in a multi-stakeholder approach to develop a strategy to tackle botnets.

In this room we all bring distinct skills to the table to find a solution. The best practices and guiding principles will serve to enhance botnet identification, effectively alert and educate customers, and will move us to the next phase of effective remediation, information sharing, and measurement.

So the White House is committed to protecting consumers in this country, particularly the most vulnerable. For example, small businesses and individuals who could suffer catastrophic loss of data from a botnet infection as well as supporting America's private sector and industry whose loss of intellectual property, sensitive

customer information, and reputation can be severely damaged when a botnet attack occurs. So, we in the White House are making a real effort to ensure that the White House, the Department of Homeland Security, Department of Commerce, and Federal Communications Commission are all on the same page here, working together. So what we're trying to commit to is a government team that's integrated and on the same page so we can work most effectively with all of you who are outside the government.

I'd just like to take a moment of thanks -- to give thanks here to Bruce McConnell from DHS, who's done a ton of work here. Of course, Ari Schwartz from Commerce, and standing in the back, Zachery Nunn. He's a staffer in my office who's the lead for the White House for this effort. So if you haven't met Zach, please find him after the session here and say hello. He's doing a great job.

Okay, third and final point, we believe in an industry-led approach and voluntary action. So I think, you know, that's clear, but I just want to emphasize that. This is not an effort towards regulation that we're hiding. This is a voluntary approach and an industry-led approach, and that's where we want to be right now. We are asking industry to lead here and close this gap.

Now, the Department of Commerce in the November RFI, which Ari is going to talk a lot more about, provided some clear feedback. Clearly, industry responded overwhelmingly that a multi-stakeholder approach is best suited to identify and notify consumers. It's best suited and can do the job, so we look for you to help in the next steps here. Innovation, customer-based software and hardware development, unique assets, are all best suited to address this challenge in your own industries and through your own business operations.

So what do we want to do? We in government want to help you. We want to support you and enable this industry-led effort to address how industry will

identify, notify, and help educate consumers. We have the ability to start today by implementing best practices from a broad range of experts like you, who deal with this challenge every day.

We also want to stay out of the way so you can make progress on your own; generally a good rule of thumb. For our part, we will commit to be an honest broker for all stakeholders who are ready to share best practices, good processes, and support the development of metrics aimed at evaluating success. That's what we're here for.

So just what happens next? We need your help with many questions and I think these are the questions that are going to come out in the next few months. How should we all cooperate here and coordinate among industry, among government, and between our two groups? How should we engage citizens and Americans on this issue? How will we measure our progress? These are the questions that we think are coming ahead that we look forward to working on.

So, just in closing, again, we believe that a voluntary national effort to implement best practices is within reach and we think we have the right team here in this room to do it.

So, with that, I'll pass on to Bruce McConnell. Bruce?

MR. McCONNELL: Okay, thanks so much, Sameer. So I want to do two things: one, explain how the Department of Homeland Security fits into this picture and also try to paint a little bit broader picture of how the various parts on the government side fit together because there is a lot of different players and, you know, that can often be confusing.

So, on the first point, Homeland Security. So, Homeland Security, as you know, our overall mission is to create a safe, secure, and resilient place where the American ways of life can thrive. And among those there are five mission areas that we

work in, and one of those is the safeguarding and securing cyberspace. So we -- earlier this week, in fact -- released the blueprint for a secure cyber future which lays out a plan for the meeting the mission of safeguarding and securing cyberspace. And as that blueprint says -- and as its precursor, the Quadrennial Homeland Security Review said -- it's a strategy and a mission just not for DHS, but for something we call the Homeland Security enterprise, which just means everybody else. So that means the other federal agencies. It means state and local governments. It means private sector companies. It means individuals.

Homeland Security is a shared responsibility and that's no more true in any space than in cyberspace. So we can't do it by ourselves. We're teamed with others up here and others you'll be hearing from today and, also, with all of you and others in the private sector and internationally to make this happen.

In the blueprint we talk about two key areas which are going to be our focus and I wanted to use that to set the context for this activity. Our mission is to protect the so-called "dot-gov," the federal civilian agencies, and to work with private sector, particularly critical information infrastructure, to help them protect themselves. And we're going to do that with all of you and with the rest of the Homeland Security enterprise in two ways, first by protecting critical information infrastructure, including federal agencies today. And then the other focus area is building a healthier cyber ecosystem for tomorrow.

So this project of stopping botnets is something that we can work on now and we can also work on in terms of architecture and things in the future. And as Sameer suggests, we're focused today at the moment about what can we do in the near-term to help reduce this. I like to think of botnets as kind of like a chronic, low-grade infection that you might have in your body. It slows down your performance, you're not

performing up to speed, but it also opens the door for more serious attacks and so it's bad in that way. And unlike perhaps in the biological metaphor, it's also available for other actors to rent. So, you can't rent a virus in the body, but you can in cyberspace. So a very dangerous thing and more dangerous than it appears just kind of its everyday state.

So, this area is completely an example of something that requires a shared responsibility, so I want to talk about that because our job at DHS, we work closely with the communications sector and the IT sector. We're the responsible critical infrastructure sector-specific agency for those sectors, but it's not just about us. And, in fact, you'll hear in a few minutes from Jamie Barnett from the FCC about some of their perspectives on this. And they are a partner and we are participating with them on the Working Group 7 of the CSRIC -- which I can't expand the acronym, so maybe Jamie can do that for you -- but anyway, that's the Botnet Remediation Working Group. And the focus of that group has been primarily on the ISPs. There's going to be in March of next year, their plan is to -- of the working group -- is to issue a set of principles that could become a voluntary code of conduct for the ISPs; later in the year, in September, some of the obstacles that might be in the way of that, and even later than that, some metrics for success. So we're excited to be cooperating and helping in that work.

But as the FCC has recognized, and as the RFI points out, the ISPs are only one part of the ecosystem. They're good at detecting. They can maybe have some role in notifying, but many others of us in the ecosystem need to do our part. And many others collect data about what's going on and can see what's happening in different ways and see different things about what is happening in particular botnets or in the system as a whole. So that's what this inquiry is about: trying to find out and be more precise about what other's responsibilities are, what all of our responsibilities are, and how we can work

together on this.

So, with that I'll stop and turn it over to Ari. Commerce really has the lead on this. We're there to provide, you know, the particular security perspective, but Commerce is the place which deals so much better with the private sector, so.

MR. SCHWARTZ: Thank you, Bruce. I feel like I've never had a botnet talk where I've been set up so nicely on all the topics. I don't have to give a lot of background to get to the point of talking about where we go in the future. But, you know, I think Allan really set up the Commerce role very well there, which is, you know, we've laid out in our green paper the importance we think of voluntary action and voluntary codes of conduct going forward for cybersecurity to be really successful. We've been very supportive of the legislative efforts that the administration's been pushing forward and we've been a part of that team, and we think that that's essential for protecting the networks, but we will still also need -- even when we have that in place -- we will still also need voluntary action to go after problems as they crops up.

And this area of botnets where we have best practices today -- we have companies that have been very successful in this space and we have countries that have done this in other areas. It seemed to us to be a place where we could better organize collective action towards a single goal. And to help to do that and to -- there was a lot of questions in our head. We tried to get those down through this RFI process and we received 30 responses. We thought that we would receive really high-quality responses actually. We were very pleased about that. They're all available on the NIST website now, so you can go take a look at them.

And those responses told us some interesting things. First of all, the thing that we heard -- one of the things that we had asked very clear and, to us, wasn't really a completely open question, but I think if you read the responses it comes up very

plainly that there is strong agreement that botnets are an important issue that warrant government attention. And, therefore, the things you've heard about kind of the next steps here in this space come out of that question in the RFI and the response we got out of that.

We also heard very strong agreement that the solutions need to go broader than just ISPs. Literally, almost everyone that responded, whether they were an ISP or not an ISP, and even the consumer groups and privacy groups, all said this needs to be a much broader solution than just the ISPs. It's got to involve everyone in the Internet ecosystem -- and a lot of people use that Internet ecosystem term -- directly.

There was strong agreement that this needs to be a voluntary public-private partnership and that that will help any approaches moving forward, if we have that kind of cooperation between a government and industry and multi-stakeholder approach on this subject. And there's a lot of discussion about the existing best practices that are already out there, as I mentioned: the desire for greater educational products than we have today and for coordinated educational products, a desire for greater information sharing through a lot of different paths to kind of get to the answer to that question. As Allan said, there's a lot of agreement about the term "information sharing," but when you get into the details of what, where, when, how, it becomes a lot more difficult to work out the issues on.

And similarly, there was a call for a lot more measurement to be done in this space. There have been some measures. Some of them have not been made public, some of them are public but are very broad, so we need a lot more work to be done on measurement. And there are a lot of ideas about how to do that, but not a lot of consensus on what exactly those measures should be. There was less consensus around the idea what should be done about remediation and what should be done about

incentives, which we asked a lot of questions on those topics. We did not receive, really, a general feeling of agreement at all in those areas. So that's something we'll need to push harder on as we move forward in this process.

So, what are the next steps? Well, we've already been meeting with stakeholders, of people that commented in particular, to get more information from them, and with others who were raised through the comment period. And we're trying to help to connect parties that seem to have similar solutions and help the private sector continue to develop leadership in this space. So that is something that is continuing on right now.

