112th CONGRESS
1st Session

Printed for the use of the
Commission on Security and Cooperation in Europe

ANOTHER BRICK IN THE WALL: WHAT DO DISSIDENTS NEED FROM THE INTERNET?

MAY 18, 2011

**Briefing of the
Commission on Security and Cooperation in Europe**

Washington: 2012

Commission on Security and Cooperation in Europe
234 Ford House Office Building
Washington, DC 20515
202–225–1901
csce@mail.house.gov
http://www.csce.gov

Legislative Branch Commissioners

HOUSE
CHRISTOPHER H. SMITH, NEW JERSEY, *Chairman*
JOSEPH R. PITTS, PENNSYLVANIA
ROBERT B. ADERHOLT, ALABAMA
PHIL GINGREY, GEORGIA
MICHAEL C. BURGESS, TEXAS
ALCEE L. HASTINGS, FLORIDA
LOUISE MCINTOSH SLAUGHTER, NEW YORK
MIKE MCINTYRE, NORTH CAROLINA
STEVE COHEN, TENNESSEE

SENATE
BENJAMIN L. CARDIN, MARYLAND, *Co-Chairman*
SHELDON WHITEHOUSE, RHODE ISLAND
TOM UDALL, NEW MEXICO
JEANNE SHAHEEN, NEW HAMPSHIRE
RICHARD BLUMENTHAL, CONNECTICUT
ROBERT F. WICKER, MISSISSIPPI
SAXBY CHAMBLISS, GEORGIA
MARCO RUBIO, FLORIDA
KELLY AYOTTE, NEW HAMPSHIRE

EXECUTIVE BRANCH COMMISSIONERS

MICHAEL H. POSNER, DEPARTMENT OF STATE
MICHAEL C. CAMUÑEZ, DEPARTMENT OF COMMERCE
ALEXANDER VERSHBOW, DEPARTMENT OF DEFENSE

ABOUT THE ORGANIZATION FOR SECURITY AND COOPERATION IN EUROPE

The Helsinki process, formally titled the Conference on Security and Cooperation in Europe, traces its origin to the signing of the Helsinki Final Act in Finland on August 1, 1975, by the leaders of 33 European countries, the United States and Canada. As of January 1, 1995, the Helsinki process was renamed the Organization for Security and Cooperation in Europe (OSCE). The membership of the OSCE has expanded to 56 participating States, reflecting the breakup of the Soviet Union, Czechoslovakia, and Yugoslavia.

The OSCE Secretariat is in Vienna, Austria, where weekly meetings of the participating States' permanent representatives are held. In addition, specialized seminars and meetings are convened in various locations. Periodic consultations are held among Senior Officials, Ministers and Heads of State or Government.

Although the OSCE continues to engage in standard setting in the fields of military security, economic and environmental cooperation, and human rights and humanitarian concerns, the Organization is primarily focused on initiatives designed to prevent, manage and resolve conflict within and among the participating States. The Organization deploys numerous missions and field activities located in Southeastern and Eastern Europe, the Caucasus, and Central Asia. The website of the OSCE is: <www.osce.org>.

ABOUT THE COMMISSION ON SECURITY AND COOPERATION IN EUROPE

The Commission on Security and Cooperation in Europe, also known as the Helsinki Commission, is a U.S. Government agency created in 1976 to monitor and encourage compliance by the participating States with their OSCE commitments, with a particular emphasis on human rights.

The Commission consists of nine members from the United States Senate, nine members from the House of Representatives, and one member each from the Departments of State, Defense and Commerce. The positions of Chair and Co-Chair rotate between the Senate and House every two years, when a new Congress convenes. A professional staff assists the Commissioners in their work.

In fulfilling its mandate, the Commission gathers and disseminates relevant information to the U.S. Congress and the public by convening hearings, issuing reports that reflect the views of Members of the Commission and/or its staff, and providing details about the activities of the Helsinki process and developments in OSCE participating States.

The Commission also contributes to the formulation and execution of U.S. policy regarding the OSCE, including through Member and staff participation on U.S. Delegations to OSCE meetings. Members of the Commission have regular contact with parliamentarians, government officials, representatives of non-governmental organizations, and private individuals from participating States. The website of the Commission is: <www.csce.gov>.

ANOTHER BRICK IN THE WALL: WHAT DO DISSIDENTS NEED FROM THE INTERNET?

MAY 18, 2011

PARTICIPANTS

ANOTHER BRICK IN THE WALL: WHAT DO DISSIDENTS NEED FROM THE INTERNET?

MAY 18, 2011

Commission on Security and Cooperation in Europe
Washington, DC

The briefing was held at 2 p.m. in room 2218, Rayburn House Office Building, Washington, DC, Shelly Han, Policy Adviser, Commission on Security and Cooperation in Europe, moderating.

Panalists present: Shelly Han, Policy Adviser, Commission on Security and Cooperation in Europe; Kathleen Reen, Internews; Robert Guerra, Freedom House; and Rebecca MacKinnon, Global Voices, New America Foundation.

Ms. HAN. Good afternoon. I want to welcome you to a briefing by the Commission on Security and Cooperation in Europe. And I'm glad that we're having this conversation today. But frankly, we could have been having this conversation about 500 years ago with the advent of the printing press, or maybe a hundred or so years ago with the telephone, or cassette tapes in 1979 in Iran, or fax machines in 1989 in Tiananmen Square.

You know, we're at a point in history where we have game-changing technology. And it's a game changer definitely in the way that we do business, the way we socialize and the way that we get information. And we certainly believe that there's a role for the United States to play in making sure that the Internet is as free as possible, in particular for those who live in countries that are highly restrictive in other areas of their lives.

The Chairman of this Commission, Representative Chris Smith, has been at the forefront of the fight on this issue and is working on new legislation to address these current threats. And we know that the Internet has played a role in both successful and unsuccessful popular protests in recent years.

But I want to go back a few years to 1997. And there was a study by the RAND Corporation that I thought was particularly topical for our discussion today, and that is at looking specifically at the question of communication and democracy. The RAND study looks at what is called the dictator's dilemma and specifically how much communication can be allowed before we reach the tipping point toward democracy.

But I'm not going to answer that question right now; I'm going to let our panelists weigh in first, and hopefully, through our discussion today, which will include some questions from the audience—so you can be thinking about that while we're talking—that we can maybe reach some conclusions on that question.

We've put the bios of the speakers over here on the table, so I won't go into those. But we're going to start first with Robert Guerra, who's from Freedom House. No, I'm sorry; we said we'd start with Kathleen Reen—I'm sorry. We'll start with Kathleen Reen from Internews, then we'll go to Robert Guerra from Freedom House, and then Rebecca MacKinnon with the New America Foundation.

OK, Kathleen, go ahead.

Ms. REEN. Thank you, Shelly, Congressman Smith and to the Helsinki Commission for giving us the opportunity today to share our experiences and learning. When Shelly first asked us to talk about this issue today, she was reflecting particularly on events subsequent and in the wake—and the continuing story of what is happening in the Middle East, and some of the lessons that have been learned and bringing us up-to-date onto these questions. So building on 500, 100 years ago and in the last 60, 90, and 120 days—some extraordinary changes in global communications and lessons learned for those in civil society, in government, activists, dissidents, everyone who uses the Internet or who uses a mobile phone.

We believe in an open, accessible, unfettered and affordable Internet for everyone. And if only everyone else believed the same thing, and if only it were that way; unfortunately it isn't.

There are more than 1.9 billion people in the world who get regular access to the Internet today, and there are two real critical issues in addition to those who get that access: There are those who don't receive it at all, and there are those who, when they do, are in danger as they access it or cannot access unfettered information.

