CHALLENGES AND APPROACHES TO EFFECTIVE CYBERSPACE GOVERNANCE IN A MULTIPOLAR WORLD

This panel was convened at 11:30 am, Thursday, April 4, by its moderator, Anupam Chander of the University of California at Davis School of Law, who introduced the panelists: Paul Brigner of the Internet Society, North American Bureau; Laura DeNardis of American University's School of Communication; John Kneuer of Globalstar, Inc.; Ross LaJeunesse of Google; and Jorge Villarino of the Congress of Deputies, Cortes Generales of Spain.[*]

Introductory Remarks by Anupam Chander

I am delighted to open a roundtable discussion bringing together some thought leaders in the increasingly important area of cyber-governance. They are Paul Brigner, Director of the North America Bureau of the Internet Society; Laura DeNardis, a professor at the School of Communication at American University; Ross LaJeunesse, Global Head of Free Expression and International Relations at Google; John Kneuer, President and Founder of JKC Consulting, LLC, a senior partner at Fairfax Media Partners and formerly Assistant Secretary of Commerce for Communications and Information where he served as the Administrator of the National Telecommunications and Information Administration; and Jorge Villarino, Legal Adviser on the Committee on Justice at the Spanish Parliament, where he is also head of the International Department. I will begin with some questions to the panel, before turning to a rapid response portion, and concluding with an audience question and answer session.

In December, we saw the European Union and the United States walk out of international treaty discussions for the regulation of the Internet. The international treaty they were protesting sought to bring the Internet largely within the fold of the International Telecommunications Union. Why not see the Internet as simply a new communications medium and therefore exactly the kind of thing that the International Telecommunications Union should govern?

Paul Brigner

The Internet Society was involved in the discussions leading up to this treaty conference, the World Conference on International Telecommunications in Dubai. The last time the ITUs were negotiated was back in 1998, giving us an idea of how often these types of regulations are likely to be updated going forward. If you think about how the Internet has developed over that time, if we want to have new rules, standards, and ideas brought into the Internet space from the ITU in treaties, we might be waiting for a very long time. More fundamentally, the Internet offers a different technology than the standards that the ITU has been working on in the past.

Before the Internet, telecommunications systems were basically telephone systems, largely owned and operated by state-owned entities, and it made sense in some cases for the ITU to get involved in bringing those parties together, to help develop standards and guidelines. But the Internet is fundamentally different, a network of networks, primarily developed through the early days in the academic and the business community, with governments arriving later in the process. So we have a very different form of governance for the Internet today, a multi-stakeholder form of Internet governance.

---

[*] This is a condensed and edited version of the panel.

Anupam Chander

Jorge, what is the Spanish or European perspective on the ITU and the Internet?

Jorge Villarino

First, I should note that the European Union is not a member of the ITU. In November 2012, the European Parliament adopted a resolution stating that any change in the international communication regulations have to respect freedoms and respect the Internet as a public place. The EU does not want to enlarge the scope of the ITU to include Internet governance. They don't say why not, but I think that they don't want for some governments to have a role in the governance of Internet. If the model that we have right now—the bottom-up model, the consensus-based model, the multi-stakeholder model—works, why should we change it?

Anupam Chander

Okay. So things are fixed, don't break them. John, what do you think?

John Kneuer

I think Paul was being polite.

[Laughter]

I have the luxury of not being constrained by offending anyone, but I think the short answer is that the ITU is almost a singularly ill-equipped institution to deal with what are, at their core, technical matters around the governance of the Internet. It is a regulatory and political body housed within the United Nations. It is not immune from the geopolitical macrodynamics that affect the United Nations. I think the ITU is probably the best example that you can imagine inside a UN body trying to stay focused on the tasks it has in front of it and not being swept into these other political macrodynamics, but they still do. Internet governance, and particularly the role of the Internet Society, is very much around technical coordination of technical issues. We don't look to the ITU to develop new air interface standards for mobile devices. That's not what they do. Those things come out in different iterations. There are some standard-setting bodies that are privately managed and operated that can play a role in that sort of thing to allow for universal interoperability and those sorts of things, but in terms of establishing and setting the technical standards for the evolution and deployment of the Internet, those should be left to the technical expert bodies, the multi-stakeholder model that Jorge discussed. And I think the point that Paul made, that the ITURs get renegotiated every decade or so, underscores how inapplicable that would be to the dynamic nature of the Internet.