But in general, we believe that the best path forward is going to be to try and help the drive of this kind of idea of a public-private partnership where consensus and best practices already exist. In particular, we feel as though there is -- we can make progress towards reducing the total number of botnets. That's something that other countries have shown that they've been able to do through working together, through voluntary collective action and solution. And, also, we believe that there is -- we can help to better educate those that have been infected, give them more information about what to do when they have been infected, about the fact that they are infected, et cetera.

One suggestion is to have the private sector work together in a voluntary way to draft high-level principles in this space, and that then these codes of conduct or industry best practices can grow out of. We've heard pretty clearly from a lot of the ISPs that are working through the FCC CSRIC process that they like that process that they want to see that form the basis for what happens within that sector. A lot of work still needs to be done in the other sectors and trying to draw those high-level principles that can work across sectors is going to be important. And how to get that implemented is going to be important going forward.

DHS and FCC have also been really cooperative in discussing how

they're willing to use their educational products, use some of the government resources out there, and the platforms that they have for education moving forward as well. And so we think there are a lot of ways we can tie in government solutions that already exist out there that can help to solve this problem a little bit better as well.

So we're going to continue to have that kind of conversation and look to the private sector as to how we should go about convening, whether it's a government convened solution, whether it's a private sector's convened solution. That's something that was not answered 100 percent clearly in the comments that we received, but we've been getting a lot more feedback from the stakeholders about that as we move along and we expect to have some answers to that in the near future.

MR. FRIEDMAN: Thank you. So, great overview of the topic. And I suppose we should have asked at the beginning, this might be one of the first times that there's been a high-level policy discussion where we haven't had to define a botnet, which I think is actually major progress in terms of moving forward in this area.

SPEAKER: Plenty of seats up here.

MR. FRIEDMAN: So, since we have such a packed house, I think I would turn it over to the floor for questions. We have someone coming around with a microphone. Just a few reminders on questions: it is Brookings' custom to identify yourself and where you're from. If you don't choose to, that's okay. But perhaps, more importantly, a question's chief characteristics are that it's relatively short and ends in the iterative punctuation mark. (Laughter)

So we have a -- there.

MR. RANSOM: Jesse Ransom with the Public International Law & Policy Group. Does the government have any sort of back-up plan if private sector and government can't come up with a consensus or, I guess, in the general sense as well?

MR. McCONNELL: So I think we're very hopeful and confident that we'll be able to work something out. We have a lot of public-private partnerships going in this area. And I think this is an area which lends itself to voluntary working together, so I think that's -- we don't have a plan at the moment. I don't think we're going to need one. Obviously, you know, time will tell.

MR. SCHWARTZ: I mean, one of the benefits of, you know, working on the educational piece of it is that those products will be useful whether we have, you know, the broad success that we really foresee right now or we end up just doing better education on best practices, and then we have these educational tools at the end. So I think that comes out of it either way. But I agree with Bruce completely that this is -- I mean, if we can't do this one where there's already best practices and there's already people moving in this direction and other countries have done it, we're going to be in big trouble in terms of coming up with voluntary solutions in this space.

So we think that there's motivation to do it in industry out there that people have basically been moving in this direction. If we can get it coordinated it will be much better than if it happens haphazardly.

MR. BURNS: Tom Burns. I'm the CEO and founder of ThreatSTOP. We do botnet mitigation. I guess this is a double-barreled question related to state actors and related to countries. Ari, you said that several countries have successfully mitigated and stopped botnets? That hasn't been our experience, so I'd like to know which ones?

And then the separate part is there are several countries that the state actors are actually running the botnets. How do we propose to address that?

MR. SCHWARTZ: I never said -- I want to repeat, I never said that any country has stopped botnets. I said they've been successful -- they've demonstrated that they've been successful in reducing the total number of botnets that affect their country.

Now, did notification help to do that? That is still unclear. We don't know. That's one of the problems with the measurements in this space is that it's not -- you can't tie the direct measure of people that have been notified to the drop in total number of botnets that are out there.

Japan -- and, unfortunately, Yurie is not here today, but she has pretty good documentation on the number of botnets that they've had over time and the existence of the Cyber Clean Center and that comparison compared to the same percentage rate drop in other countries. And it shows that Japan has been relatively more successful over that period of time in total number of botnets dropped.

Is that related to the fact that the Cyber Clean Center exists out there? That's something that could be debated. We think that the fact that they're doing education certainly helped with that process. So we tend to see the numbers that they have and if, in fact, they've been a success there.

Australia, again, they haven't said, you know, the recidivism -- they don't know the recidivism rate, but they do think that there has been some effect on the number of botnets when you talk to the people who put together the program, and they feel pretty confident about that. And they feel that their security marketplace has changed as part of the kind of collective action taken from the ISP association, doing education around this in a coordinated way, which is a positive thing as well.

So, you know, again, we don't have the measurements that, say, have a direct tie because people are being notified in Japan, Germany, Australia that the number of botnets have directly gone down. However, we do feel as though it has had impact on those marketplaces in a positive way and that we feel that we can do better than that in the U.S., and we can come up with better measures to show that it's working and help to solve this problem better across the world.

One of the things that we asked questions about that I didn't get into was kind of how do we view this internationally? And there has been some work at the OECD around this issue and coming up with best practices in this space. I'm trying to share information there.

There's a question about whether APEC would be a good forum to do this. Korea has been looking in this space as well, and you have Australia and Japan already as leaders in this space. And now we have this RFI out there and at least have gotten back information moving forward. So it's a ripe issue for better coordination internationally and that could help to bring down total numbers, too, if you have more countries on the same plan, working towards the space.

So, again, I don't think you're going to get to zero because you take on one program -- zero number of botnets -- and stopping botnets. Bringing down the numbers would be successful and creating a better environment for the security marketplace would be a better result as well.

MR. FRIEDMAN: A question in the middle in the back?

SPEAKER: Is this on? Yes? Some time ago I was on the President's National Security Telecommunications Advisory Board and I noticed from Googling it last night, it's still up and active. And it represents on that board just about every major telecommunications producer of a platform. Have you thought domestically of asking them what -- each company -- what they could possibly share, be willing to share about known intrusions into their system? And then, going forward, is that a basis for your metrics?

MR. McCONNELL: So, thank you for that. Actually, the NSTAC -- the National Security Telecommunications Advisory Committee -- so great to see you -- is still active, as you say. And, in fact, last week we had a meeting of the members, an in-

person meeting here in Washington, which was open to the public and this topic came up. In fact, Ari and I gave a presentation on the RFI, similar to the one that you've heard today. And there was quite a good discussion among the members from those companies -- senior people from the companies, some CEOs -- about what they could do and they had quite a bit of interest in the RFI process. Many, if not all, of the companies responded to the RFI, either directly or through their industry associations, so they're definitely interested. I think they're, at this point, they're going to watch what happens for the moment before they decide whether they should take an action as a group. But it's definitely on the plate, so thanks for that.

MR. FRIEDMAN: There's a question on the aisle.

MR. CHATTERJEE: Samar Chatterjee from SAFE Foundation. Just curious, since the presentation was fairly low-key, because whenever problems like this happen, the United States always goes to war, you know, we didn't hear that term. Is the botnet problem still within manageable limits? Because I know the military has set up a cyber warfare program and I'm sure the CIA and the FBI have also prepared their programs for that. Is that not needed to bring the botnet problem under control internationally?

MR. BHALOTRA: Thanks for the question. So this is not a cyber warfare thing right now. And, in fact, to connect, you know, your previous question with this question, what we're focusing on internationally are largely law enforcement cooperation and diplomacy. You're seeing increasing investments in diplomatic efforts, multilaterally and bilaterally, under the President's international strategy to secure cyberspace. You're also seeing, building on a long history of law enforcement cooperation with other countries, increased efforts there; increased investments in, for example, FBI and domestic law enforcement capacity in cyber agents and experts as well

as more and better cooperation with other countries to go after botnet operators. I gave an example in my brief comments about something we announced last month about a major botnet operator that was taken out due to U.S. and foreign cooperation and law enforcement. So that is where we are focusing our efforts now and, you know, hoping to build on our recent success and do better and better.

MR. SCHWARTZ: I mean, I think, you know, one of the things we say in our green paper is that for the non-critical infrastructure space most of the problems that we see out there today have solutions. There are standards that are built to address these problems. There are best practices out there to address the problems that we see. The hard part is incentivizing people to actually put them into place, especially when you need everyone to do it, right? So we need a lot more effort on figuring out how to get that done, which is in line with how the Internet grew up. Right? We came up with solutions and we figured out ways to get people to incentivize people to implement them, to make it happen globally, without heavy regulation and without, you know, kind of addressing it in that kind of a way. And that's what we want to try to keep promoting in this space. We feel like not enough attention has been put onto those existing solutions to move them forward to get attention to get this done, but that's what we want to try and do.

MR. RASCH: Mark Rasch, CSC. Ari, you knew this was coming. How do we incentivize people to do this, especially when, at the end of the day, particularly in the commercial sector, you spend millions of dollars or tens of millions of dollars and, at the end of the day, nothing happens? In other words, if you're successful, nothing has happened. So how do you make a business case for spending all this money in resources to ensure that nothing happens?

MR. SCHWARTZ: Well, I think what we learned, you know, I said that there was not agreement and not consensus on the incentives piece, and what we

learned is sort of that the harder part here is going to be the fact that different industries in this space have different incentives. And you're going to need to try and take advantage of the right incentive for the right industry.