There are four ways in which we recommend and seek to ensure that access is built and promoted across the Middle East and everywhere where censorship is most acute. The first is to encourage what we call tool development: The use and promotion of technology is absolutely critical to increasing access to the Internet, particularly a censored Internet. The continued investment in those tools is absolutely vital. We believe that there is no silver bullet, that there must be a continuing growth and availability of international tools and locally available tools that are constantly adapted to keep up with what we know and call the cat-and-mouse game in censorship and in access.

We believe in education and outreach. A phenomenal number of people around the world today and perhaps in this room don't understand how their Internet works, how their mobile phone works, and just how vulnerable they are as evidenced by what has happened in various countries in the Middle East in recent weeks and months.

This is an issue that is not particular to the Middle East, but to everyone and every citizen in the world today. We believe that digital safety and digital security, and appropriate investments in those, are absolutely essential to ensuring that citizens everywhere are safe and can safely consume, create and share information.

We believe that R&D, research and development, is an absolutely vital and important piece of staying ahead of censors and authoritarian regimes who continue to crack down on the Internet. Without that investment, we will lose, and citizens around the world will have access to less information over time.

A particular area of that investment needs to be in mobile technologies. Every day more and more people around the world are getting access to mobile. And, for most citizens in the world, mobile is in fact their key form of communication. Most people do not have access to a laptop or a desktop, and most people don't have access to Internet cafés

either. It is the mobile phone and increasingly the smart phone that is the tool of choice and the tool of access and, perhaps in some cases, the tool of endangerment for those who are accessing the Internet.

This is a growing field. It's a new area in terms of accessing and using circumvention tools or building technologies and making them humanly available and accessible. It's growing rapidly, and it needs additional and more support. Until now there probably has not been enough investment to ensure that that growth and that those issues are being dealt with adequately, and we strongly believe that more needs to take place in that space in order for that to happen.

As an umbrella set of issues to ensure that more people have free and unfettered access to the Internet, I wanted to reflect very briefly on what's been happening in the Middle East. First of all, one of lessons we've learned is that network security—that the very structures that people use and the technology that is used to actually build it—is vital. It has to be open; it has to be safe; and it has to be secure. So a safe and accessible telecoms environment that is kept open at all times is very important.

We believe that enhancing security is essential. Many networks around the world aren't as secure as they should be right now, and it's individuals and organizations, particularly at the civil society level, who are the most vulnerable. Education and training for them and stronger networks at an ISP level and at a structural level is essential.

We also believe that supporting the fundamental freedoms of the Internet and access to information must be considered going forward. For that to happen, a truly global, open and free Internet has to be built, and it involves truly multidisciplinary intersectional work. It involves the work of governments and civil society activists, and actors and organizations. It involves national security departments and elements around the same table solving the complex problems of how to build a truly open Internet. So a legal framework and policies also instituted at the sovereign level are absolutely essential. Thank you.

Mr. GUERRA. Thanks. Good afternoon, everyone, and thank you. I personally would like to thank Shelly, Representative Smith, and the Helsinki Commission for giving me and my colleagues an opportunity to brief you on—of our thoughts on what could be helpful going forward. I'm going to very briefly talk about some of the work related to Internet freedom that I and my colleagues do at Freedom House.

We recently put out a report on the state of Internet freedom; we work on technology support for activists that are on the ground. I actually work around issues related to policy.

I think what's important to recognize—before we get into kind of the issues of the Middle East and when we're talking about Internet freedom—is, what is it exactly? We need to have some sort of definition. And we'd say that in any issues that the administration or Congress is—a strong definition of Internet freedom is key.

We take a kind of generalist approach, and just want to have a conversation so we could think about it in terms of techniques that are used to control and censor the Internet. We could think about the main threats to Internet and digital media freedom, and we could talk about positive and negative trends and trying to assess that in some way.

Without getting into the details of our Internet freedom report, the way Freedom House looks at it in their analysis is, what are the obstacles to access—and so how available is the Internet, mobile phones in different parts of the world, and how complicated

or how costly it is; what are the limits being placed for people to be able to use that technology to create content; and what are the violations of user rights. And that's a framework; other people have slightly different ones. In the report that we did, our highest-ranking top three countries was Estonia, the United States, and Germany, and the bottom three were Cuba, Burma, and Iran.

But getting into the issue of civic activism and some trends and some recommendations for the folks here is to recognize that the use of technology for activism is not something particularly new. If we just go back, you know, 50 years, samizdat in the Soviet Union—posting of notes everywhere and sharing it between people—is a modern version of Facebook, except the intermediary were people's homes, was a piece of paper. In parts of the world where the Internet is not very developed, there's a term that may not be familiar to some of you called sneakernets, which is basically people with sneakers go from house-to-house to share USB drives and content. And the most common quoted example is Cuba, but it was—the term was first used in Serbia when it was part of the former Yugoslavia in the way people used content.

Now, it's Facebook, and what with there—a lot of focus is on the Middle East right now. One of the first examples that Facebook was used for social mobilizing was Colombia, in the "million voices against the FARC." That did a lot to change the environment in Colombia. And we have other services such as microblogging services that were used not only in Tunisia and Egypt but also in Moldova. And we also have other technologies where—not necessarily the Internet, but are increasingly merged with it, like SMS. And I would say that activism in the past was also traditional media like radio and TV that more relayed a message to people.

In terms of repercussions and how states are responding, you know, this is something that we need to monitor; and increasingly, governments are using general media, legislation, to try to go after organizations and individuals, and starting to develop very comprehensive Internet-specific legislation that will target the use and the innovation that can happen.

What's very worrisome—and I'll get into more details in a second—is what Freedom House and many others have called technical violence. It's not necessarily going after activists, but going after where their content is hosted—so hacking, DDoS attacks, surveillance, cyberespionage isn't something that's just directed against governments, against the military. Increasingly, NGOs are facing these very same risks.

And so to understand this a little bit, let's take a look at—very quickly—kind of the evolution of what I call, kind of, Internet repression.

If we go back in terms of—Shelly mentioned efforts by Congressman Smith and others—if we go back 5 or 6 years, when we're talking about Internet repression at the time, or what I call Internet repression 1.0, it was really focused on Internet censorship—what governments and others were doing to block sites—and that was it. So it was around defining sites that are harmful, creation of software and hardware that would block sites, and that was it.

Internet users, foundations, governments started supporting the use of the Internet, and the activists had the edge. The governments are now reacting, and we're in a stage on what I would say is around Internet repression 2.0, which is where governments are very actively responding to the great liberating potential of the Internet, and they're not just blocking websites; they're being incredibly more sophisticated. They're using the cloud

or users to try to identify content and delete it; they're turning off telecommunications infrastructures, as has been the case, not only in Egypt and Libya but also Burma and Iran.

The technical attacks are getting even more sophisticated everyday where targeted malware that we were first seeing in China, is also finding its way to Egypt. And DDoS attacks are targeting a variety of organizations both in the Middle East and abroad. And censorship has evolved to not just be a whole website but a particular section of the website; and censorship that only really activates in a particular moment in time when it's more critical, whether it's around elections as we saw in the Middle East, in Egypt in November and elsewhere. When there's civic mobilization, when there's protests, governments will turn off the Internet; leave it on otherwise.

Got some photos, which I'll share, in terms of how this looks like. But I would say we're now shifting beyond this to something that's even more scary Where folks here in Washington might be able to be helpful is, given that governments are getting more sophisticated in blocking and censoring and attacking websites, there's now a whole industry that's spawned to support Internet repression. So I would say that we've moved on to Internet repression 3.0 where now companies want to get into the game. The list of companies includes both U.S. and foreign companies; I'll go through a couple examples.