Anupam Chander

Laura, you have written about the Internet Protocol and standard-setting. John described these as technical matters, but you have argued that there is often a politics to technology.

LAURA DENARDIS

The design and governance of technology is absolutely political. With this technically embedded politics in mind, the Dubai conference was not supposed to address the Internet. The conference was convened to discuss possible updates to a 1988 treaty on cross-border telecommunications arrangements. There are many political concerns embedded in these agreements, but these agreements focus on telecommunications. Yet the gathering included proposals coming from Russia, China, and Arab states that would have expanded the discussion far beyond telecommunications into Internet connectivity and content. For example, there was a proposal related to spam and one that raised the specter of ''sending party pays,'' which would change the nature of how service providers and content companies compensate each other for interconnection. Telecommunications interconnection, which is already political, should not be expanded into governments regulating Internet content at interconnection points.

ANUPAM CHANDER

Ross, Google is at the epicenter of these things. When people are thinking about Internet governance, they're often thinking about governing Google.

ROSS LAJEUNESSE

I was actually a member of the U.S. delegation during the ITU Treaty Conference, and so I have the benefit of being on the ground there for two weeks while this was going on, along with Sally Wentworth and a lot of other committed wonderful folks from the multi-stakeholder organizations that have been referenced before. I think the right way of looking at the question that you posed is: Why would we move away from a model that has not only worked well, but is the primary reason for the robust Internet that we see today? And the reason why it works so well is because it is truly multi-stakeholder, and it's hard for governments to wrap their minds around this, but it works. You know, we've seen things, like incredible challenges to the Internet before, like the Conficker virus, and we've seen organizations like the Internet Engineering Task Force rise to the challenge and effectively address it. So this multi-stakeholder constellation of organizations really does work, and into this, the ITU—which I agree with John is a particularly problematic organization to be dealing with some of these issues—wants to step in.

More broadly, you have a number of governments who simply don't like the way the Internet is being run today. There is a kind of unholy alliance. Proposals that came out of Russia, Syria, Iran, and China have joined with the ITU's own goal of ensuring its continued relevance in a world that increasingly communicates over IP networks and not through old-form telecommunications. And that's why you saw some of the proposals that you saw, including a focus on spam. The particular favorite of some of these folks is to talk in terms of ''cyber security.'' But then you look at some of the proposals, and you realize that anything that anyone wants to address is called a cyber security issue.

The ITU is incredibly political. You have 193 countries there, and they're voting on things like human rights issues, trying to bring those proposals into a telecommunications conference. The Iranian delegate took to the microphone numerous times to submit numerous proposals. The ITU is governments-only. It is not transparent as an organization. They do not put their proposals online. The only way I was able to participate in that conference was because I

was appointed as a delegate by the U.S. State Department. I had to leave my Google credentials at the door in order to even participate in this sort of conference. And it has no expertise in these Internet issues at all. So why are we talking about turning over governance of this amazing tool for social and economic development and advancement to this organization?

ANUPAM CHANDER

So is there a role for international treaties at all? Is the Internet an international space or mechanism or tool or technology?

PAUL BRIGNER

I think we can look at the ITU's World Conference on Telecommunications and say that not all of it was bad, that there was some good there. There was the provision for greater transparency on mobile roaming rates. There is the recognition that interconnection of traffic routes should be determined by private operators. I think there are things that can be done at the treaty level that make sense. I wouldn't try to determine what those are here or make any suggestions, but I wouldn't say never. When you do get into working on the technologies, the nuts and bolts of the Internet, I think it's pretty safe to say that that's not treaty-making material just because of the speed of which it develops and the way that it needs to adapt and be dynamic to serve the Internet's interest.

JOHN KNEUER

I think you need to remember that a few years before the Dubai conference the same cast of the rogues gallery—China, Iran, Russia, and Syria—brought up the same issues at the World Summit on the Information Society (WSIS) in Tunisia. There, we had a much louder unified voice coming out of that conference in response, which was that the status quo on the technical management and Internet governance was the least suboptimal solution to these difficult issues. WSIS also acknowledged that there were areas of common concern and interest that go across borders, but those areas of interest and concern should explicitly involve not just governments, and they created the Internet Governments Forum as a place for governments and the private sector to come together and discuss some of these issues and seek solutions.

