CARNEGIE COUNCIL *for Ethics in International Affairs*

The Global War for Internet Governance

Public Affairs, Global Ethics Forum TV Series

Laura DeNardis, Joanne J. Myers

Transcript
Introduction

JOANNE MYERS: Good afternoon. I'm Joanne Myers, and on behalf of the Carnegie Council I'd like to thank you all for joining us.

Our speaker is Laura DeNardis, who will be discussing her recently published book, entitled *The Global War for Internet Governance.*

The rapid growth of the Internet and the risks and rewards this brings are moving issues of cybersecurity and Internet governance to the forefront of policy debates around the world. While most of us are familiar with the issues associated with cybersecurity, for many the term "Internet governance" may be less well-known. Internet governance can be confusing, as it is a broad term which applies to activities on the Internet as diverse as the coordination of technical standards, the operation of critical infrastructure, development, regulation, legislation, and more.

The problems arise because there is no centralized governance in either technological implementation or policies for access and usage, as each constituent network sets its own policies.

Professor DeNardis writes that in its simplest terms, Internet governance is the most direct and inclusive label for the ongoing set of disputes and deliberations over how the Internet is coordinated, managed, and shaped to reflect policy. As such, it includes the activities of many people, including national governments, corporate entities, and civil society.

With so many players, it's not surprising that Internet governance has been contested by many different groups across political and ideological lines. In fact, one of the main debates concerns how to balance competing interests and conflicting values with outstanding questions about who should play a role in defining the Internet's governance and to what extent should they be involved.

Drawing on over two decades of experience as both engineer and scholar of science and technology, Professor DeNardis has been able to seamlessly weave together different aspects of technology and policy. As a fundamental part of the global economy, how we manage the future of the Internet, including access to information, resources, privacy, intellectual property, national security protection, and surveillance, will be decisive in facilitating developments for all users.

Wearing two hats, as Laura does, has given her a front-row seat in imagining how governance issues will play out. Her book, *The Global War for Internet Governance*, is a wonderful guide that will provide an understanding about how this international system can be adequately secured and governed, issues which go to the heart of our economy, stability, and civil liberties.

We are fortunate to have Laura with us to unravel the political intricacies behind Internet protocols so that we all will know what is at stake.

Please join me in giving her a very warm welcome to the Carnegie Council. Thank you.

Remarks

LAURA DENARDIS: Thank you very much for that very kind introduction.

Good evening, everyone. It's very nice to be here, and I want to thank the Carnegie Council for the invitation. It's always wonderful to be in New York. I'm from Connecticut originally, so I feel like I'm home right now, up on the train from Washington, DC.

I have just written a new book, *The Global War for Internet Governance*. I selected a provocative title because I really do believe that conflicts over Internet governance are where political and economic power struggles are working themselves out right now.

Internet control points do exist, and they mediate civil liberties, like freedom of expression and privacy. They are entangled in national security. They affect global innovation policy.

But Internet governance has traditionally been so technically complex, and also institutionally complex, that it really has taken place out of public view—not intentionally out of public view, but it's technically concealed. Much of the work is done by private industry and by new global institutions, such as ICANN, which stands for the Internet Corporation for Assigned Names and Numbers. And much of this has nothing to do with traditional governments, which is what makes it so interesting.

But even though a lot of it has not been visible, there have been recent events that have brought some of these issues into the public consciousness and in front of policymakers in a very acute way. Think about the last three to four years alone.

We had Wikileaks releasing sensitive diplomatic cables, and the aftermath of that was how financial companies cut off the flow of funds to Wikileaks and hackers retaliated against those companies. There's a whole subterranean set of things that happens outside of the realm of content.

Think about down in Washington, Hillary Clinton, when she was the secretary of state, gave a speech at the Newseum, which was called "the Internet freedom speech," calling for private companies in the United States to push back against surveillance requests and requests for censorship from repressive governments.

And then, fast-forward three years. Internet freedom advocates had to experience the cognitive dissonance of that speech versus the revelations that Edward Snowden produced about NSA [National Security Agency] surveillance practices.

So there's a lot more going on. Those were very public.

There was also something in the technical communities that was a great concern. The narrative as it was presented was, "Will the UN take over Internet governance?" There was a conference that was very controversial, called the World Conference on International Telecommunications. It's another acronym—WCIT. There were a lot of concerns about that.

We also had the Internet boycott over the Stop Online Piracy Act in the United States. I read Reddit a lot. I like to go to Wikipedia. I read it a lot. I sometimes update Wikipedia. On that day it was

completely blacked out to protest this proposed legislation. That's just in the United States.

But of course, we have the Egyptian cut-off of the Internet. That really raised the profile of the role of infrastructure. We have had a lot of high-profile hacking attacks, like GhostNet, and we've had revelations about the regime of censorship in China, roughly called the "great firewall of China." And way too many hacking denial-of-service attacks to recount.

So there's a lot happening.

At the same time that we have every system of economic life and social life completely dependent on the Internet to function, we have this loss of trust. It's a loss of trust in technology, in some cases a loss of trust in governments, and sometimes, by default, a loss of trust in the private entities that are involved in the design and administration of the Internet.

One point that I always like to make is that the Internet is already governed. The first chapter of my book is called "The Internet Governance Oxymoron" because it's not necessarily about governments but about other entities that are running various administrative coordinating functions.

This kind of governance has been around since the inception of the network that preceded the Internet, ARPANET [Advanced Research Projects Agency Network]. Someone had to make design choices and figure out the values that would be designed into the system. So these coordination points go back a long way.