Gamma International, a U.K.-German company, has most recently been discovered, through the raiding by civil society in Egypt of the state security archives, of providing technology to the Egyptian Government that conducts covert surveillance and targeted malware, which is very difficult to detect. Not only was there a commercial offer found in the state security archives but also an 8-month free trial was offered to the Egyptian authorities and which is—this is why a lot of the Egyptian activists found their conversations in the state security archives. And these are activists that are very smart, that had received a lot of training; but when malicious malware is there, it's very hard to detect.

We have NORIS, which is a California-based company owned by Boeing, that develops deep packet inspection technology which is used for a variety of legal purposes here in the United States. But when all the features are turned on in countries where there's no due process, it can be used to conduct real-time interception of email, social network traffic, and to report that back to any operator that has that.

Research in Motion, famously the maker of the BlackBerry, is increasingly collaborating and drafting agreements with countries around the world, including Saudi Arabia, the Emirates, and India, where they're allowing for surveillance of noncorporate communications. Well, activists are not corporate users; they do not have access to the security infrastructure. And so those choices that activists made to choose a type of technology that they think is more secure, in fact will not be the case in the months to come.

We can go into Nokia, Siemens and others. The Washington Times recently reported on the issue with Gamma International where you can see a list of all the items. Getting into what hearings and briefings are all about, about Congress. Well, what is it that can be done? And I hope—I'm going to suggest a couple things, and merely hope that there's a conversation with my fellow speakers here as well as you who are listening.

It's first—Congress must recognize that dissidents are facing far more sophisticated attacks and require far more sophisticated and nuanced support than has been the case in the past. We also must recognize that technology has a human rights impact and so, in certain parts of the world, surveillance equipment and others, when in those hands,

will have a terrible impact. And so, if we maintain a list of countries that severely repress Internet freedom, perhaps companies should report on this in their SEC filings in terms of what that impact is and what is it that we can do.

We must also, perhaps in these very repressive countries—like China, Vietnam, and others—if there's a certain threshold—have a regime of export control. Now export controls a lot of times are not popular in Washington, but I think that something needs to be there to know what the capability of these different countries are. And the question is that technology changes all the time, and so one must try to use technology-neutral languages that might encompass the threats today, but tomorrow as well.

The European Union has—or European Parliament has proposed language in things that they're trying to do at the European level, and their text is that interception technologies and digital transfer services for monitoring mobile phones, text messages, and Internet surveillance should be restricted and under export control.

We must also encourage, or the U.S. Government must also encourage, efforts that bring different stakeholders together to promote human rights and free expression online. There are current efforts underway by the Global Network Initiative, and perhaps might be others, that bring different communities together. There will be differences of opinion, but having a frank conversation of what the issues are and what companies face is really important.

Other democracies must also be supporting Internet freedom; it must not be the United States alone. And so I would encourage efforts of the U.S. Congress to work with their counterparts in other countries where legislators also want to make an impact. I'll suggest four countries: Canada—they just had a new election and has a parliament likely that will take up the issue—the U.K., Sweden, and the Netherlands, the latter two being countries that have actually put money down to support Internet freedom.

In terms of supporting—getting to the point that Kathleen mentioned ûwe must recognize that past are the days that only firewall-busting technologies were supported. They need to be complemented by other measures—such as training, security—going back to the point that I said that NGOs also face the same cybersecurity issues. Yet they have no resources; they have no networks; they have no access to the technical knowledge, and they need to be supported because otherwise, they'll just be inundated and not be able to help.

Urgent response mechanisms that traditionally the commission has seen in regards to human rights defenders and activists on the grounds must also be made available to Internet activists but they need to be coupled with technology support.

I'll finish in saying that also privacy efforts at home are very important because the credential information, which is how one logs into one's social network, one's user account, is the key that unlocks your digital identity, but also your digital friendship network. And if that gets exposed, it's not just that your ID has been compromised. It isn't about ID theft; it's about—particularly in many parts of the world—all your friends and colleagues being at risk. And some measures that can be taken to make sure that it's not important to address privacy—what I would say is that privacy should be set by default.

We can't do it at home, for whatever reasons; we should make sure that companies that provide these services abroad turn those on in the very repressive countries. I could go on, but I'd first just like to thank Shelly for the opportunity and look forward to your questions. And thank you.

Ms. HAN. Rebecca?

Ms. MACKINNON. These are really great overviews by the previous two speakers, and so I'm going to try to drill down on a few things, and perhaps address some assumptions that we often make, both—I come from a journalism background, but also I've noticed that a lot of policymakers make, that are sometimes proving not to be entirely true and that we may be hindered in solving problems by clinging to assumptions that may not necessarily work in the networked environment.

And one actually has to do with this dictator's dilemma. And I think in the Western world and particularly in the United States, we assume that all you need is more connectivity and, if a repressive country gets enough connectivity, freedom will inevitably result. And I think what we're seeing in countries like China particularly, but also a number of other countries, that it's much more complicated than that. That you—particularly in China—you have a country of nearly 500 million Internet users now; it's—yeah—it's not quite 500, but it's over 450 million at this point. And the government has managed to adapt to the Internet. And I've recently written a paper about this that was published in the latest issue of Journal of Democracy on what I call network authoritarianism. And it's how China is proving that, with enough resources and enough foresight—you know, we don't, you know—forever is hard to predict. But at least for the short- to medium-term, authoritarian regimes can survive the Internet much better than anybody ever imagined.

I was a journalist in China working for CNN when the Internet arrived in China in 1995. And Warren Christopher, the Secretary of State at the time, came to China and made a speech about how, you know, the software of freedom will prevail over the hardware of repression. What we didn't expect was that the Chinese government would be able to compel the rewriting of the software and the adjustment of the hardware. And that's what we're seeing happening in China.

And then, you know, Bill Clinton famously said, trying to control the Internet is like nailing Jell-O to the wall. Well, if you can change the recipe of the Jell-O, control the temperature of the environment and the porousness of the wall, you might actually succeed. And so this is the thing about the Internet: The Internet isn't like air or water; you know; it's just sort of chemically the way it is no matter what you do, that people—you know, businesses, governments and users are constantly shaping and changing what it actually is and what people actually can do with it and through it.

And so what we're seeing in China is that you have the government that has basically turned the private sector—because of course the Internet, right, is—we access it primarily through platforms and services that are owned and operated by private companies or by state-owned monopolies depending on where you are. And in a country where the government is able to control the infrastructure and strongly regulate all the Internet companies operating web services and mobile platforms and so on—basically the government can effectively turn the digital platforms and networks into an extension of state power to the extent that, while people feel freer to do a lot more things than they used to be able to do—and in China there's a lot more discourse going on than there was 20, 30 years ago when people were exposing corruption of their local officials and so on—if you try to organize a party to change the political structure, you go to jail. And everybody who had anything to do with you gets questioned, and that the state is able to do this because it compels the companies that are running the networks and the platforms to cooperate both in censorship and in surveillance.

And so one of the things, I think, that a lot of people in the United States still don't understand—when we think about censorship in China, we often think about what's known as the Great Firewall of China. And all we need to do is punch enough holes so that—in it, and it's going to be Iron Curtain falling down 2.0. But what's actually going on is that, you know, the blocking of international Web sites—the blocking of Facebook, the blocking of Twitter, the blocking of VOA and whatever else—that's just the first layer of censorship in China.