So in the same way that we have international treaty arrangements on currencies and on varying areas of criminal law and so on, there is no reason that just because an activity takes place on the Internet, it should be free from examination. But you should not try and architect the Internet in service of your preferred public policy options because there is just such a great diversity in viewpoints on those things, even among nations as closely aligned and similarly situated as our European partners in the United States. We have very different views on speech, for example. There are countries in Europe where any variety of speech that we would find abhorrent but protected is legal, and so you need to be able to recognize the differences in those regimes and figure out ways to do that, but the way not to do that is to answer the calls of those who say, well, we need to control the infrastructure and the technology of the Internet so that we can control the behavior.

JORGE VILLARINO

Let me underline this one thing that Ross said before about the ITU. I was quite surprised because when I wanted to get access to some of the documents of the ITU, it was absolutely impossible if you have no credentials. I mean, how do we want for an international organization to deal with Internet, which is the most transparent place in the world, with an international organization that does not even let you get access to their proposals? There is no way.

On the other hand, talking about what we have just said, is there a place for international treaties regarding the Internet? I would say there is no place for international treaties on the Internet as a whole. But there is a place for international treaties on some aspects related to the Internet. For example, in order to fight against cyber crime or things connected to cyber security or even with privacy or freedom of speech, it is true that we have different approaches. I guess that we are going to have the chance to talk about some of them later on, but for sure there are some aspects in which we will be able to agree, at least I would say in western countries. With some other countries, like the ones we have mentioned—like China, Iran, Russia, and Syria—it will be much more difficult to find those places for agreement.

ANUPAM CHANDER

Right. So, Ross, has Google participated? What is its position on international treaty making, the draft treaties, the treaties that are being considered by the U.S. government or by other governments?

ROSS LAJEUNESSE

We follow them. We are interested in them. And from my perspective at a company, I see them as a vehicle for advancing things like cross-border dataflows and seeing information as we see any other good and service, and that erecting barriers to cross-border dataflow is no different than setting up a trade barrier for anything else. And you can take the analogy even further when you look at China's indigenous innovation initiatives and the way that they're treating cross-border dataflow, which is very similar. It's, ''We're trying to set up our own Internet here, we want to advance our own industries internally, and the rest of you stay out, or come in but on our terms and conditions.'' So I would like to say that we are more engaged than we honestly have been, but this is an area where we are increasingly looking at as an opportunity for us to play.

ANUPAM CHANDER

Almost all of you have mentioned this word ''multi-stakeholder.'' What is this multi-stakeholder model, and how do we apply it to the Internet? Is it possible to have a multi-stakeholder governance? What does it mean? Is it a good idea?

LAURA DENARDIS

Internet governance is what happens on a day-to-day basis outside of these red herring discussions. The Internet is governed, but not in the traditional way that we understand sovereign nation-state governance. Governance is enacted through technical design and via private corporate policies on privacy and freedom of expression. Global institutions like

standards-setting organizations, ICANN, and regional Internet registries wield a tremendous amount of power, but they exist at an international level that transcends government. Multi-stakeholder governance is the constantly shifting balance of power among various forces—national governments, new institutions, civil society, and private companies.

The reason this has worked is because it has been driven in a grassroots manner. Discussions about multi-stakeholderism in international forums often lead to the question of government enforcement of multi-stakeholderism. For multi-stakeholder Internet governance to work, it must remain at a grassroots level lest it convert to multilateral rather than multi-stakeholder.

PAUL BRIGNER

We sometimes talk about multi-stakeholder governance as though it's something that was invented just for the Internet. The Internet evolved from the bottom up because of multi-stakeholder participation. It wasn't invented by governments, it wasn't controlled by governments from the beginning, and, as the Internet grew, it actually created an environment where multi-stakeholder participation could occur in all diplomacy, in all government interactions, and I think we're going to see more and more of that outside of the Internet space. This is not a concept that's limited to the Internet. It's actually a trend that is going to be affecting governance in almost any area.