I think one thing that we need to see really is, as I was talking before about coming up with a healthier ecosystem for it to build up a good marketplace for security and improve the marketplace for security in this space, that there has to be some more responsibility from some of the consumers and residential actors out there in terms of when they get infected. First of all, they have to find out that they're infected, right? It's hard to give someone an incentive to clean up their computer if they don't know that they have a problem in the first place. That's one of the reasons that we started with this particular project because we think that this could help to do that. So if you can give them some incentives to clean up their own systems and demonstrate to them why it is helpful to them and to society to do it, we think that people would be willing to engage in managed security services and other kinds of services.

That should then give incentives to companies to try and get them, to convince them that their solution is the best solution. There are problems with that as well in that you can -- we know there have been fraudsters that have tried to do that in the past, telling people that they're infected, and we have to monitor that and figure out ways to combat that. We have to figure out, you know, better ways of education to make it easier for people to get those kinds of solutions.

So there are issues involved with that, but we do think that, you know, the first step is informing people that they have a problem and then we can build some incentives around that for this one space. Other areas we're going to have to come up with different kinds of incentives.

MR. BHALOTRA: Just to jump on that because this is a great question.

You know, nothing happens is a classic security problem, right? I think here there's an opportunity for all of us to do better at improving our story. You know, if we just baseline where we are today, there are massive losses, like dollar losses, right, from identify theft for consumers, intellectual property theft from companies, loss of operation and income from companies who are out of action during a botnet attack. That's real money, that's real dollars. Right? And if we can do a better job quantifying that, it's always hard to get good statistics, but, you know, the better we can do, the better our story is. And then you go to your CFOs and your CEOs and you say this is what we're losing now and this is the loss in confidence that your consumers and customers are encountering, and we can bring that down. And then it becomes a cost savings argument, at least for CFOs.

I think there's work we can all do here to improve our story, starting with baselining how bad things are now in actual dollar terms and then showing how we can maybe take a chunk out of that.

MR. FRIEDMAN: Question all the way in the back.

MS. SCHOLTES: Hi. Jennifer Scholtes from *Congressional Quarterly*. And I'm just hoping to find out what you expect to see from Congress or what you want to see.

MR. FRIEDMAN: See, I knew there was a reporter sitting back there because they're in the chair with a computer on their lap, so.

MR. BHALOTRA: I'll start. So first of all, I appreciate the question. We didn't want to focus too much on the larger legislative efforts, as Ari referred to. The administration has been very active, right, in advocating for cyber legislation across the board. I think we've had over a dozen different hearings in the last few months with Ari and Bruce appearing frequently on the Hill. So if it's okay, I think I'll take that offline or refer you to the debates we've had on the Hill already.

In this area, again, notification -- dedication and notification of botnet remediation, you know, we are not looking for legislation. I think I'll just repeat the point again; this is not a path towards regulation. This is not a step towards congressional action. This is a let's take best practices, let's find common interest, and let's work this together on a voluntary basis. We think there are companies that have done a lot of good work here. We think people are primed to work together here and we think we can really take a bite out of this problem and close the gap in this country. So that's where we are.

MR. McCONNELL: This is actually a case, though, where, as far as education, the classic technique of holding hearings would be handy from the standpoint of helping Americans have a better understanding of the problem and the costs and all those kinds of things. That'd be a great service.

MR. SCHWARTZ: I'd like to point out to the Republican task force on cyber legislation, point to this exact area as a space where voluntary efforts by industry would be extremely helpful. So I think that's directly in line with what we were already in the process of doing. So, I mean, it's great to have the Hill being supportive of the efforts in that way.

MR. FRIEDMAN: Question in the front here.

MR. SACHS: Mark Sachs, Verizon. Detection, notification, mitigation very important. What about prevention and the role of law enforcement to actually get out in front of this problem and start making it go away rather than trying to just mitigate after the fact?

MR. McCONNELL: So as Sameer suggested, that's a key part of our approach to this on an international basis and also on a domestic basis. This, like many other computer crimes and some of these definitely fall into that space, you know, need

more prosecution and I think we're going to -- not just because it puts away the individual person or persons who happen to be performing, you know, running that particular system or performing those specific actions, but because it creates a deterrent effect. So I think, as Sameer said, we're definitely ramping up the law enforcement side of this to help because I think that's going to be a key part of the deterrent part of preventing. In the Blueprint for a Secure Cyber Future we mentioned law enforcement a number of times in the "prevent" space from the standpoint of creating a deterrent effect and raising the cost for malicious actors, so yep.

MR. BHALOTRA: And just to give some data points, you know, to show we're serious, right, if you look at the Fiscal Year '12 budget that Congress is working on now, you're seeing increased investments in domestic law enforcement capacity, experts to actually do exactly what you're talking about. And as we build out next year's budget, February timeframe, I think you'll see that trend continue.

You're also seeing just more creative legal actions, right, that we're working on. So I think there are a plenty of good signs in that direction, but today we're just focusing on the other piece. So, thanks.

MR. FRIEDMAN: We have time for a last question for the panel. Yes, on the aisle there.

MR. SCHOETTLE: I'm Pete Schoettle from Brookings, and sorry for the simple question, but I'd like to get back to incentives. As I look at this sort of simplistically, I get the impression that the incentives of what's good for the system are totally contrary to what's good for the individual. Example: Why would any bank -- Citicorp, any bank -- say, hey, we're vulnerable, we've got a problem? Their total -- because their competitors then win. Their total incentive is keep it secret, don't let the customer know we're vulnerable; we don't want to lose customers. So all the incentives

in a marketplace, you stressed market incentives, are to keep it secret and not share.

Can you see any ISP or some other manufacturer saying to the world, hey, we got -- a second point -- we got a vulnerability right here? This is our vulnerability, help us fix it? Hell no. Their total incentives are to disguise, to hide their vulnerabilities, the opposite of what's good for the system. So I don't understand how in a market arena the incentives work.

MR. SCHWARTZ: First of all, I mean, in general on cybersecurity, I completely agree with your main point, we do not have the incentive structure today to deal with this issue and we need to help to create that. If you read our green paper, the Commerce green paper on this topic, we go into detail about why insurance markets have not worked to date in this area and some other issues as well. And we look into things that we think could be -- could help to address some of the issues involved. However, it's going to be a challenge.

This is space, though, with botnets where that's not necessarily true for all the actors involved. For example, there are ISPs that -- and, you know, Comcast being the main one that has made this actually part of its brand, right, to say we're going to protect our consumers and we're going to tell them when they've been infected in ways that other ISPs don't today, and they haven't shown that they have an incentive to have security like that today. So I think that there are incentives for ISPs out there.

And the other one you mentioned, too, is banks. Banks have a big incentive to make sure that their customers know that they've been infected. It is hard for them to do a loan today, but what we've heard from them, and they come -- the bits, the high-tech folks involved in the space, what we heard from them is they would like to work across the ecosystem to help to come up with solutions to get -- so that they can find the ways to notify their consumers and have others notify their consumers when they've been

infected so that they don't have the fraud problems and the number of fraud problems can go down without talking about their own vulnerabilities. Right? They're talking about the vulnerability of their customer, not the vulnerability of the bank in that case.

So I do think that this is a space where we can come up with different kinds of incentives if we can get people working together, come up with the high-level principles to do it. I don't think it's going to be an easy task to get the incentives for all the different places working together quickly, but I think that there is the possibility for incentives.

MR. FRIEDMAN: All right.

MR. SCHWARTZ: You're not going to challenge me, Allan?

MR. FRIEDMAN: That is a very long discussion, but I think you're right that this is one of the few areas where the incentives do seem to line up and it's an information problem and a coordination problem. Coordination games are the games that you want to be playing.

So I hope you'll join me in thanking Ari, Bruce, and Sameer. (Applause) So I think for the next part, I'm going to ask Ari to stay up here.

So it is now my pleasure to welcome Jamie and Brent up here once we've -- they have to know where to sit. It's very important here.

So we've heard the basic discussion of what the government is doing and now we get to criticize it, which is always the much more fun part, I think. We've asked Ari on the panel to talk about the international component, but to begin the conversation we'll have Michael Kaiser, who is the executive director of the National Cyber Security Alliance. As their chief executive he engages in diverse constituencies -- business, government, nonprofit -- and works on their education outreach efforts to strengthen the nation's cybersecurity infrastructure. They are most noteworthy for their

annual Cybersecurity Awareness Month, although I think it's important to note that it's a year-round process, which they like to emphasize, as well as education at the higher education, K-12, and small business area.

Prior to joining NCSA, Michael spent 25 years in the field of victim services and rights at the National Center for Victims and Crime in Washington, D.C., and at Safe Horizon in New York City, where he held a variety of senior staff positions, including the director of program development and strategic alliances. Throughout his career Mr. Kaiser has worked on public education efforts that work on building broader constituencies to put different groups together to highlight important problems.

He is the co-author of *The Official Guide to eBay Buying and Selling and Collecting Just About Anything*. And he is also deeply engaged in a number of non-profit boards.

So talk about some research in terms of the consumer side, we have Brent Rowe, who is senior economist at RTI International. His research focuses on technology policy and security issues and has been funded by the Department of Homeland Security and Commerce, among others. In particular, Mr. Rowe has led several studies aimed at evaluating economic issues surrounding cybersecurity policies, including a recently completed study aimed at assessing the market for Internet service providers to provide more security to home Internet users; a very timely study, I think.

And to talk about the broader government questions we have Jamie Barnett from the FCC. I want to point out, as soon as I can pull up his bio here -- excuse me -- Jamie Barnett is chief of the Federal Communications Commission's Public Safety and Homeland Security Bureau. He's responsible for overseeing the FCC activities pertaining to public safety, homeland security, emergency management, and disaster preparedness, and represents the commission on these issues before federal, state, and

industrial organizations.