Most of the Chinese Internet is run by Chinese companies; it's in Chinese; it's run by companies called Renren and Qesha (ph) and QQ and Baidu, and lots of other companies you may never have seen or heard of, but that is the Internet that Chinese people know. And those companies are required to carry out very extensive regimes of censorship. So if you try to organize a group, on a Chinese social network to support your friend who just got put in jail, your account will get shut down. And there are constant instructions going from the authorities to the companies that run these social networks, platforms, search engines, and so on.

And so I think—and also with surveillance, they're required to hand over information about their users to the government, so of course this is one reason why the possible entry into China of Facebook is so controversial because if Facebook were to go into China and set up a local version of its service, it would be required to hand over user information, and it would be required to censor heavily. And there is no other way that it would permitted to operate in China. So this kind of myth that Facebook could play the same role it played in Egypt and Tunisia; in China if it were to go to China is, I think, you know, based on somebody smoking something really interesting.

But to broaden it out a bit, I'm involved with something called the Global Network Initiative, which the other speakers mentioned. And I think what China highlights is the responsibility of the private sector in determining whether or not this Internet that we would like to keep open and free and upon which we would like our universally recognized rights to be protected and respected that private companies have an obligation to contribute to the Internet either remaining that way or becoming that way in places where it isn't or ceasing to be that way. And that again, technology is a lot more political than a lot of companies would like to admit. And so what we're seeing more broadly, I think, is a range of trends in a lot of different countries whereby governments are seeking to regulate private networks in a manner—usually the reason being child protection, IP enforcement, you know, fighting crime, fighting terror. But the regulations that many governments in a range of countries, including quite a number of democracies, the measures that are being sought push the private networks and operators to take on more and more of a policing function, more and more of a surveiling function, particularly when it comes to child porn and IP violations, without thinking about how if you're putting more and more pressure on private networks—even in democracies—to take on these functions.

And if there's a certain amount of opacity and lack of accountability in how these functions are carried out, are you really setting up the global Internet to potentially be on a slippery slope to being a bit more like China in places where democracies are weak, particularly where rule of law is weak, or in a democracy that just happens to have a really bad election where some really unfortunate people get elected and then abuse the lack of accountability in the network to erode people's freedoms.

So the point being is that we really need to think carefully and that is why I like to say that Internet freedom begins at home, and I think it's really incumbent on us here

in the United States and on all democratic societies to get the balance right, to figure out how we ensure that we shape the Internet, regulate the Internet, construct the Internet, govern the Internet going forward in a way that maximizes its compatibility with democracy. And that does not create structures that will enable unaccountable abuse to be built in or to become more likely.

And so in speaking to activists—I'm just going to end on one point and then we can open it up for discussion because I don't want to go too long—but speaking to activists in the Middle East and elsewhere and of course activists, particularly Internet activists in the Middle East pay a lot of attention to policy discussions—Internet policy discussions going on all over the world including the United States. And one of the things that people have been saying long before the Arab Spring happened was a concern that legal norms and also technical norms being implemented in the West would be—would have increasingly negative repercussions for the way in which repressive regimes are able to use and manipulate technology.

And so one of the most—I would say—controversial techniques of Internet freedom policy here in the West came from a Tunisian activist Sami ben Gharbia who actually ended up playing a very key role, was a very key member of the Tunisian cyberactivist community that helped bring down Ben Ali's government. And he wrote a very long critique last September about Internet freedom policy from the West and sort of, you know, with the approach that oh, we're just kind of trying to free these oppressed people and not really paying attention to what we're doing in our own homes, and that the West needs to get more consistent

And he interviewed—interestingly enough in this blog post—an Egyptian activist named Elah Abdel Fatah who also played a very prominent role in the Egyptian Spring in the Internet activism there. And he asked Elah, you know, what are your concerns; what would you like to tell people in the United States and the West about what they ought to be doing to help you the most? And Elah said—and I'm going to just read from him here in closing—he said, if people in the West want to support democracy in the Middle East, the best they can do is to continue to develop a free neutral decentralized Internet, fight the troubling trends emerging in your own backyards from threats to net neutrality, disregard for users' privacy, draconian copyright and DRM restrictions, to the troubling trends of censorship through courts in Europe, restrictions on anonymous access and rampant surveillance in the name of combatting terrorism or protecting children or fighting hate speech or whatever. You see, these trends given our own regimes great excuses for their own actions. You don't need special programs and projects to help free the Internet in the Middle East. Just keep it free, accessible and affordable on your side, and we'll figure out how to use it, get around restrictions imposed by our governments and innovate and contribute to the network's growth.

And so I just kind of want to throw out that little bomb, not because I don't support the U.S. Government helping with tools and development but that there's a strong message, I think, coming from a lot of activists in the Middle East that we need to be consistent with what we're doing across the board.

And then just finally I would note that again this whole issue of global policy by democracies—that it's quite important to international strategy for cyberspace that the administration rolled out on Monday; it's a very high-level document; it's got a lot great words in it; we'll see what gets implemented. But what's very important about that was that one of my concerns for the past several years has been that while on the side of the

State Department and some people on the Hill, there's been great support for Internet freedom, you know, there've been other people sort of pushing trade policies—and all very legitimate, necessary interests, you know, trade interests, defense interests, other you know, anticrime/antiterror interests. And not that you don't want to pursue those interests but without really giving much thought to how the pursuit of those interests might impact Internet freedom and civil liberties on the Internet in a negative way. And so just complete lack of coordination between different parts of the government on different parts of cyber policy.

And what is important about the strategy, I think, is an attempt to say, look, we can't be working at cross-purposes that we need to pursue these policies with an eye to basic values and make sure that we get it right. And, again, we'll see, we now get to hold the administration accountable for this. But I think it's very helpful in starting a conversation amongst democracies about how do we get the balance right? How do we get these legitimate aims of protecting children and fighting crime and terror and so on, protecting intellectual property, which you need to do? But how do you make sure that you don't do it in a way that eliminates due process, violates privacy rampantly and gives regimes—not only authoritarian regimes but also weak democracies—a chance to abuse their citizens via private networks. And we just really need to be careful. So, on that, I'll stop.

Ms. HAN. Thanks to all three of you for some really great comments and things to kick off our discussion; I appreciate that. And I would like to get the administration strategy in just a few minutes and talk a little bit more about that since it just came out this week.

But first I'd really like to discuss something that all of you touched on in one way or the other—and particularly Robert was talking about the 1.0, 2.0, 3.0—how basically repression on the Internet has evolved over time. And the Open Net Initiative has a great book called "Access Control," which—the original version was called "Access Denied"—which I think, if you go from "access denied" to "access control," you can kind of see the evolution that they talk about and how repression has changed. And specific to the topic that we have today is how do we meet the new challenges that are coming about on the Internet? And they do talk about first-generation, second-generation, and third-generation.

And it's interesting that they focus specifically on Europe and the former Soviet Union. And Rebecca mentioned China, which is always a great example of how—China kind of breaks the mold for everything. I think when we all thought that, you know, free trade would lead to democracy, and maybe a free Internet would lead to democracy, you know. China's kind of broken the mold on both of those fronts.

But that's also been the same that we've seen in Russia and in some of former Soviet states in Central Asia. And certainly Central Asia doesn't necessarily have as much of a free Internet as we'd see in other parts. But Belarus, Ukraine, Armenia, Azerbaijan—there's some really good examples of where you do have Internet access but it's extremely controlled.

And so I'd like the panelists to discuss a little bit about the first, second, and third generations and then kind of where we are with the tools to combat those and maybe some example or some other suggestions on where we need to go. Now the first generation we normally talk about is the straight-forward blocking of the Internet. And I think we've all seen that there are a number of tools that have already come about through funding

and through innovation in the private sector to get around that. But are there other areas on the first-generation side that we could explore or should be exploring?