ANUPAM CHANDER

I'd like to turn from the ITU to another international institution, ICANN. Recently, ICANN has permitted any entity to apply for its own top-level domain. A Turkish company has applied for ''.islam,'' and ''.halal.'' Life Covenant Church has applied for ''.church.'' Will Italians be upset if an American company doles out ''.pizza''? Who decides what is a church or what is halal, or who has ''best.pizza''?

JORGE VILLARINO

The Italian one.

[Laughter]

JOHN KNEUER

Like much of everything around the Internet, this top-level domain (TLD) program grows out of a sort of series of historical accidents, and that's where this multi-stakeholder approach really comes from. So you've got an authoritative root zone, you've got the Domain Name System, you've got registrars and registries, and you've got different organizations that create standards for each of their individual roles, and ICANN is the place where that's all supposed to be pulled together.

One of the things that people had complained about was the limitation on top-level domains, the ''.com'' has the overwhelming majority of the top level domains. They expanded that with ''.net'' and ''.org.'' They expanded to what they call sponsored top-level domains where entities had to come forward and show that they represented a particular group, and so you had ''.museum'' and ''.arrow,'' and those sorts of iterations. And ICANN, trying to perform its dispassionate technical function, found itself in the role of choosing among

competing bids for sponsored domains, as in, ''Well, who's the real sponsor of this domain?'' That reached its peak of controversy around ''.xxx,'' which also swept in all of the content issues that we're talking about. So an entrepreneur put forward they wanted to have the ''.xxx'' domain, and they said that their community of sponsorship was the responsible pornographers of the world, that they would have some certain standards. Then all the real pornographers of the world said, ''Hey, we don't want there to be a '.xxx.''' You had an aspiring pornographer up against the established pornography community, and then you had everybody in the world who was offended by these sorts of things saying this is a bad idea. So as many things in the early phases of ICANN have been resolved through litigation, and ''.xxx'' is an established top-level domain, but getting through that experience, ICANN looked around and said, ''Never again do we want to be in this position.'' So their answer was to say, ''We won't make any judgments of any kind about who sponsors what. Anybody who wants a string can apply for it.'' And they've got a series of complex issues on how to resolve competing strings, and they've got a process through which governments of the world can submit objections.

ICANN has, in its multi-stakeholder model, a place for the governments of the world called the Government Advisory Committee where governments can give advice and ICANN is not bound by that advice, but the entire ICANN model is one of consensus. It works only because all of the constituent pieces agree that this is the place that we're going to coordinate these functions and these activities. If ICANN loses that trust and loses that consensus, that's the primary constraint on its behavior—that it really does have to operate as a consensus organization, or people will go elsewhere.

So the GTLD program continues to have growing pains on a couple of levels. One is that they have not really resolved what they're going to do about objections. Again, this gets to competing areas of views on content in a variety of levels, but most recently the question has been raised, ''Is the stability and the security of the Domain Name System so robust that it can handle infinite numbers of top-level domains?'' VeriSign has the registry for ''com'' and ''net,'' and also the operator of the authoritative root zone raised some technical issues just last week saying ''We're not entirely sure; you ought to go slow.'' So I think going slow makes sense, but now they have introduced a new competitive dynamic in which people say, ''If you're going to do a few, which are you going to do? And how do I get to the front of the line?'' And there are issues around—you mentioned ''.pizza''—giving a generic word to a commercial entity, and could you operate that as a closed network, or does it have to be open? So there remain a great deal of unanswered questions that are not easily resolved, but I think the place to work through these issues remains ICANN.

ANUPAM CHANDER

Ross, Google has applied for some of these TLDs. But is expanding the domain space a good idea? Will it just add confusion for ordinary users like me? Trademark owners complain about cyber squatting in new top-level domains.

ROSS LAJEUNESSE

Our view is that ICANN is actually doing a pretty good job so far, that there are a lot of challenges to doing something like this, but they're doing that in response to the fact that we're losing space on the ''.com'' string. We think there are opportunities by opening this up for innovation and new business models. We are participating in the application process

with that attitude, and some of our applications envision having these generic TLDs as an open registry for others to come in and use. We're intrigued by the idea of, ''What can we do with some of our products if we allow others to have their own string?'' For strings that involve our own trademarks, we would like to see what we can do as far as innovating new approaches to products.