Barnett served for 32 years in the United States Navy and Navy Reserve, retiring in 2008 as a rear admiral. His last active duty assignments were deputy commander in the Navy Expeditionary Combat Command and the director of the Naval Education and Training in the Pentagon.

Before coming to the FCC, Barnett was senior research fellow at the Potomac Institute for Policy Studies, a policy think tank devoted -- focusing on science and technology issues and the importance of the nation's security, including cyber conflict and cybersecurity. From 1984 to 2001, Chief Barnett was senior partner in Mitchell McNutt & Sams as their government law practice expert.

So with that, I'd like to Michael to talk a little about what his organization is going to be doing in terms of coordinating these efforts.

MR. KAISER: Great. Thank you so much and thank you so much for having us in this afternoon. This is really an important topic and already the discussion's been quite interesting and, you know, I hope we'll continue this dialogue in a more significant way as well.

Let me just quickly tell you about NCSA. We're a public-private partnership, which means we work with industry and government. We have 18 corporate board members; some of my esteemed board members are sitting in this room this afternoon. Thank you for coming. We work closely with government, with DHS, with NIST, with the Department of Education, with the IRS, with others who we engage in around education awareness, around our shared responsibility for keeping people safe and secure online. We worked very closely with the Anti-Phishing Working Group and with government, DHS especially as well as many others, 25 industry partners, to develop the Stop.Think.Connect campaign in a coordinated way. And I'll talk a little bit

about more of that in a second. But the way that public-private partnership evolved has lessons for us, I think, in efforts like this as well.

And recently, we actually signed an MOU with NIST and the Department of Education to address in a comprehensive public-private way the future of cybersecurity education in this country from K through life, as we like to say, to really try and address these issues in a comprehensive way, which is one of the reasons that you do a public-private partnership, is to try and actually solve the problem for everyone at the same time as opposed to just recommending one way to do it.

Let me just tell you what I think a little bit some of the elements of a successful public-private partnership is since that words gets bandied around quite a bit. But, you know, and it's almost a hackneyed phrase in a way unless you really dig down a little bit deep and take a little closer look at it.

So first of all, there are some obvious things, right? You have broad stakeholder involvement. You have people from many different areas participating in the effort.

You have to have experts. You can't have a partnership without people who actually know what they're talking about, right, about the issue that's at hand.

The effort has to be owned by this group that works on it together. They can't be created for them or on behalf of them. It has to be owned by all the participants equally at the table.

Somebody raised earlier the idea of consensus and we very much feel that in a public-private partnership you must move ahead by consensus or else people drop out, you're not going to get what you want, you're not going to keep people at the table in the way they need to stay.

You have to be -- know what -- your end result that you want, but, you

know, sometimes the path between A and B is not a straight line, and so you have to be flexible as you move along.

People have to be engaged in this process in a meaningful way. They have to have assignments and participation that allows them to feel like their work on this effort is worthy and will produce results.

And I think this specifically -- we'll talk about botnets in a second -- but it has to be grounded in a shared problem, right, a problem that we all agree exists, or a strong belief that a solution is possible. So you can either have a problem that everybody agrees exists and you want to solve it or you have to have a sense that there's possibility that we could actually solve the problem. So I think you can go either way, and I think this actually speaks very well of the botnet industry myself.

You have to understand that in order to really have a successful partnership in this arena that the solutions are going to require a shared investment, right? No one's going to be stuck footing the bill by themselves to solve the problem. The reason you come in partnership is because you understand from the very beginning that everybody plays a role in solving it and they're probably going to have to make some investments along the way to make that happen. And that's why it's important that you have the multi-stakeholder process, of course, and that people have roles and that it's not -- I mean, there are many different kinds of ways for people to come together, but in a public-private partnership it is not advisory role. It is an active working group, right? If you want advisors, go get advisors. If you want to solve a problem in a collective, collaborative effort, that's when you put together a public-private partnership.

And I'll just say a couple things why I think this is important on botnets and why we can do it. First of all, everybody's used the "ecosystem" word a lot already today, but the reason that we use that word and I think the reason it's important here and

especially when we're talking about botnets is that in an ecosystem it's very complex, and what happens in one part of the ecosystem impacts other parts of the ecosystem. And if we're talking about an ecosystem that has things like botnets or maybe use the virus example that was used, you know, earlier that Bruce kind of raised, if you just get rid of one of them, but everybody else is still sick, you're not really solving the ecosystem problem. If just one group goes out and cleans out the botnets in their area of the ecosystem, it doesn't solve the problem and they're likely to be re-infected again. So that's an issue.

This a complex issue. There are many -- it's already been raised, you know, the elements of, you know, education, awareness, remediation, notification, information sharing, there's a lot of issues that have to be addressed. And I think people sitting around a table trying to hash that out is really important.

There are many owners of this issue. There's no one who's solely responsible for this issue. There are many owners. Government has a very important role. Government has an important role as a user of the Internet to make sure that citizens aren't infected who come to their websites, let alone banks, let alone ISPs, let alone other financial institutions or e-commerce sites, right?

There are already some good ideas out there. I think as Ari has raised already that there are some good ideas that are worthy of some really serious and rigorous looking at that could be done across a broad way. And I think one of the most important aspects of this on the botnet issue is that there are already a lot of people who want to get involved. There's already a broad group of people who believe that by coming together we can make some movement on this issue. So I'm really excited about the prospects of a public-private partnership or a collaboration or a multi-stakeholder collaboration process, whatever you want to call it, to address this issue because I think a

lot of the fundamental pieces to make that happen are possible.

I'm happy to say that following the meeting that Ari mentioned earlier, that the National Cyber Security Alliance agreed in early January, on the 4th, to pull together a meeting, I like to say sort of get the ball rolling and bring people together and start to talk about the way we might organize around this issue and create a structure in which a partnership might be created in some way, shape, or form still to be determined; a lot of work to do on that regard. And that meeting will hopefully be the beginning of a process that will lead, I hope, in many ways to some early results because I think there are some issues, like education and awareness and some other things, that a lot of motion can be done very quickly, and maybe start the process for a longer approach.

And I'll leave it at that for now and will be happy to answer some questions later.

MR. ROWE: Hi. My name's Brent Rowe. I'm an economist at a nonprofit research instituted called RTI International. I'm going to talk a little bit, I'll skip over some things that I think have already been said, but kind of do a little conceptualizing of this issue from an economics perspective; talk about some of the gaps that I think still exist in terms of our knowledge; and then talk about some of the work that -- or the particular study that Allan mentioned that we've done to try to help fill those gaps.

So first of all, as has been said, but in a very direct way, from an economics perspective it makes sense for ISPs to have a role here. From a legal standpoint it's normally thought that the person that can act best with the least cost is the actor that should take a role here and that makes perfect sense for ISPs to have this role. So from a conceptual standpoint this makes sense.

But that assumes that ISPs, A, can provide security, which, as we talked

about before, is not 100 percent certain that some of the actions we're talking about will improve security; and B, that there aren't any significant unintended consequence, such as increases in the price of Internet access for home Internet users, thus potentially increasing the digital divide.

So what can ISPs do? We've talked about this, but I think it's important to take the different actions that ISPs could contribute and say that they don't all have to be involved in all those areas. So the primary areas, I think, are that ISPs could have a role are education, identification, notification, and remediation. In all of those areas you need data on how much it's going to cost ISPs to get involved in this area. You need to add on how much it's going to cost any type of public-private partnership to get involved in this area. And some of that data is more available since you do have some companies getting involved and you do have some international public-private partnerships. But you need both cost data on each of those specific areas as well as benefits data. Who's the right person to do it? Who can do it for the least cost and the most benefit?

So why aren't ISPs acting? It's fairly obvious, but they don't perceive a demand from home users for this. There are legal issues involved and there's a high cost, particularly with notification and remediation. There have been some solutions internationally that are coming about and locally, where organizations have automated some of these things. If more organizations -- if those types of things are made in an open source format, that could be a way to lower the cost for lots of organizations. But these are real barriers and they're barriers that need to be lowered before anyone's going to be able to act.

So what are the different ways that ISPs could be motivated? One is increased private demand. And I'll talk a little bit about the study we did, but if home users started saying we care, we want you to secure us more, ISPs would start acting

more. So demand is one way to do it.

Another one is to reduce the cost for them to act. So if the government took on one of those four roles or multiples of those four roles that would reduce the overall cost for ISPs to get involved in some way. Again, each of those components needs to be thought of separately and you don't have to necessarily say the government gets involved in all four or that ISPs are in control of all four. It could be a mixed bag and there could be incentives for them separately.

So what do we need to move forward? Like I said, we need more cost data and more benefit data, and that means for each of those specific areas you need to know how much it's going to cost ISPs to act and how much it's going to cost any other structure to potentially act in this area. And you need to also understand any adverse impacts. So if the ISPs start acting, if some type of public-private partnership or government organization starts acting, is there going to be any potential impact on legal activities on the Internet? If so, that needs to be thought about. And maybe it's so insignificant or so small that it's worth the cost, but it shouldn't be ignored and kind of swept under a rug. So objective data I think is the key here.