Second-generation, at least according to the Open Net Initiative is really more of a tricky issue—and Robert has shown this—it's really more the state being very selective about how they control, not only access but the actual physical ability of the information to stay up on the Internet. And sometimes it's through DDoS attacks; sometimes it's through malware; sometimes it's through getting the ISP to actually take down websites for certain periods of times. But it's usually a little bit more sophisticated or at least more subterfuge is involved than just absolutely blocking it and creating a firewall.

Third-generation—normally it's what they're talking about—is looking at the—also a little bit more sophisticated—you—let me read this because I'm going to get it wrong. OK, so it's more of active use of surveillance and data mining as a means to confuse and entrap opponents. And it also includes sort of more of a nationalized view of the cyberspace within the country. You know, so Russia is viewing the cyberspace of the [inaudible] as just the Russian space and that they have control over that, and expanding the powers of state surveillance through those tools.

So maybe if each of you could just touch on all three of those generations and what suggestions you might have on how—particularly on second and third—because we're seeing that—I think we see all three of them in places like China and the former Soviet Union, but I'd be interested in hearing your thoughts.

Mr. GUERRA. OK, I can go first.

I think one of the challenges is with the more recent generations of repression and censorship—is that, increasingly, it's a very well-developed adversary that is creating huge dossiers that is enlisting the private sector companies and using—I would say—far more sophisticated cyberweapons, such as malware against users.

The problem with malware is that—you know, it's—get to that because I'm saying that it's the scariest problem is that there's been a series of trainings. There's been a series of support around circumvention tools, getting around blocks. Malware is what I would say is a paradigm change that's complete because one could have the most secure device, take the best precautions. But if an insidious, almost impossible-to-detect piece of malware is installed on your computer or your cell phone, it will be the electronic spy in your pocket. It will send your geolocation information. It will send your files. We've seen this happening in China, and we've seen this now starting to happen elsewhere. So I think, almost—you know, that needs to be nipped in the bud now because if we don't, then all the measures and the incredible amounts of funding that are put together, not around Internet freedom but around cybersecurity will be moot. We'll have to start again. So it's—any weapon that's in the arsenal——

QUESTIONER. Are there tools to fight malware right now that you know of?

Mr. GUERRA. I mean, the problem is that the malware before—they used to be global in nature. And now they're regional. And so the antivirus manufacturers can't get them; and then there are companies that are making them. And so—I mean, there are also antivirus software that you think is antivirus, but in fact, it's a virus.

And what I would say is, if you want to take a look at it from a strategic point of view—it is connecting that community that's following that trend with the folks that are wanting to help the activists as well—to making sure that there is a clearinghouse, or some sort of information—what I would say is the technical community.

And so the way that the business community and government and academics have done this, is that they have systems in place call CERTs, which are computer emergency response teams, that share information around threats, that communicate with each other and do training, but also deploy steps. So that pooling type of approach for the activists or NGOs—doesn't exist. That's No. 3.

If we go to No. 2—I think No. 2 is basically, there is surveillance, so it's basically activists and users, particularly in repressive regimes, need to understand the vulnerabilities and great threats that they face. And what are some very simple measures? They can use not—they can decide not to use technology. And that might work. Having—you know, paper, and they burn it, or speaking to a friend. I mean, when people are in the same room sending an email to each other—I mean, there may be people in this room that may send a text message to each other, which is great. But it's gone to the mobile provider and come back, and you've opened the exposure to a whole variety of different people. And a lot of times, the younger activists forget the older approaches that have worked.

Scale is a problem, of course, when you resort to old technologies. But recognizing the risks and working with that. One of the great challenges now—and this is something that needs to be recognized—is that it is dual-purpose. And so when we're equipping activists to stay smart, to communicate securely, it likely will be used by a variety of actors we do not like. But we might just calibrate, for everything that we do—there is good and bad, and we do need to make sure that we take great care to make sure that—you know, that the benefits—and for censorship, I think the issue is that it's not just about blocking.

And so governments are changing the way they block. And so if we fund tools—and there's a variety of, you know, great tools that are made. One of the representatives of the Tor Project—and I think just was here earlier and stepped out. It's a tool that is innovative not so much in what it does, but in its approach in that it builds in privacy; it builds in anonymity; and builds in the recognition that it will be blocked and has backup systems for people to be able to access it.

So I think the tool developers, and those that support them, need to recognize that there will be blocks. And so the systems need to be smart. So what I would say is, tools that have some sort of artificial intelligence, that monitor the network and adjust, I think, is particularly important. But that requires funding, not over a year, not over 2 years. It requires not just the technology developers, but the larger cyberspace community.

So maybe those are three different things. And again, they're higher level, and I'm happy to get into more details. But I think they could be helpful going forward.

Ms. REEN. Just a quick comment building on the question of civic activism, and talking about individuals, in particular, because this is such a massive and broad subject. And I think one of the things that we sort of need to think about and distinguish as we talk about it is that there's a lot of concern about censorship and access to information—the ability to share and consume information.

At the same time, there's a massive spike—an escalation in what Robert referred to as technical violence. And the environment for civic activists and organizations everywhere, and ordinary organizations and well-to-do organizations and NGOs and businesses are increasingly vulnerable to this. We focus on this today when we're talking about civic activists, throughout not only the United States but everywhere in the world, because the vulnerabilities of those users are so high. And the techniques that we're using—we're

finding that it's—that we very much need to broaden the scope of online anti-filtering tools such as circumvention tools, to expand other innovative ways of protecting, and that kind of access.

And so migration to other host sites, particularly for entire sites that are blocked, not sites that are partially blocked but especially those that are under, enduring DDoS attacks, need other specific kinds of help. That that distinguishing is very important for us, because when we talk about the three levels, we start finding ourselves in a very deep and complex discussion about the governance of the entire Internet and the behavior of the entire private sector within it. And that includes absolutely everybody.

And so I think it's very important to sort of focus on what it is that you are trying to bring the resources to, and the problems that you are trying to solve. And I think it's worth emphasizing a point that Rebecca made, which is that the overall structures—if there is no global agreement—if there is no question put to the private sector as they develop tools and think about how those tools are used—if those questions are not asked, and those agreements are not brought to the table, it will continue to be an uphill battle, a Sisyphean feat to try and protect civic activists everywhere, which is really looking through the wrong end of the telescope.

We're looking at the issue the wrong way, if we think that we can solve it, activist by activist, when the very structure that people are using is starting to break.

Ms. MACKINNON. Just to add—I mean, hear, hear, everything both of you said—I mean, beyond sort of basic circumvention, I think what we're hearing, and what I will echo, is that the solutions are as much human, if not more human, than they are technical. And it has a lot to do with people's awareness and understanding, as Kathleen said, of how the Internet works, about how their mobile phone works, about what is the relationship between these networks and their government or other governments, and where they fit within that, and what their rights are likely to be and what their threats are likely to be based on their personal situation.

And then, understanding that the technology is going to change constantly, and that people have to adapt. But I've seen, in a number of countries, not just China but also in the Middle East, that where people are best at adapting, it's again because there's a community, not just relying on tools that are sent to them by Americans. But there's a community of local programmers and geeks and people who understand the tools, understand how their government is functioning locally, and are able to work with people like the Tor project people, and with others, to adapt their tactics, And also to make requests of the Tor project people, or whoever else they're working with.

You know, can you change it? Or could you do something kind of along these lines, because nothing we have right now is meeting the threat that we're facing, because the threat just changed?