ICANN is not just allowing governments to object; it's allowing anyone to object. It has also appointed an independent objector to be an ombudsman on behalf of everyone's interest out there. So in a true multi-stakeholder way—as opposed to how others might run this—they're trying to be transparent and open about this process.

ANUPAM CHANDER

That brings us to civil society. A year ago, we experienced a mass mobilization against a proposed bill, the Stop Online Piracy Act. The bill ostensibly targeted foreign rogue sites but was written to broadly apply to domestic sites as well. Many in civil society worried that the ideas in SOPA might migrate elsewhere. Should those who criticized SOPA be worried about other venues for its ideas?

LAURA DENARDIS

This is an excellent transition from the TLD discussion because the history is relevant. At one point, there was a single file that mapped all domain names into their associated Internet Protocol addresses. In the early 1980s, the Internet engineering community decided that they needed to expand this, decentralize it, and distribute it. It is now a massively distributed system but one that is hierarchical and has, essentially, a central root point. The Domain Name System is a point of control because it provides authoritative mapping between Internet names and the numbers.

Now the reason this ties in with SOPA—is that SOPA's proposal to use the Domain Name System for blocking intellectual property infringing websites is part of a broader global trend of turning to the DNS and Internet infrastructure, more generally, for controlling content. This co-opting of the DNS for functions for which it was not designed could affect the operational stability of the Internet. The DNS is already used for content blocking, whether for censorship or intellectual property rights enforcement but there is interest in expanding these techniques. What happens now involves a government agency approaching an authoritative registry, such as VeriSign, for example, that operates the ''.com'' registry, and asking them to block or redirect an infringing domain name by altering the IP address resolution. So, for example, a ''LouisVuittonKnockoffs.com'' website can be redirected to an IP address pointing to a website with a law enforcement message. This only works if the registry resides in a country's legal jurisdiction. SOPA was suggesting a method far beyond this that would ask non-authoritative DNS servers operated by Internet service providers, for example, to modify the globally consistent mapping of foreign jurisdiction names into different numbers. Internet engineers warn that such mechanisms would prohibit security-enhancing encryption of the Domain Name System and possibly compromise the Internet's universality. Civil society and policymakers should be concerned about global interest in using the DNS for content control.

PAUL BRIGNER

At this time I was at the Motion Pictures Association of America, and I was serving in a technology policy role, so I experienced this firsthand. I would be very surprised if we see another SOPA-like effort to implement DNS filtering because of the overwhelming outcry from the Internet community and the potential impact on the Internet's stability and operations. The technical community observed that the DNS security mechanism now being rolled out by large Internet service providers would be affected by the filtering in the legislation.

I want to bring to your attention a new initiative involving both content owners and Internet service providers called the Copyright Alert System here in the United States. That system gives a series of warnings to users who are downloading content from peer-to-peer sites that has been identified as copyrighted. So this takes more of an education approach that doesn't involve changing the nuts and bolts of the Internet.

ROSS LAJEUNESSE

What I think is most remarkable about the SOPA/PIPA chapter is the level of engagement of users themselves. We're seeing other examples from the local battles over Uber and taxicab commissions with users flooding councilmember phone lines, to the ITU struggle where we ran a free and open campaign because we thought one of the fundamental issues was the lack of user awareness. The ITU's lack of transparency seemed to be by design. You couldn't get those documents; you couldn't go to that conference room in Dubai; you had to be part of a country delegation even to participate. We were able to get about 3 million users in a very short period of time to engage with their local governments and with the ITU. So I think the most interesting story here is that we're seeing a new way of civic engagement using the Internet as a way to participate in public policy battles.

ANUPAM CHANDER

Last night I was with my family at the Lincoln Memorial and the FDR Memorial, and it was freezing cold, and there was no cab to be found, so I would have loved to have Uber on my smartphone to call a car. But critics of Uber argue that it uses unlicensed taxis. So this pits the historic way that the taxicab industry has been regulated against a new upstart business, and this offers a tension.

ROSS LAJEUNESSE

And it's called democracy.