So moving down, because I think we've talked about a good number of these things, what did we do? So we went out and did a survey of 3,500 home Internet users. For those -- and I don't think we probably have too many economists in the room -- we used the technique called conjoint analysis. It's very common in the marketing world to basically put price information on specific attributes of a product. So you could think about it like a toothbrush: it helps you price how much someone cares about -- wants to buy a red toothbrush versus a blue toothbrush; how much they might care about hard bristles versus soft bristles. So the techniques that you use to help price that information can also be used in other areas. It's been used quite frequently for 30 or 40

years in environmental work, benefits analysis environmental work. So we took some of those techniques and set up a series of questions to ask home users how much -- or excuse me, to choose between options in which their ISP might provide them security. And they also had an opt out, so they could say I don't want either of these options.

Within those choices they would see a price. They would see how much their ISP might be willing to restrict their Internet access or even cut them off. They would see if they were ever going to be asked to spend any time on security. And then on the benefits side, and this is not to say that these benefits would necessarily come true, but we were able to monetize how much people cared about these benefits. We showed reductions in identity theft, reductions in the potential for your computer to slow down or crash, and reductions in the risk to other people. So getting 3,500 people to fill out this survey we were able to monetize each of those costs and benefits.

And in the end, the kind of take-home number that I'd say -- well, two numbers I'll mention and then I won't talk about the report anymore, it's online. But at the top end, if you reduce all the costs, so if people are not asked to spend any time and they never had the potential to have their Internet cut off, if they are told that their identify theft is going to be significantly reduced, if they're told that their threat to their computer crashing or slowing down is going to be significantly reduced, and the threats to other people will be significantly reduced, so not many costs, lots of benefit, people are willing to pay up to $7.50 per month. On the other end, if you impose all the costs and very few benefits, people are still willing to pay about $1.50 per month for a little benefit and cost.

So people are willing to pay something for this. The question is what does $7.50 get you? We don't know because there's not good data out there on how much it costs to do what some ISPs are doing today, what some ISPs could do today but aren't, and what certainly the smaller ISPs you get to, which would be extremely

expensive for them to do because they don't have any of the capabilities.

So my main take-home here is we need more objective data. Conceptually this idea makes a lot of sense. But from a strictly cost-benefit standpoint, we need more information. And some of that information I think exists, both internationally and within the U.S., but some of it doesn't. Some of it needs to be collected. And the more we can do that and the quicker we can do that, I think that will help solve this problem faster.

MR. SCHWARTZ: So I've been asked to, in the last 30 minutes, been asked to cover the international side, and I'm going to do my best to make sure that I have everything right, although I didn't have time to check my work. But I know that Mike O'Rierdan, who works through the Messaging Anti-Abuse Working Group internationally with the different countries involved here, will stand up and correct me if I am wrong in any of these data, so -- because he's the real expert.

So I mentioned Japan. You know, I really was hoping that Yurie would be here because she really does have the best numbers out of anyone, any of the countries that are implementing in this space, not to say that they address the questions that Brent raised, but I do think that they at least start to move us down the path of showing that some of this works and showing what else we need to do to get to the specifics here to get better measurements.

So they have what's known as the Cyber Clean Center run by the Japanese CERT originally, at least set up by the Japanese CERT. And so it was a government-organized agency. I really do like the name actually, Cyber Clean Center, because you have this vision of Japanimation kind of thing with some computer going through and getting cleaned. (Laughter) And they do do commercials around it, too, so I kind of really want to -- I haven't seen those yet, but I want to see if they actually do do

that, put it through a car wash or something.

So it was set up by the government in cooperation with the ISPs, with the eight largest ISPs originally. They worked together to send people to this center where their questions were answered and they were able to get cleaned up. There's a lot of information up front and then if people need more they can call and interact with the center directly. That has now been -- over time they've been able to get more ISPs involved. I think it's something like 97 percent of the ISPs in Japan now participate. So they originally had the eight largest, so they already had most of the population covered with those eight, but now they have a much larger number of ISPs involved, including the small- and medium-sized ones, which I think is a good -- shows that people have seen benefit to this and being involved in this program voluntarily.

And that has now been spun off. They're in the process of spinning off the Cyber Center, so it's going to be run through the voluntary donations of the ISPs, membership fees from the ISPs, and not through the government anymore at this point. So it was sort of incubated by the government and now is done as a voluntarily, private sector-run program.

Australia has a program that's run by the Australian ISP Association, and they give notice -- well, the ISPs are given notice. The ISPs work together to come up with what is a code of conduct and they call it a code of conduct, a voluntary code of conduct that they've entered into where they will give notice. And then they send people to the same set of resources, online resources, to get information about how to clean their systems up. And it has actually a list of tools there for them to use.

Germany also works through the German ISP Association. They also have a -- first send people to when they notify -- when individuals are notified, they send them to a website. And then that website, if the person does not get clean, then they can

go back to their ISP. Their ISP will give them a ticket that they can use that ticket to call in once they've shown that they've actually gone and tried to use these resources.

So that's basically the three different models that we've seen. They're all pretty similar, but they have some differences around how active you can in calling and how much burden is on the individual, which Brent, you know, discussed the tradeoffs on that point earlier.

So with that, I'll pass it once since it's about used up my knowledge on the international side.

MR. BARNETT: Good afternoon. As Allan told you, I'm Jamie Barnett. I'm chief of the Public Safety and Homeland Security Bureau for the Federal Communications Commission. I really appreciate the opportunity to come and talk FCC's activities with regard to botnet and botnet remediation. And Dr. Friedman, thank you and the Center for Technology Innovation and the Brookings Institute for hosting this important colloquy.

So I've been at the FCC for a couple of years. The Public Safety and Homeland Security Bureau has been given the cybersecurity I guess you could say portfolio, but also we've always been about network reliability. When I got there we started a process of transforming one of our divisions and it's now the Cybersecurity and Network Reliability -- I'm sorry, Communications Reliability Division. And so while we are -- I guess you would say that the FCC, I don't think, will ever be in charge of any aspect of cybersecurity, yet I think we play an important role. And that role really stems, I think, from our traditional relationship with the folks who operate the networks and really the core of the Internet.

Because of our traditional role in network security and reliability, we really recognize botnets as a particularly nefarious threat. And certainly infected zombied

computers pose a risk to the owners on particular security, privacy, wealth, wellbeing. But at the macro level literally botnets are threats to economic security, public safety, the safety of public safety communications, and really to national security. And so that really is where it triggers FCC interest and responsibilities and that's why we're very committed to working closely with the Departments of Commerce, Homeland Security, with NIST, and other federal partners against botnets. We view it as a team sport and we want to be a member of the team.

So to be effective the initiative to remediate botnets must be coordinated across multiple sectors and it must recognize that government is not really the front line and does not control the front line. The front line is largely in the hands of commercial industry and Internet service providers, software developers, equipment manufacturers; even consumers must play a role.

And I would say, as others have up here, the FCC acknowledges some very effective efforts by industry stakeholders in this ongoing struggle. But there government can and I think should play where industry has a hard time acting together collectively, where the marketplace is not providing initial solutions or solutions fast enough. And I would submit to you that probably botnets may fall in that role.

Government action should be limited to least effective means, least restrictive means that can achieve effective results. And, quite frankly, the FCC has a long history of working with industry on best practices and helping coordinate industry solutions.

So I do feel very strongly that cooperative, focused, public-private partnerships, not mandates or regulations, will prove the most effective means in combating botnets. In furtherance of this goal we charged the FCC's previous Federal Advisory Council, the FACA, and this was the Communications Security, Reliability, and

Interoperability Council, so known as CSRIC, and in this particular case the previous one was CSRIC II, we asked them to compile a set of voluntary best practices covering botnet prevention, detection, notification, and mitigation. And the group also identified the means to address some crucial penumbral concerns such as privacy.

So that was delivered. And building on this work, working jointly with DHS, the Department of Commerce, and NIST, CSRIC III is currently developing a voluntary model which will detail methods ISPs can use to detect and remediate botnets.

We really have an outstanding group of experts from industry, government, advocacy groups, who are working on several cybersecurity projects, not just botnets, but -- and some of these of folks are in the office -- in the assembly here today, so -- and I'm going to drop a few names. Experts like Michael O'Rierdan of MAAWG fame; Rodney Joffe; Dr. Steve Crocker of ICANN; Ed Amoroso; Pete Fonash is working with us on this; Alan Paller; Barry Greene; and Professor Jen Rexford of Princeton, just really to mention a few. Ari Schwartz has been to speak to us. He's provided -- Donna Dodson, too, is to work on this from NIST. And so really having experts like this -- and there are many more because I didn't mention them all -- to work on this.

But for botnets in particular the information is being studied to create the model, and it includes relevant, you know, Internet engineering task force, requests for comments, the work of the Messaging Anti-Abuse Working Group, and the comments gleaned from the RFI. So the Departments of Commerce and Homeland Security's RFI really has asked extremely pertinent, salient questions on this topic. It's really a major step forward in the vast challenge presented by botnets. And we at the commission really fully support that effort. And we're especially pleased to hear that the responses to the RFI's questions identify steps even non-ISPs' stakeholders to the Internet community

can play to address botnets.

CSRIC is also evaluating the efforts undertaken within the international community, as Ari mentioned -- Germany, Japan, and perhaps especially Australia -- and their Internet industry code of practice, or icode, to determine applicability to U.S. ISPs and perhaps provide a potential U.S. framework.

We have asked CSRIC to identify potential obstacles that ISPs may encounter when attempted to implement this model and will establish the steps that the FCC and other federal entities can take to help overcome those obstacles. And you can expect the CSRIC to vote on this model in March of 2012, so this is coming up quite, quite quickly.

CSRIC will also work on recommendations for incentives to ISPs, which is the comments that we had earlier, to adopting this model. And those incentives, that report is expected in September 2012 or in that timeframe.