And so having communities of people who are not only able to communicate with kind of this global community, but also who are able to educate people around them and then kind of create feedback loops of awareness going back and forth, is absolutely critical because the situation varies from country to country, even from city to city sometimes, in terms of how—you know, the local police department—its relationship with the local carrier in one city might be different than in another. And then the primary threat might be different. Or any number of things.

And so it's very, very local, is the point. And so there's absolutely—you know, kind of no magic app, no one-size-fits-all solution, increasingly, as we move, as Robert said, from filtering and blocking to technical violence, which is increasingly localized, and developed locally.

So yeah—so a lot of it's about—you know, as Kathleen puts it, public policy at the top end, but also public education, as much as possible.

Mr. GUERRA. I'll maybe add to this, there's—but we also have to recognize that people have problems. People are needing urgent assistance now. So all the support takes time. The countries are getting more sophisticated, both in the region and covered by the commission in others. But activists are in need.

And so I think that if decisions are going to be made—you know, I mean, I hate to say this, but—you know, what's easier sometimes is if one forgets about the longer term stuff, that's fine. That's a missed opportunity. But at the same time, it's recognizing that there's a new generation of electronic democracy activists that are needing a little bit more sophisticated type of support.

And that should not be lost, and they need to be recognized. They need to be supported. And the ideas need to come from them, because at times—like Rebecca mentioned, it wasn't the U.S. activists; it was a Tunisian activist. And it's long been about these issues, to play a role in his own country, and other countries in that region as well.

Ms. REEN. I think we're talking about the difference between the urgent and the critically important. And so—you know, when we're talking about activists, it's right now. It's yesterday, and it's definitely tomorrow. And then, when we're talking about solving these larger questions, we have to keep our eye on the ball. And we have to engage it now, because the problems that we're facing today and tomorrow will continue to be our problems today and tomorrow if we don't develop those larger—answers to the larger questions that have been put by the panel here today.

Ms. MACKINNON. One of the things we did find in the Middle East with the Internet kill switch being deployed in Egypt is the need for people to—you know, there are technologies out there, actually, to create sort of a combination of what Robert called sneakernet, and people using kind of Bluetooth phones to sort of network locally with one another, and the Bluetooth on their laptops, and sort of send things amongst each other, and then get it to the Internet—you know, there are things like that. These are the sort of hacks that could people perhaps could be better prepared for if the technology's available.

And so those are some of the things that people are thinking about, but û

Ms. REEN. And there are locally adapted and adaptable solutions. So you do have some of the stronger tools that have received investment and continue to grow, like the Tor project, which has widespread use. But you also have people, as Rebecca's saying, in these environments, coming up with their own locally networked solutions.

And there are certainly people where those lessons could be shared internationally as well. Mesh networking—you know—is possibly an area to look at more closely when we consider what happens when a government decides to turn on the kill switch. As rare as it's been, I don't necessarily think it's the last time it will happen.

And as governments play catch-up with how the Internet is controlled, and how they control their telco environments, it is a tool that they can continue to use.

Ms. MACKINNON. That discussion of the kill switch brings up a question that I wanted to raise, and that is something that your colleague, when you were at the Berkman Center, Ethan Zuckerman, coined a wonderful phrase: the cute cat theory of digital activism. It basically means that when you get to the point where there are so many people who are online, looking at cute cat videos, you can't use the kill switch because so many people will turn into political activists that—because you've shut off their access to cute cats.

Whereas if you're just deploying technologies that are just annoying dissidents, that's a price tag that you can afford—you know, as a country. So—you know, the question is, how do we raise the price tag for these countries? You know, how do we make everybody a cute cat? [Laughter.]

Well, you know, this is why Facebook and Twitter were so important in the Arab Spring, and it wasn't some—you know—government-funded application—you know? You know, that's exactly why. Because these tools are used every day for all kinds of non-political purposes; and that's how they spread. And that's why they became the place where you go, when you want an audience for whatever it is you're doing.

And so I guess that's the point—I mean, there are some people in the activist community who are advocating—oh, you know, what we really need to do is develop these tools that are totally non-commercial. And like—you know, they can't be controlled by any government, and they can't be—you know, they have nothing to do with any company. And that's where it's going to be totally free. And that's the key to the future.

But again, the problem is, you're not going to have any audience. Like, if you're trying to run a political movement that means you need to get beyond the hardcore, dedicated people, to the people who are normally blogging about their shoes that they bought at—you know, whatever boutique, and cats. And get them concerned. I mean, that's how you have a political movement.

And you're going to find them on Facebook. You're not going to find them on some—you know, super cool dissident network. And so—which is why bringing companies on board, in terms of making sure that their networks do not get used as extensions of repressive power, even if they didn't intend them to be.

And to ensure that vulnerable minorities and political activists are protected—that their rights are protected within these networks, while everybody is doing their cat blogging and—you know, dating, whatever else. I mean, that's why it's so important to have the private sector on board, with the understanding that they have a broader public responsibility, and that—really, the future of democracy may depend on whether they step up.

Ms. REEN. And I think that's why, when we're talking about this, we're talking about the digital economy. And the digital economy is the economy. And there isn't a country in the world today that doesn't have a stake in it.

And that stake is growing and deepening as they strengthen and build out their networks so that every citizen in the world can have access to it. And I think, while we understand that to be the case, we can recognize why it was that Egypt turned their Internet back on as quickly as they did.

You are no longer just talking about activists in Tahrir Square. You are talking about the entire economy being put on hold. And that's a tremendous disadvantage. That's an extraordinary decision for a government to take, and one that I think is the least optimal.

But as Rebecca says, I think it's also one of the most important reasons why our engagement on this question has to include the business community.

Mr. GUERRA. I kind of see the cute cat theory a little bit different, and I see it more that it's important to have conversations about noncontroversial subjects first. If you get the skills to exchange photos about cats, about babies—you just replace the picture of a cat with an activist, but it's the exact same skills.

So building of skills, and building a conversation—and make it depoliticized—I think is particularly important. And countries that try to limit that are ones that we should single out. And a country in point, in Europe, that's often talked about that has very draconian measures is Belarus.

Belarus did not allow people to assemble in its main square smiling. People who were all smiling together got arrested. There was a flash mob that had people bringing their ice cream cones together. They got arrested. And it's a country in the region that has incredibly draconian Internet control legislation as well, that, if effective, will spread to that region as well, too.

So it is countries that aren't pushed back. And it's very difficult. And supporting and monitoring the technology flows. I think that's the other issue; what the activists do. But also if countries are supporting other countries, the worst practices are being spread in different regions. And if the United States has an influence, it can try—that's why I mentioned—you know, stopping the technology flows, or at least knowing where they're going, particularly important.

And there are a variety of different instruments that don't have to be created, or existing ones that can be used, but just updated to have some of that. So it's—I think keeping it simple, having people being able to have access to the Internet, if they don't have it at all. So the U.S. can encourage the Internet being deployed, but not a reengineered Internet that's one of control. That's one that's increasingly being found in Africa, supported by the Chinese.

QUESTIONER. OK, I've got one more question for the panel before I open it up to the audience. And that's—you were talking about the necessity of having conversations online. And one of the—I was reading an article by Clay Shirky who's a professor, he's written a lot on Internet issues, and he's arguing that access to information is less important politically than access to conversation. I mean, the other way around. And that conversation itself is really important. And I agree with that, but I think it ignores this growing phenomenon of control of the conversation.

And where China, Russia, other countries are actually deploying people to have the conversation in a really artificial manner [laughter] are paying people to do the conversation. And so when you distort what is supposed to be this free flow of dialogue among friends or acquaintances on the Internet to become, really, what is propaganda. What do we do about that? It's there; it's information; it's free flow of information, but it's not necessarily free information. What sort of responses can we have to that?