[Laughter]

That underscores—not to bash the ITU too much—but you've got the Internet enabling massive disruption in an entrenched industry that has captured the regulator. Many of you here in town know about this example: Uber is an app, a livery car service that you put on your phone. It does a geolocation where you are, it tells you where the cars are, and you press the button to call a car. It's not a taxicab. They're typically town cars or SUVs, they're clean, they're nice, and cost about 30 percent more than a taxicab. The taxi operators went to the District of Columbia Taxicab Commission, and the Commission launched a sting

where they gave an Uber driver a huge fine for operating a taxicab without a license. The Commission told Uber drivers that they could continue to operate in the city so long as they charge consumers three times more. So the Commission is not serving the public, but is trying to raise prices to protect their industry.

After Uber reached out to customers, everybody in D.C. who is on Uber was calling in to the Taxicab Commission, and the Commission revisited its decision, and we all still get to use the service. The slightly tortured analogy, though, is that in the ITU world, where you're not talking about the disruption of a taxicab industry, you may still be disrupting industry that the state actually has a direct interest in, whether these are old incumbent monopolies, including broadcast services or content providers. If the ITU ran things, Uber wouldn't be allowed to appear on a cell phone. I think it's an example of the kinds of things that happen when governments try to approach what may or may not be their legitimate concerns indirectly by going to the Internet as an architecture and as a network rather than trying to deal with the underlying policy issue directly.

Anupam Chander

Jorge, I wanted to ask you about the Rojadirecta case. As you know, Rojadirecta is a Spanish website that collects links to streaming video of sports matches around the world. It used top-level domains, ''.com'' and ''.org,'' that have root servers in the United States. After it had been declared legal in Spanish courts, U.S. Homeland Security agents—ICE (Immigration and Customs Enforcement)—seized its domain names in the United States. Its domains vanished from cyberspace for a year or so until, without explanation, they were returned to the company. This case exposes some of the international conflicts that arise on the Internet.

Jorge Villarino

As you said, the appeals courts in Spain declared Rojadirecta.com legal. Why? Because under Spanish law, if you have a website that just links to other websites, even though those websites host illegal content, that's okay, you have no responsibility. The Spanish parliament is now considering a bill that would declare such sites illegal.

Your question pointed to one of the key problems of the Internet: that it is a global space. Whose law should we apply to the Internet? Which courts are competent? Recall the Yahoo case in 2000 between the approach to freedom of speech here in the United States and the approach in France. It was more or less the same thing. The point is that Americans have the technical ability to block access to a website due to the fact that you are the ones who manage the ''.com'' domain. It is difficult to see how to resolve these kinds of problems except perhaps through an international treaty. The American embassy has been lobbying to obtain this reform of the Spanish intellectual property law.

Anupam Chander

That gives an entirely new meaning to ''multi-stakeholder.''

[Laughter]

Jorge Villarino

Absolutely. I had a chance to speak with the American ambassador a couple of weeks ago, and I can understand your government's position. I mean, there are some little companies in Spain that indicate to the content industry that have gone into bankruptcy.

I can understand that they are very much concerned about this. But I don't get to see how we could find a solution for the big problem, you know, what kind of legislations will be applied to Internet when we have this kind of conflict.

Anupam Chander

Ross, I want to talk to you about another kind of conflict between the United States and Europe, and this is in regard to privacy. A few years ago, executives at Google were convicted of privacy crimes in Italy. We see a very different approach, not only in speech, as Jorge mentioned, but also in privacy. The United States NTIA (National Telecommunications and Information Administration) is proposing voluntary multi-stakeholder codes of conduct, while the European Union is proposing an even stricter version of the Data Protection Directive. Are we destined here for a clash of Titans?

Ross LaJeunesse

The case you're referring to is the Vividown case in Italy, which involved a pretty horrible video of the bullying of a disabled student in Italy. It was uploaded to Google Video and as soon as we were notified of it, we took it down because it violated our terms of service. Nevertheless, an Italian court convicted a number of our executives for violating the privacy rights of the victim. I see it not so much as a clash of views on privacy but more an issue of intermediary liability, which is holding platforms liable for the content provided by others. These convictions were overturned this year.

Does it make sense to hold a platform like YouTube responsible for all the content that might be posted on it, especially in a world where there are 100 hours of video posted every minute? It's just fundamentally impossible for us to proactively police that content. We basically rely on our users to flag content for us that might violate our community guidelines, and the minute it's flagged, it goes through a review, and we usually take things that violate the terms of service down within an hour, which in and of itself is a pretty incredible feat when you're talking about that amount of content.