Now, this next one is important. We recognize that if a voluntary code of conduct is to a be of real and lasting value, there must be objective methods to evaluating its effectiveness. And this is, admittedly, a difficult assignment, but CSRIC will identify outcome or any performance metrics which will be used to evaluate how effective the code of conduct is in addressing the botnet problem. And these metrics are also scheduled to be available really next year.

Education and awareness are key components in fighting botnets. And I wholeheartedly agree with Michael Kaiser with educating consumers about the hazards that face them online, and really requiring them to take responsibility for maintaining a safe online environment is vital and key to the security of our communications systems. And I applaud the Stay Safe Online Initiative taken by the folks at the National Cyber Security Alliance.

Once again, I congratulate the Departments of Commerce and Homeland Security on the thorough and first-rate information that's being gleaned from this RFI. And again, thank you to the Brookings Institution for inviting me to participate in this discussion, and I look forward to our continued discussions.

MR. FRIEDMAN: Great. Thank you, Jamie. So I'm going to seize moderator's prerogative here and ask the first question of the panel, which is this challenge of collective action, where if it is going to be a private sector-led approach, what do we know about sort of related or past efforts of firms to work together, both in terms of the outside of government and then inside the commission? Is there notable successes we can point to? Are there lessons that we've learned? Are there notable failures where either people didn't work together or, perhaps even worse, they worked together, but didn't get anything done?

Can the panel speak to that? And Ari and Brent, I think you might have some thoughts as well.

MR. SCHWARTZ: I'll raise the three that we raised in our green paper in particular why we think this can be successful and then other people can raise the failures.

So in particular, we've seen really great success out of the work that MAAWG has done on spam in particular. I think that they've demonstrated that through a collective action you can make a difference in cutting down on the amount of spam that consumers see, in particular. So that's a Messaging Anti-Abuse Working Group.

Yeah, the Anti-Phishing Working Group, which has been successful in not only helping to cut down on kind of the bulk phishing attacks that we see out there, but also information sharing. Right? They helped to write IODEF, which is kind of seen as the way to share security information at this point through the IETF.

And then the third one is the Anti-Spyware Coalition, where we -- that basically helped to get rid of adware that was paid for by mainstream advertisers, which was a big problem, you know, six, seven years ago, and almost doesn't exist at all today in terms of that kind of adware. I mean, you'll see some malicious pop-ups out there, but not in the same way that we did six or seven years ago with -- that was funded by venture capital, et cetera.

MR. KAISER: Yeah, I would just add to that on the education awareness side, the Stop.Think.Connect effort was just such an effort as well, which brought together companies -- not only companies, but government, and a lot of government agencies and nonprofits, all who were already engaged in education and awareness, but were sending different messages out to consumers. And the ability to coalesce around a single message and use the available networks that they had and that they were already using on education and awareness to be a force multiplier for that message is really a critical way. And I think there are a lot of similarities here, especially when we talk about education and awareness on botnets that people can work together around, you know, a clean and simple message. One of the messages, actually, in the Stop.Think.Connect campaign is keep a clean machine, which seems absolutely appropriate to this discussion because that's what we're talking about.

MR. BARNETT: If I could use this non-cybersecurity example where I think there's successes on this kind of public-private thing where you can do voluntary things going forward, I mean, a predecessor to CSRIC was NRIC. And NRIC came up with best practices as basically industry groups, experts, advocacy groups coming together that had basically improved network reliability, come up with best practices on that. We've seen -- because we also understand the power of data, being able to come up with some metrics on that to kind of judge that we've seen sometimes as much as 50

percent increase in reliability in certain areas, and that can be from 911, any number of things like that. So this model, I think, can be very effective and that's kind of the one that we're approaching it, with this current CSRIC and the botnet remediation.

MR. FRIEDMAN: Then we can open it to the audience now if there are questions for the panel. In the middle in the back there, black jacket.

SPEAKER: So I'm the first one from the computer industry, I think, in the room that's stood up. I'm from Microsoft Corporation.

I'm curious, first, your comments, Mr. Barnett, on government helping to facilitate or accelerate progress amongst industry. I haven't seen too many examples. I'd like to hear a little bit more about how you can do that. I think the average program from government perspective, from buying and acquiring software to going operational is 81 months, but the iPhone took 21 months to develop. So I'm interested in that. And that's just more of an editorial.

I'm confused, however, on the sort of taking down a specific area of cybersecurity down to the type of attack and creating a pretty complex group of folks -- economists, think tank, industry, White House -- where some of the cyber command initiatives done by General Alexander and Cyber Command have tackled a lot of this stuff already. They're buying the same hardware as we're selling to our private sector. They're buying from Cisco and IBM and Microsoft. We don't have a DOD version of Windows. So they have tackled all these problems. I don't see the connection between the industrial strength that the DOD brings and the complexity of these disparate organizations you were talking about here today. I mean, a little clarity on that.

MR. FRIEDMAN: You want to take this or --

MR. BARNETT: Well, with regard to the FCC, of course, one of the things that we concentrate on, and I think other people have said it, the FCC is not going

to address the entire ecosystem because that's not really, I think, our strength. We deal with networks. We deal with pipes. And that's probably where we're going to concentrate. And there are examples where we have been able to accelerate and improving.

So, for instance, the example that I gave with the network reliability, I mean, because collective action among the carriers is called collusion, being able to bring them together with -- they report to us information that we can anonymize, we can analyze it, and we have results that indicate there have been significant increases.

You may remember the outage, the 911 outage that occurred in Montgomery County back in January this year. Because we were able to look at that, we had a great discussion with industry on that, they discovered a very unusual glitch, that it was not specific to that carrier and were able to spread that throughout the industry and increase that reliability. So those are the types of things that allow the power of data.

But I would say this, so, you know, we're concentrating on those things that FCC can do and not trying to branch out to things that we really can't.

MR. SCHWARTZ: I'm really going to challenge this notion. I think that it is completely unrealistic what you just said. Right? I mean, we're talking about home computer users and you're comparing them to soldiers and the computers that they use and the restrictions that the Army can put on and NSA can put on to its computer users, and you're suggesting that we put those same restrictions on home residential users.

SPEAKER: No, I didn't suggest that at all (inaudible).

MR. SCHWARTZ: Well, that's -- I'm just telling you what I heard back, which was how come the NSA can solve this problem for themselves and DOD can solve this problem for itself, and we can't solve this problem for the rest of the world? Right? There's a very easy answer to that question, which is you can solve a problem for a set of

people when you have very strong controls and very -- that you can place onto those individuals, individual users. It's just not acceptable to place those same kind of restrictions on home computer users, residential computer users, and it's not politically realistic to suggest that you can do that either. So when we're talking about the society as a whole as compared to a single institution, right, I mean, we have different kinds of things at stake here. That's why you see this complexity.

MR. FRIEDMAN: And just taking a step back in terms of why this is a policy priority, I think you can argue that in one -- this is a subset, and one might argue a somewhat small subset, of the cybersecurity threat we face. However, it has a couple of advantages. One, we can do it and, two, I think as Ari pointed out, in the process of doing this we will lay some of the foundation in terms of bringing the intermediaries together with the vendors, which I think is something that they're usually separate when we have cybersecurity conversations. So we're laying that groundwork.

And then finally on the national security side, it has been very hard in a diplomatic environment to push on certain things when all someone has to do is say, listen, we see where the attacks are coming from on our network and they're coming from IP space in your environment. So we won't eliminate that, but at least we can make it harder and more expensive, and I think that's going to work.

So I think your point is well taken that this doesn't solve everything, but I think it does make some substantial policy gains.

Other questions? Yeah, on the aisle here.

MR. TURNER: Francis Turner, ThreatSTOP. I have a question; you talked a lot about incentives for end users. But, in fact, the botnets basically are controlled through command and control hosts, which are hosted on hosting providers. That's a much smaller target. It seems to me the real incentive ought to be to take down

the hosting providers and the hosts, maybe unwittingly on the hosting providers that are -- providing the command and control host. Because if -- we know this works. I mean, this guy from Microsoft, he didn't mention Conficker, but Conficker Working Group that's exactly what it did, it took out the C&C hosts. Conficker is now a mostly dead problem. It's not completely dead, but it's mostly dead.

So what I'm saying is why shouldn't we be concentrating on taking out the -- you know, working with the hosting providers as opposed to the ISPs? I mean, the ISPs are doing a good job, but maybe the hosting providers are an easier target.

MR. FRIEDMAN: So who wants to solve bulletproof hosting?

MR. SCHWARTZ: We did receive an RFI that -- a response to the RFI that did mention the stop adware, raised this point. I think that's it a completely legitimate point to say that we should be spending time on hosting providers and I think that's something we could look at in the future. You know, this is sort of a one-at-a-time kind of problem, especially if we can show some success in this space, we think that it could be helpful down the road in that way.

One benefit of looking at this side is the end user equation, which is can we build an ecosystem where people feel more responsibility for security, et cetera. And this gets somewhat at that problem. Hosting you have that same situation, too, but, you know, we have to see whether -- what the best practices are in that space and how to get at it.

And it's great that the industry groups have already been forming around and trying to solve that problem, too, together through collective actions. So there already has been some collective work in that space, which we need to build on -- to monitor and build on and see how government can be helpful in that way, if we can be, so.

MR. FRIEDMAN: Anyone else on the hosting side?