Ms. MACKINNON. You know there's another academic—I won't get too far into academic wonkery who talks about something called authoritarian deliberation. And, you know, one of the things I think in the reporting on a lot of authoritarian countries and the Internet is that, you know, if there's a lot of public debate about issues that's seen as, oh, well that country must be liberalizing and it must be on its way to democracy.

But what we're actually seeing is that a government, like China—but there are others like Bahrain comes to mind, and a number of other places—where exactly that—you have quite a lot of discourse going on; you have tremendously lively conversation. But it's constrained within certain boundaries and also very manipulated by people who—some people who are paid by the government, other people who are just kind of—you know, all the nationalistic people are encouraged to do whatever they want, no consequence, and the liberal internationalists, you know, have consequences and get censored. So it's manipulated in a particular direction.

And it's hard, you know, because there's no app to deal with that, right? But, at least in China but I think also in other countries, again it comes back—it goes away from the technology and comes back to human community. And in China one reason why the government, I think, has been so effective in maintaining control while still having a very lively Internet is that they've marginalized this liberal blogger community, you know, they've got—just the amount of space they have to talk, the ability to converse is more and more squeezed; more and more people are threatened, and so on.

And the rest of the country has no idea that these people even exist. So part of it might be, you know, just helping to create alternative spaces for these communities where, you know, some other place for them to go online outside of their national cyberspace where they can be safe, and have their conversations; and maybe build critical mass so that maybe more people in their country might want to join those conversations. And Twitter has actually had something of that effect in China, in that it's known as the place where you go when you want to have uncensored conversations in China. It's getting harder to access, but—and it's getting more surveilled, so that kind of window is also closing.

But, there is a community of people who found that to be a safe space for a while. And so I think part of it may be just helping to create—if people cannot create spaces for communities and conversation on their own, or in their own countries, are there ways to help support those conversations and communities, you know, digitally elsewhere. But it's difficult.

Ms. HAN. Any thoughts on that before——

Mr. GUERRA. I'll just say—and the simplest is in those cases is just making sure that the activists in these particular countries that are subject in a way to cyberbullying because they have all these people posting hundreds of paid blogs—that they be recognized. So whether it's Oleg Kozlovsky in Russia or others, very valiant young people in Belarus and other countries as well, that when they're facing great threat they need to be recognized.

And for them the best thing is to know that they're not alone, and they'll keep the struggle and they'll brush off all the comments. But you know, a lot of young people, which are, the vast majority of the people online, don't have these very basic skills of defending against criticisms take it—see it personally and just turn off. And so it's all of that, it's all support, but equally as important.

Ms. REEN. And, you know, a last shout out for education, it's just absolutely critical that people, you know, know how to use their Internet well, and have a level of sophistication and knowledge about what it is. And I think that that's especially so for civic activists who are feeling very alone, but it's also the community writ large. And, you know, we have an absence of information in this space, which is—and it's a very contested space.

And in the competition for ideas we have to somehow make it—some of the fundamentals truly and obviously available to everybody. And I don't think we've been able to do that fully yet and I think that, you know, we've been surprised. I think Western governments have been deeply surprised at how contested those basics are in terms of that education. And I think that we have a long way to go.

Ms. HAN. Are there any questions from the audience? Anybody who'd like to ask the panelists—if you could step up the mic here—you're first, that's fine. [Laughter.] And if you could just tell us your name and affiliation that would be great, thanks.

QUESTIONER. My name is Patrick McKay; I'm an intern with the Center for the Democracy and Technology. And my question is kind a followup to what Rebecca was saying: the domestic threats to Internet freedom.

And my question concerns a bill that was just introduced in the last week by Senator Leahy to protect IP [inaudible] which we groups have express concerns would establish a similar U.S. censorship regime by—in the name of protecting intellectual property. It would for the first time employ tools such as domain name blocking and internet search engine censorship, restrict results censorship, on a wide scale to the United States.

I was just wondering if the panel could discuss any concerns you may have with that, especially in regards to undermining U.S. ability to influence the rest of the world in a positive direction for internet freedom.

Ms. MACKINNON. Well, a couple of things, I mean, I'm quite concerned about that bill for the same reasons you are. I would, just with one caveat, just emphasize however that I'm not equating the United States and China. There are a number of key differences, one being that I'm standing here today saying critical things and I'm not going to jail later. [Laughter.] And that's a really big difference.

And, you know, and the fact that we can share information; we can discuss; we can rally; we can debate; we can lobby to have laws changed that we don't like, and we don't go to jail for doing that. And there are bloggers who are, you know, being very outspoken about this all the time, but that organizations like yours can actually exist, you know, that's, like, in China they couldn't. So there are a lot of really key differences so I just want to get that out of the way so that nobody accuses me of saying that the U.S. and China are somehow equal, or remotely equal.

But, that said, there is a dangerous erosion of due process and accountability in a lot of proposed legislation and also some legislative trends, administrative trends, over the past decade that are of great concern. And a lot of delegation of policing to private networks, the lack of clarity about what information is being shared with various government agencies, and how the, you know, the fact that content might be taken down due to a fairly specious accusation of copyright violation that ends up not being true, but, in the meantime the critical period of time for your activism has passed and, you know, the extent to which there's enough due process and accountability when it comes to manipulation of speech, I think, remains a concern.

And, you know, we are a robust democracy. But democracy is like a marriage, if you take it for granted you're going to wake up 1 day and discover you don't have it anymore. And in the Internet age, I think, we're at this critical point where we really need to be looking at, how we are balancing these various policy interests and policy aims including defense, law enforcement, IP protection, and so forth.

And make sure that we are defending civil liberties and freedom of expression as robustly in digital spaces as we have always defended them in our physical spaces. And what I'm concerned is that there are a lot of policymakers who see the cyber realm as a place where you don't have to have tradeoffs, where you ought to be able to have perfect security, where you ought to be able to have, you know, no more copyright violation at all. And it's just like, well, yeah, we can have a crime-free Washington, DC, but at what cost in our physical space.

And so I think, the point being is that we're going to have to have balance and tradeoffs. You're not going to have perfect security. You know, its human solutions to human problems. And I think sometimes that there's too—a lot of policymakers, lawmakers, have pressure from their constituencies to just make certain problems go away. And just as in this physical world we can't make most problems go away completely, we're not going to be able to make them disappear completely in the digital realm, unless you want to ruin democracy.

Mr. GUERRA. A slightly different set of points is that there seems to have been a variety of proposed legislation around kind of copyright and trying to restrict access. We haven't seen the same number of legislation to try to protect the space of the Internet in other countries. We've had Gopher; we have Durbin in the Senate that's proposing funding, and then we have a plethora of other type of restrictive legislation, so there needs to be legislation that also promotes, kind of, speech online as well too.

You know what I'll say is dangerous from—if you take a look at kind of trends in the past is—you know, while I personally may have one view or another on the cop rate discussion and whether it's gone too far or it hasn't, what's important is that there is a whole industry that's developed—that technology policy—embedded into technology. So the device itself is the one that does all the deciding, so—this is what the deep packet inspection technology was all about, to try to take a look at—BitTorrent was being streamed, or other things were being streamed, and stop it.

That technology gets developed here. For the legislation that people may or may not disagree with, but that gets implemented here, that piece of technology finds its way into other countries and all the due process is turned off. So my worry is that with the technology that gets developed to implement technology choices made here at home, have an incredible effect on repressing free speech, and surveillance abroad. And we need to make sure that that unintended consequence gets controlled somehow, because otherwise that's what we're creating. We're creating the monster.