I think intermediary liability is a very real issue, especially with how it intersects with freedom of expression. When you think about intermediary liability combined with things like criminal defamation law in many parts of the world, there is a real concern with regard to freedom of speech and the free exchange of ideas.

With respect to privacy, I think the most interesting thing that's going on in Europe is this right to be forgotten. At its core, it poses a fundamental clash between privacy rights and the right to free expression. When I talk to a lot of Americans about this right to be forgotten, they can't ''grok'' it; they simply don't understand what you're talking about.

JORGE VILLARINO

In some aspects, neither do I.

[Laughter]

ROSS LAJEUNESSE

It's a really interesting example of how mores and ideas about freedoms and rights vary around the world, and it keeps all of us in the policy team at Google very, very busy.

JORGE VILLARINO

The right to be forgotten really worries the U.S. government. Another concern is that the scope of the new European regulation on data privacy will include almost all websites around the world because if you are offering goods or services to data subjects in the Union, you are under European jurisdiction. I don't know honestly know how are we going to handle it.

ANUPAM CHANDER

John, you mentioned security earlier, and it is on everyone's mind. We've had all these espionage issues, including both corporate and government espionage. In South Korea, we saw an attack on the cyber infrastructure recently. Google and the *New York Times* have faced these issues very dramatically. But at the same time, security is often used as a vehicle to do other things, such as content regulation. The Obama administration has just announced a new cyber security program that would involve information-sharing with the U.S. private sector. Everyone across the world is concerned about our cyber security. So there is a real concern here, but there is also a real fear that it could be misused. What are your thoughts on the future here?

JOHN KNEUER

When it comes to the Internet, there is a habit, for lack of a better word, of people looking at things that happen in cyberspace, and rather than trying to apply a real-world analog, assuming that there has got to be something different. When it comes to cyber security, to the extent that it is a crime, we have ways of enforcing laws and proving crimes. The challenge with cyber crimes is typically around attribution. So the issue with information-sharing between the government and the private sector is really just one of basic good management. Cyber crimes are known by their signature, and they change over time, and the private sector is as much a victim, if not more so, than the government. General Motors, I'm sure, is having terabytes of information exfiltrated out of their networks or daily attempts at exfiltration. Understanding what is taking place at General Motors and comparing it to what is taking place at the Defense Department is a good idea.

If the government tries to establish standards for defense of networks rather than simply sharing information and establishing the right incentives, you have a danger that regulatory compliance now becomes an end in itself. The signatures change, everything changes, but the government has said if you're not defending your network in this fashion, you're somehow out of compliance if you run a critical infrastructure. I think that's a negative incentive in

driving the maximal security. And then I think the real challenge is dealing with attribution, applying existing rules on the books, dealing and stealing. We understand how to deal with that. We have now to understand how to deal with someone who steals and goes to another country. You know, vandalism is vandalism. I don't think that we need an entirely new way of defining and talking about these things. The challenge is coming up with rules of attribution, and not even rules, but simply common understandings of attribution. The Chinese have said, ''Just give us the standard rules of the road and we'll follow them. We're just shocked that there is something like that going on around here. We have no idea what you're talking about.''

[Laughter]

JOHN KNEUER

It's the Casablanca casino. So the challenge is to be able to call people out on what happened, here is where it came from. Just because from a technical standpoint, this is extraordinarily difficult, we shouldn't turn to a more blunt tool that erodes the core underpinnings of the Internet in a way that it will have cascading negative effects.

PAUL BRIGNER

I really like the way John framed that. I think that focusing on compliance can lead to complacency, it can make you focus on just those rules rather than looking forward and trying to keep up with what's coming down the road.

JOHN KNEUER

We have a largely successful example of collaboration among many different market participants in the protection of children online. I don't mean keeping children from finding inappropriate things online, but going after the monsters who profit from the abuse of children. There has been increasing collaboration at every part of that chain, including notice and takedown procedures at the registrars and the registries, ISPs, and online payment systems. So where there is general agreement on a norm, there are models for dealing with malfeasance on the Internet.