MR. ROWE: No, I would just say in general we should always try and stay away from thinking there are any silver bullets, right? I mean, I think that's part of the issue and then that actually tears us apart as opposed to bringing us together. I think we have to put all the possible potential solutions on the table and work towards all the ones that we think will be beneficial. And I think that's one of the reasons that people should come together to work on it as opposed to, say, oh, you know -- as opposed to saying, you know, I have the ultimate solution over here. Because getting people -- I actually think it's harder to get people to all agree on somebody else's solution than to sit down together at a table and come up with a solution collectively. And that's what we need to do, I think, on this issue and I think we'd make a lot of progress.

MR. ROWE: I think that's a great point. I think unfortunately, though, that made me think in this case that's going to be one of the big problems. Because once you go to home users and say we're going to make you more secure, they're going to think 100 percent security. Right? And so I think that's going to be a problem with this whole effort that you're really going to have to find a way to communicate that we're not making 100 percent secure, but it's going to be better, and that's going to be difficult.

MR. SCHWARTZ: Can I just -- I think we're actually already there. I think actually home users already have a false sense of security. I think small businesses already have a false sense of security. So I don't think that we will actually exacerbate that problem, in all honesty.

MR. BARNETT: Because they've got an AV. I've got an AV, so I've got the umbrella that I need, is that what they think?

MR. SCHWARTZ: Well, that or they don't think that they're going to be a target. They don't think they have anything that's worth stealing. I mean, you know, it's

-- and by the way, that's not only limited to the cyber world. I mean, in regular crime world people often think they don't have things that are worthy of criminals come taking and those kinds of things, so I think we already have some of that built into the system, but we've just got to like, you know, grin and bear it and know -- and I think that has to be part of the messaging is that no one's ever 100 percent safe and secure. It's true when you drive a car. It's true when you're on the Internet. It's true when you walk across the street. So, you know, it's part of our society. So I think we can deal with that.

MR. ROWE: You know, I agree. Just a quick point. The psychology behind all this is going to be very important, though. I think a lot more work needs to be done on how to communicate to people clearly, and, yeah, I don't think enough's been done in that area.

MR. FRIEDMAN: So we also need to solve the problem of American citizens understanding risk. Okay, we'll put that on the list. (Laughter) Yes?

MR. MARGOLIS: Hi. Joel Margolis with Subsentio. I'd like to know if the panelists think that we need best practices in data retention so that IP logs are available to trace back the origin of botnet attacks.

MR. FRIEDMAN: I don't want to go on record.

MR. SCHWARTZ: Well, I mean, I'll point you to the IETF spec right now that helps people to figure out how -- that the ISP's information without going into great detail, without doing longer than usual practices for data retention. There are already ways to do this today. So I'm not quite sure what benefit -- if you were implementing what is the best practice out there in this space, what benefit longer data retention would bring.

Also, I mean, we have this issue with law enforcement. Mark Sachs mentioned earlier about the importance of law enforcement. I completely agree. There is

this tension that where they get the information, right, they know where the botnet is, but they don't want to have people take it down until they've finished their investigation and finished bringing the case. So we have to figure out ways to be able to share information and still allow law enforcement to do its job. I think that's more of a challenge than the data retention problem is today.

MR. FRIEDMAN: A question in the front here.

MR. SACHS: Thanks. Mark Sachs, Verizon. Just a request. I think we're zeroing in on users being absolutely centric towards the next thing we need to do. It's clear that users clicking on things, opening attachments, installing badware, there are roles for ISPs, there's roles for software, there's roles for everybody. But to get at that user, to get them aware, one of the quick things the government can do -- and I would invite the two gentlemen from the government to at least think about this and pontificate a bit -- could the government do a campaign, an awareness thing, much like Smokey Bear, Click It or Ticket, any of these things that we see nation to nation -- or nationwide that says this is a problem? It's a problem facing our nation. It's a problem, only you can prevent botnets, or whatever you want to come up with.

And if we do a lot of work through Stay Safe Online that's great, but I don't see the federal government in its bully pulpit role really stepping this up and saying we have a national problem and we need your help as users to think before you click, Stop.Think.Connect, or whatever words you want to use. But we can do that right now. We don't have to have meetings about this. This can happen almost immediately.

MR. BARNETT: So this is the first time I've ever been asked to pontificate, so I appreciate that. (Laughter)

Mark, I think you're right. I think it's a great idea. The FCC certainly has had situations where it has chosen to do consumer education through our Consumer and

Government Affairs Bureau and other ways to do that, getting word out, and things like that. We've had fairly significant I guess you could say public information campaigns, whether it was the DTV or even with the recent Emergency Alerting System nationwide test which we had. Our budget for that was zero and yet we were able to get the word out by working with the EAS participants, the broadcasters and things like that.

So I think you're right. I think there is definitely a role with that in working. That's part of that public-private partnership, I think. And other parts of government probably would have a bigger role in that than the FCC.

MR. SCHWARTZ: Well, I'll tell you, Andy Purdy has got his hand up and he's like really anxious about this. This makes me nervous to comment at all.

But I would say, you know, one of the things I like about this particular issue that you're doing the education, two people who are infected who don't realize that they're infected. Right? So I think it's the timing of it works a lot better. I think one of the things that --

MR. BARNETT: Relevancy, yeah.

MR. SCHWARTZ: Yeah, so it's really relevant and we can get the message across directly to the individual. So that's one of the things that excites me about this particular effort around education.

I also like the work that Stop.Think.Connect has done in K through 12 because I think that, you know, as people use more -- it's almost easier to educate kids around it than it is to educate their parents around it. So having a campaign, the Smokey the Bear campaign, I think is a good idea.

One of the things we say in our green paper around the educational efforts is talk about places where we haven't done measurement, right, we have no idea what works for cybersecurity measurement, at least not -- we asked people that question

in our green paper, in the RFI for our green paper, what education efforts work? We got no response to that -- pretty much no response to that question. Now, Michael may say that work's being done on that, but we still haven't heard, so how do you start a campaign without knowing at all where to start beyond what is logical? And that's why we're starting -- kind of aiming at things that are logical first and then we can talk about metrics on this down the road.

MR. KAISER: I just have to respond to that in a couple different ways. One is when you talk about something like Smokey Bear, right; you're talking 40, 50 years. Right? That campaign has been going on for 40 or 50 years. So things like Stop.Think.Connect have been going on for 14 months. Right? So, you know, we are in early days. And to have a -- to create a cultural message, right, which is what you're talking about here, a message which applies equally to every single member of the community no matter where they sit or stand or walk or drive, is a long-term investment by all the players who participate in that effort. And you have to do it, you have to stick with it, you have to stay with it over a long period of time and it has to be drilled down from more than one place. It can't only come from government. It can't only come from industry. It can't only come -- it has to come from parents. It has to come from school teachers. It has to come from older siblings. It has to come from everybody in order for it to become that kind of universal message which we all agree people need to have.

I will say actually, you know, in these international models there were large investments in education. I believe both in Japan and Germany at least, I'm not sure what happened in Australia, they made large investments in education as a core piece of that effort. And I think that's a good lesson learned.

MR. BARNETT: You know, 40 or 50 years of Smokey Bears and we're still having forest fires, too.

MR. ROWE: And one other comment on that. Yeah, it was actually Smokey the Bear is a good example of a campaign that had the wrong slogan for 30-some years. I mean, they were saying no forest fires instead of no wildfires, so that cause a lot of problems. So you don't want to do this too quickly. But I think studying what these guys are doing with Stop.Think.Connect really rigorously is a first step to seeing how well that's working. Certainly, you know, it's not all over TV or anything like that, but, you know, so you have a scale issue there, but at least seeing the impact for people that do see it and understand that and then thinking about it, I don't think you want to jump and just throw something up on the screen not knowing if it's going to have any impact or the impact you want.

MR. SACHS: Before I notify a customer I need to know why I'm notifying (inaudible).

MR. FRIEDMAN: So Andy in the back.

MR. PURDY: Yeah, Andy Purdy with CSC. It's a pleasure to just fundamentally disagree with Marcus, my good friend. (Laughter) I think the lesson that we've got to learn from the last few years -- and frankly, I saw an unclassified briefing by the National Counterintelligence executive earlier this year, an unclassified briefing by the CIA earlier this year. If we think an awareness campaign is going to deal with the significant threats we face, we are crazy.

Let's do it, fine, Kumbaya, great. But the lessons that we're learning from the Australia icode experience, the lessons we're learning from the Cyber Clean Center in Tokyo, and, frankly, the lessons from a financial perspective, Brent, I think we can learn from our experience with financial institutions, where financial institutions have created an incentive system where the individual customer is not held liable if there is an online theft against their account. And the banks are using user name and password,

even though they know there's malicious software on a lot of their customer's computers. They know a lot of their customers are being used as bots. And because the customers are going to get reimbursed, the customers don't care.

So this initiative by Commerce and DHS and the White House is sorely needed because it's not just looking at attribution. It's not just looking at getting the individual user to do something. It's looking at the enablers. It's looking at the ISPs. Because right now legally and ISP is responsible. If an ISP contacts another ISP and says one of my customers if being hurt by one of your customers, that ISP has to do something, not because of the government, but because of the terms of use, the agreement between ISPs and the customers and the agreements between the ISPs.

And so the lessons we're -- this initiative and, frankly, the efforts by DHS and the other agencies, the cyber ecosystem effort, the National Strategy for Trusted Identities in Cyberspace, this is very exciting initiatives. And so I think we need to support this. We need to support it wholeheartedly, do all the awareness we want, particularly when we're talking about these experiences. And I think, Brent, I don't know if you want to comment on the economics of it, where the customer gets notified, then they can do to a website and then there can be folks who can help them, than can help clean up the system. That's what's going to help make us more secure.