And let's not forget that the legislation created by Congress to support schools many years ago with Internet access also added provisions around pornography in schools. And everyone may find that fine, but there's a whole industry that spawned to make sure that censorship was available, and then that found its way around the world.

And so for everything that we do, there is an international implication. And, you know, we're not tracking that enough. And so maybe that's something that we can do. And then the technology policies we make at home stay at home. Then it wouldn't be as bad. It won't be as easy, but let's at least limit the damage that we might have.

Ms. HAN. Did you want to say anything?

Ms. REEN. I think we recognize that lawmaking around the Internet, whatever the subject, is extremely hard. It's amongst the most complex because it has to consider so many variables. And I think that we can only urge our lawmakers and the best of our

decisionmakers, and those who are trying to help frame this going forward, to bring the right people to the table to make sure that they're as informed as possible of the unintended consequences and the possibilities so that there's a more measured and balanced approach to these.

It's not that we don't believe in solving these problems; it's that we don't have an easy outlook on what the consequences of those decisions are. And so that's why it involves often an unusual array or cast of characters around table. But I think, increasingly, we have to be able to speak across the bow to different industries and across different groupings in order to be able to solve them.

Ms. HAN. You had a—you had a question?

QUESTIONER. Where do we start? I mean, I'm not expecting lawmakers to jump for joy at the prospect of a bunch of slides talking about [inaudible] teachings [laughter] or anything like that. But a lot of legislation obviously shows the hallmarks of ignorance about technology. Whether it's the situation surrounding certain [inaudible] that people want to hear that someone is going to singlehandedly take down the great firewall in-between World of Warcraft games instead of having a bunch of geeks do long-term research trying to anticipate, trying to be 5, 10 steps ahead of what the censors are going to be doing, while sustaining the tools that exist. It's boring stuff. And but if you're going legislate in this arena——

Ms. HAN. Congress does boring really well. [Laughter.]

QUESTIONER. It's a different kind of boring. [Laughter.] I mean, I've read legislation, but this is a different plane of boring. Where do we start? We're willing to talk, but the reception is not there, at least in my experience, to understand the technology that we're legislating.

Ms. HAN. And can you just tell us your name, and your affiliation?

QUESTIONER. Oh, I'm Karen Reilly from the Tor Project.

Ms. HAN. Oh, OK, great. Thanks. I think that's a great question and it also, kind of, plays into a question that I wanted the panelists to weigh in on; it's like what's the fourth generation? I mean, what are we looking at on the horizon for next? You know, and what should we be focusing our attention on? And I think that's a great question.

Mr. GUERRA. It's a variety of different things, I think that—I wouldn't say necessarily fourth generation—but developments that we're seeing, is that we're seeing governments that want to be supportive, like the United States, having a variety of different priorities that they need to try to solve. And so you have, you know, what's considered by some, you know, quite high-levels of support around, kind of, Internet freedom. It's one of the few areas in the FY11 budget that kept more or less its levels that it did before, didn't have a bunch of it cut.

But it won't be able to do it forever. And other countries need to pitch in. And so seeing this shift to a more international scope, I think's particularly important. And, you know, I think that's something that hopefully we'll see over the next probably 6 months or so, other countries coming in. I think what I was talking in terms of the third generation in terms of—there's a whole industry.

And I think what the risk we have is that despite all the great efforts that we all have, is that there will be something that changes the game, that resets all the measures that we've done. You can think about it as there was conventional warfare during World War II, and there was the atomic bomb. And it changed—I think that something like Na

Ware will change that for cybersecurity because fractioning of the DNS, which is the system we all use that everything uniquely identifies through the system coordinated by ICANN, if that fractures, that's a problem. And so if the governance of the Internet fractures we have a completely different world.

Ms. MACKINNON. Yeah, I'm a relative newcomer to Washington and so the way things worked in these halls is—continues to be something of a mystery to me. But, yeah, I mean, politics ultimately is all about constituencies. And I think part of the problem, I mean there are so many different problems, but one of the problems is that the policy is really just being discussed amongst a fairly narrow group of people. And I think we just need much broader public concern as well. You know, on the one hand, you need better technical knowledge in crafting legislation; I think on the other hand, you need a much bigger movement.

And, again, I tend to look more at the long game because that's sort of where my head is and other people are looking more at the short game. But, you know, I mean, I think just in terms of where the Internet is going, whether it's going to maintain its open and free nature, you really need a global movement of people who are pushing for its protection, kind of like you have an environmental movement.

And you need people asking their Congressmen and Congresswomen, you know, in that cybersecurity bill, or in that IP protection bill, are you also making sure that my civil liberties are protected? You know, asking those questions. And I don't think legislators are getting enough questions of that kind from their constituents, I don't think companies are getting enough questions of those kinds from their users and customers. I would like to see a lot more, kind of, demand for transparency on the part of companies in terms of how they're handling the information and in terms of, you know, what the government accesses and how and when and how those processes work.

In addition, there're a lot of things I think around the public needing to demand more sensible and balanced legislation. Understanding—you know, I mean, it took a few decades for the public to realize—or at least some critical mass of the public—that, you know, companies needed to be held responsible, and that there should be a way to do it and to get legislators on board in a more holistic way, and it's, you know, really hard every step of the way—with environmental issues. But we're sort of, like, back in the '60s, you know, as far as the Internet kind of freedom movement is concerned. You know? [Laughter.] Still, we haven't even hit Earth Day yet in terms of awareness.

But it needs to get there somehow. And that might help, I mean, obviously we're never going to solve the problem, right. I mean, we're human beings, which means, you know, it's always going to be a mess. But I think definitely just people recognizing that the internet is a politically contested space, and recognizing that they are citizens of that space and they need to push for their rights and demand their rights be protected in that space.

And that whether the rights of the person in China are protected in that space could ultimately effect whether our rights are protected, you know, because it's globally one, you know, potentially one space. People aren't thinking of the Internet and our technology that way, and I think more people begin to think of it that way there may be more pressure on lawmakers in all democracies to think more broadly about the longer-term consequences when they're trying to solve very specific problems.

Ms. HAN. All right, we have time for one more question, if there's anyone else who'd like to ask any questions. Nope? OK. Well, I want to just close by telling you that in the RAND study they actually did say that there is a tipping point, where the dictators can have, a little too much democracy for their tastes and that it could lead to more democratic societies. But I would really like to ask those authors to redo that study given everything that we've seen today and the way the countries—how the governments have responded to the Internet. I think they've been quite agile and creative and a lot more than I think that we considered before.

And I wanted to close with a quote that was in the study, by Aldous Huxley who is a, you know, an author who wrote a lot about the future. But he wrote that, "Mass communication, in a word, is neither good nor bad; it is simply a force and, like any other force, it can be used either well or ill. Used in one way, the press, the radio and the cinema are indispensable to the survival of democracy. Used in another way, they are among the most powerful weapons in the dictator's armory." And that was from 1958. I think the same quote could be said today about the technologies that we have, and I think it just outlines for us what the real challenges we're facing, and that we're going to continue to face, as we try to do this.

And I appreciate your interest in this issue and I hope that we'll see you again at another event. Thanks. [Applause.]

[Whereupon, at 3:30 p.m., the briefing ended.]

○

This is an official publication of the **Commission on Security and Cooperation in Europe.**

★ ★ ★

This publication is intended to document developments and trends in participating States of the Organization for Security and Cooperation in Europe (OSCE).

★ ★ ★

★ ★ ★

http://www.csce.gov

The Commission's Web site provides access to the latest press releases and reports, as well as hearings and briefings. Using the Commission's electronic subscription service, readers are able to receive press releases, articles, and other materials by topic or countries of particular interest.

Please subscribe today.