ANUPAM CHANDER

Now we turn to a lightning round of questions. Before I do that, I want to advertise for the two academics on the panel. Laura DeNardis has a brilliant new book coming out—*The Global War for Internet Governance*—from Yale University Press in August. I also have a book just out from Yale University Press. Like Laura's, my book considers global Internet governance issues.

Now the first lightning question: If we want to follow Internet governance—I'm going to begin with Ross here—what international institutions should we be spending more time watching?

ROSS LAJEUNESSE

We should be paying more attention to the Internet Governance Forum (IGF). It's a fantastic organization that convenes once a year and brings everyone to the table that needs

to be there. It has some issues with funding and governance right now that we are trying to solve, but IGF is the place to be.

LAURA DENARDIS

An international arena not usually addressed in Internet governance discussions, but one in which Internet governance actually takes place, involves the regional Internet registries (RIRs). There are five: APNIC in Asia, LACNIC in Latin America, AfriNIC in Africa, ARIN in North America, and RIPE-NCC in Europe. These institutions manage globally unique critical Internet resources—IP addresses. They have considerable power as the gatekeepers for the resources necessary to access the Internet and, in areas where expanding power might be needed, they would be the logical institutions for additional global coordinating power.

JOHN KNEUER

I'll give you a Google plug indirectly: Google's chief Internet evangelist, Vint Cerf, not only authored the original Internet protocols but was a founding chairman of ICANN and travels the world speaking on these things. I'm sure he's got a Twitter handle.

[Laughter]

JORGE VILLARINO

Well, following what we've been saying, I would say that there is not just one, there are several organizations to follow. But yes, the IGF is the one that involves the multi-stakeholders that we have been talking about.

PAUL BRIGNER

I agree with Ross: the IGF is the primary one to focus on going forward.

ANUPAM CHANDER

Twitter handles that we should follow, Paul?

PAUL BRIGNER

Internet Society, for sure.

[Laughter]

JORGE VILLARINO

The Economist.

LAURA DENARDIS

I'll reiterate—Internet Society.

Ross LaJeunesse

I think Cory Booker is doing an interesting job not just getting the news out, but connecting with his constituents and the media.

Anupam Chander

Now we have time for some quick questions from the audience.

Alain Pellet, Independent Objector at ICANN, spoke briefly, and his remarks are summarized here.

Generic top-level domains raise, not only issues of competition, but ethical issues, which is why I have been appointed. I can intervene on two levels, in the interest of the global community or special communities. I have objected to 26 names now. Anybody can launch an objection before International Chamber of Commerce panels. This is costly. So in these cases, I thought it my duty to intervene. Now, the ICANN process is transparent. I am completely independent. They have never tried to influence me. I have had to invent criteria for when a TLD is contrary to the international public order or community interest. As a law professor, I have adopted a very legal international approach. My criterion has not been freedom of expression because that has nothing to do with international public order. I have posted on my website all my possible objections in order to pre-negotiate. Finally, the process before the ICC panels is obscure.]

A question was asked regarding international enforcement cooperation with respect to cybercrimes.

John Kneuer

The modifier ''cyber'' typically doesn't change the nature of the offense. If you are interfering with somebody's network, you're breaking somebody's property. If you're exfiltrating their data, you're stealing from them. In the national security environment, there are distinctions between Title 10 and Title 50, between covert and military actions. The international rules of the road are when you get caught doing something like that, you take the consequences. With respect to military actions, it's incumbent upon us to make a case to a candid world. This happened, here's who did it, and this is our response, and our response is commensurate with what happened to us.

A question was asked about projects such as the Google Transparency Report that indicate information sharing with government.

Ross LaJeunesse

We generally take the approach that we're subject to the laws of the countries in which we operate. We're a law-abiding company, right? We push back on some of these requests, but at the end of the day, if they have jurisdiction over us, we abide by them. But we say to those governments, ''We're going to tell the world that you've asked us to do this.''

Sometimes regional prosecutors, who were very quick to contact the Google office and say, ''Hey, take down this thing that's criticizing me,'' may not do that quite as often because they know that we put it into the Transparency Report. It doesn't solve the issues entirely, but transparency is helpful.

ANUPAM CHANDER

Thanks to our wonderful panelists for an enlightening session.