MR. ROWE: Well, certainly I don't think anyone up here is saying that we need to -- we need to motivate end users. We don't necessarily -- I don't think we're going to be successful at teaching them very much. And that sounds not very nice, but I don't think we should try to make anyone who's not already a cybersecurity expert become one. I think we should make it easier for them to find expertise. And I think that's a critical point here.

If we notify people -- and that's a big problem with this whole scenario is

that if we don't have enough techniques, enough places to point people, enough call centers and/or websites that work for 99 percent of people, this whole thing isn't going to work if there's any assumption that people need to act on their own.

The bank example, and I guess it's not quite as relevant for the discussion here, but certainly for NSTIC, I know banks, you know, really want to move -- find some way to get people to care and right now they just don't have it, so they're really clamoring for something like NSTIC. So that was another great point.

MR. FRIEDMAN: So question on the aisle here.

SPEAKER: I have a really naïve question. As a residential user how do I know if I'm infected by a botnet or other sort of malware?

SPEAKER: Run the program with us.

SPEAKER: We have an app.

MR. FRIEDMAN: Well, we try to avoid endorsing specific solutions here, but I think the policy approach is, in fact, to address that very problem. I don't know if anyone wants to say something particular.

MR. KAISER: I would just say, you know, that the world has changed. You know, five years ago people would have said that your computer would have slowed down, that you would have been getting all these kinds of, you know, pop-ups and other kinds of things, and that doesn't happen anymore. This stuff is very stealthy and underneath. So you have to take the basic precautions that you would take in general, you know. You have to have a good suite of security software. You have to have an up-to-date browser. You have to have an up-to-date operating system. And that's where you start. And actually that's going to take care of a bit of it, not all of it, I think, you know, in the same way just when you get in your car and you put on your seatbelt and you make sure your anti-lock brakes are working. It's not going to prevent you from being in

an accident; it's just going to make sure that if something happens you'll be a little bit safer.

So you've got to start there and that's what this discussion is really about. There may be ways to help people find that out and then, I think as people are saying, point them to places where they can get help and fix it. And I think that's a terrific move forward to clean up the ecosystem.

MR. BARNETT: You might be able to ask your ISP.

MR. FRIEDMAN: So I think I may jump in with another question here, which is the challenge Brent alluded to of perhaps unintentional consequences. And I was curious if anyone on the panel had thoughts about that or perhaps sort of moving forward, assuming that this initiative is quite successful, the one thing we've learned about cybersecurity is that, in terms of the ecosystem metaphor being very relevant, is that attackers are adaptive. How might we expect the bad guys to react to this type of initiative in terms of moving things internationally, in terms of changing their behavior, changing their business model? What can we expect?

MR. ROWE: Yeah. I think -- well, so certainly, like we talked about earlier, there are groups in the U.S. and there are groups internationally that have lowered the cost for a lot of these different things that need to be done, but the biggest up-front problem is, are you going to raise the cost of service, right? If you're going to raise the cost of Internet service, then you might have people dropping off and, you know, we're trying to shrink the digital divide versus expand it, so that's a problem.

I think, though, not to say obviously we should worry about kind of the future and what happens once this is all in place. But if you raise the cost, if you raise the overall cost for people to go after it, to create bots, then you are necessarily going to have fewer bots. You're going to have fewer people at least -- excuse me, I should say

that differently. You'll have fewer people involved in creating bots, at least in the beginning. Now, that may change and there might be a whole other set of solutions we have to come up with, but by raising the costs I think you're only moving in a positive direction.

MR. FRIEDMAN: All right. Is there --

MR. SCHWARTZ: You know, we could see a lot of -- I mean, it's impossible to know what terrible thing will happen next, right? So --

MR. FRIEDMAN: It's fun to speculate, though.

MR. SCHWARTZ: But, yeah, I know, that's what you guys do around here, right? (Laughter) But you can -- but I'd say one thing about some of the things we're talking about in terms of incentives and in terms of information sharing is that you hope that you -- if you can get the whole Internet ecosystem, right, working on a particular problem and you get more information shared among each other and ways to do that, that you're going to be able to take on new problems. I think the Anti-Phishing Working Group that I've mentioned before, that when they created their processes for sharing information about phishing websites opened up the door to more kinds of sharing for a whole bunch of different kinds of security -- types of security information by making that extensible to other types of attacks. So that's the kind of thing that comes out of this kind of solution. So I think, you know, as things change, you know, you hope that you can adapt and bring whatever institutions or whatever memory comes from this towards going after the new attacks as well.

MR. FRIEDMAN: All right. I think we have time for a final question here.

MR. BURNS: Tom Burns with ThreatSTOP. I was actually hoping MAAWG would do this. This is to Brent really. It goes to what do you do once you've identified it?

So ISPs are -- currently AT&T is identifying people and saying you're botted and we're disconnecting you. In the Netherlands it happens; if you're botted, you're disconnected and then you have to go clean yourself up. MAAWG estimated that if only 100,000 people did that, that would cost $150 million a year and that's just to identify them and notify them.

The cost of remediation is extremely expensive. We did a live demo at ISSA. Forty-eight percent was what (inaudible) would do. So how do we address the economic background? People are going to get infected. They're going to get notified. How do we deal with that cost and who bears it?

MR. ROWE: That's the exact right question to ask. And there's not a perfect answer, but I will say the identification, I think, at least I hear, is one of the lower costs, at least for ISPs that are, you know, fairly big ISPs. The smaller ones we've got to put in a whole separate box and deal with them kind of differently I think, but -- so put that to the side. Notification and remediation, those are the two big costs factors, I think.

Notification, you know, you've got to, I think -- I hadn't even thought of some of the things IETF had in their write-up. You know, you've got about 15 different ways you can notify people, the most common being e-mail, mail, and phone, and they all have their own problems. Phone calls, people don't answer and they may not believe you. They may think it's telemarketing and hang up. E-mail, you've already seen lots of phishing attacks and so that has its own problem. And mail is costly and somebody could potentially intercept. So there's not a clean way to do that. But that is -- if you separate that out completely and say -- I mean, one option is to say ISPs only identify and that's it. And then they pass it off and then some kind of public-private partnership or government-funded group does the notification, and they do that as streamlined as you can. You know, if you're notifying everyone's that's infected from all ISPs, it's coming to

a central place, then their costs per person are going to be lower than each individual ISP doing it.

The remediation at least there seem to be a good number of automated techniques out there that help. Now, the number of types of botnets that those solve, I don't know and I don't know what percentage you can get up to with automated techniques, but that's certainly the best approach to for there. There's a website you can send somebody to and you just, you know, can automate it from there and you don't have to call them or talk to them. Then you cut those costs down dramatically. But the question is what's left? What fraction of people are left after that? Is it 5 percent, 10 percent, 15 percent? And that's where the big cost is, right? You said 50-some percent?

MR. BURNS: (inaudible)

MR. ROWE: I mean, if it's 50 percent of people that are going to have to call in and somebody's going to have to step them through it, that's a huge cost. So getting that automation as high up the threshold as you can and then if you can't get it high enough that the total cost for an average user is small enough, then, again, I think that's a role for government to potentially be involved because that cost is now not something that they can sustain without raising rates on users, and then you have issues related to that. But understanding where those thresholds are or where they could be in a year or two I think is critical.

MR. SCHWARTZ: My understanding is that Germany's numbers actually are lower than 52 percent. I don't remember if anyone -- I don't know if anyone knows those off the top of their head or seen the data, but my understanding is that it is lower. I mean --

MR. BURNS: That's the number that (inaudible).

MR. SCHWARTZ: Okay. Well, that's a different story then. But -- well,

in terms of the directions that they give to individuals, that Germany gives to individuals that need to call into the call center -- because remember they have to go back and get the ticket -- that percentage was lower than -- from what I've heard from the Germans on this, that number is lower than 52 percent. It's more like 25, 30 percent.

SPEAKER: It's (inaudible).

MR. SCHWARTZ: Twenty-eight percent? See, I was close, Germany says. So 28 percent, that's high. I mean, 28 percent's high, but it's not 52 percent. And that shows that you can do targeted education in a way where people respond positively.

So then the question -- there is this question about the cost of the 28 percent that are leftover from that, and I think we need to, you know, figure out ways to go about addressing that, get better at it. I do also think that Brent's study shows people are willing to pay for it, right? And if they're willing to pay for it, then the cost goes to the consumer. And I think we can come up with ways to incentivize people to do that so that they don't have to go through this again and again. Right? I mean, they bear the cost either way, right? Are they willing to pay for it and make it clear and then do prevention down the road or does society have to pay for it and then we figure out other ways? So, I mean, that's really what it comes down to.

MR. ROWE: And, I mean, telephones are, you know, an example of that, right? You've got all these fees underneath at the bottom of your telephone bill. What if, you know, you had $1 or $1.50 and that's security. Right? Yeah.

MR. FRIEDMAN: Jamie's not going to comment on that. (Laughter) I think it's also important to remember that targeted interventions do have externalities, so, you know, when police come and arrest someone for doing a bad behavior that minimizes the behavior inside that social context; people tend to stop doing that. And similarly you can imagine that people will say, listen, I, you know, got this message and

that's going to promote the broader message of cybersecurity education and awareness.

So unless there are last words from the panel I'd like to thank you all for joining us today and particularly thank the panel of Sameer and Bruce, Michael, Jamie, Brent, and Ari for stepping in and serving on two panels. (Applause) So thank you very much.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

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

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2012