But another point I like to make is that there is not one single system. It's not one system. I say that because I often get asked, "Well, who should control the Internet? Should it be Google, the U.S. government, or the United Nations?"—a question like that makes no sense on its face because there is layer upon layer upon layer of design, administration, distribution, coordination issues.

That's what motivated me to write this book, is to try to explain where the Internet already is governed and what is at stake in this governance and what is at stake in some of the open global debates that exist right now.

I think what I'd like to do today is to go through some examples of how the Internet is already governed and then maybe raise a few issues, some of the debates that are going on around the world, and what might be at stake.

I always like to start with this issue. It's the most technical issue, so if you will allow me to start there, I would like to.

It's the management of critical Internet resources, which usually is a term to describe domain names—like cnn.com for example or american.edu or lauradenardis.org—these have to be globally unique. And also Intranet addresses, which are binary numbers, which just means a series of zeroes and ones, that is necessary in order to send or receive information on the Internet. Similar to the postal system, we have a unique address and that's how people find us—except it's not physical, it's virtual; it happens in the computer systems, and it's logical in nature.

So what's political about this? It's a technical area, but the global struggle over who controls Internet names and numbers has actually been a very longstanding issue. Power struggles have reflected tensions over new global institutions and their role, like ICANN for example, as well as the private companies that are involved in the governance.

A key feature is that the Department of Commerce in the United States has retained a historic relationship with this function, through having a contract within this organization ICANN, which I'll say a little bit more about in a minute, and also by having authority to update some of the technical functions that are involved in translating the names that we understand when we type in cnn.com and the numbers that a computer understands when it's routing information around the world.

So what is ICANN? It's a private non-profit organization. It's incorporated in California. It has oversight of names and numbers. It ultimately has oversight over the distribution of these numbers, although it is further allocated to regional Internet registries around the world that further allocate the addresses.

There are also a lot of private companies that take care of the mapping between names and numbers. They are called registries.

If you saw the Go Daddy advertisement—Danica Patrick is one of the spokespeople for that—they are called a domain name registrar that hands out domain names.

There are a lot of institutions. This is just one small area of Internet governance. But you can get a sense of all of the different entities that are involved in the management.

What are some of the political implications of this area, because it is highly technical and it's a little bit esoteric? I'll give you a few examples.

Who should control or who should be able to use united.com—United Airlines, United Arab Emirates? I'm not a sports fan, but is it the Manchester United, United Van Lines? And who decides? Well, this institutional system does decide.

Sometimes there are very onerous trademark disputes that happen. There is something called typosquatting, where someone might intentionally, instead of coke.com or pepsi.com, someone might try to get pepsy.com—I'm just making up a hypothetical example. But these kinds of things happen.

Another example of how this is very political is the authorization of what are called new top-level domains. What's a top-level domain? That's an area of naming on the Internet, such as .com, .edu, .gov—you're familiar with all of these. When you type in a domain name, you sometimes type in those various suffixes that represent an area of organization of naming on the Internet.

Who authorizes the development of new top-level domains? It's this institution, ICANN. What's controversial about that? Well, can .xxx be authorized or .sex be authorized? There are freedom-of-expression issues. There are issues of public interest and child protection and law enforcement that come up in that, and really just interesting conflicts that can arise, for example, between a private company and a territorial entity like a government or a region.

Recently, someone proposed, "I'd like to manage .amazon"—and, not surprisingly, it's the company Amazon. Well, the countries that have the Amazon rainforest within their borders said, "Wait a minute." There was a controversy over .patagonia for the same reason.

I could actually go on for hours and hours and hours about the conflicts in that area. But I find it very fascinating, because here we have public interest concerns ranging from freedom of expression to the protection of innovation and trademark, and we have this private non-profit entity that has done a fairly good job of keeping things operational but always under the microscope and always with

symbolic and real concerns about the connection between the U.S. government and this entity.

So that's one area.

What about standard-setting, another technical area? This is another technical but also political area.

What is an Internet standard? Things just don't work without having some kind of blueprints that tell them how to exchange information. Do you remember the days of the proprietary online systems of the 1990s, when you couldn't exchange email if you were on Prodigy with your friends who were on America Online; or, going back further than that, when businesses, if they used, for example, an all-IBM environment, maybe couldn't exchange information with networks that were all DEC?

It was a very interesting and important move to have interoperability made possible by universal and open standards that manufacturers can use to design computing devices that can interoperate. That's an economic issue.

You've heard of a lot of these: Internet protocols, Internet standards. What are some examples? WiFi, MP3, HTTP, and then a whole lot that most people have never heard of. There really are quite a few of these.

Many of the core standards are set by institutions, such as the Internet Engineering Task Force, which goes back a long way; the World Wide Web Consortium. They are almost never seen, the specifications. They're not software. They're not hardware. They're blueprints, so you can see what they are.

It's very important to have openness in how they are constructed, allowing corporations to bring their expertise in, talk with other people in an open environment, and come up with these specifications. How they are set is important because they do have innovation implications, but also political implications.

What would be an example of a technical standard having more of a sweeping political implication? The easiest examples are encryption protocols that make decisions about things like encryption strength and they mediate law enforcement values versus issues of securing information—always global values in tension.

What about an area such as developing accessibility standards for the disabled? The World Wide Web Consortium is involved in that.

And who has heard of BitTorrent? BitTorrent is a protocol that was just designed to have efficient file sharing, but it's always closely associated with piracy because it's used often to illegally download movies and video games and music. It's also an interesting area and also one that's technical.

And then, of course, cybersecurity governance is an important area as well. Beginning in 1988 with the Morris worm, which took down an approximate 10 percent of the Internet—does anyone remember that? I was actually at Cornell at the time as a graduate student. It originated from another Cornell graduate student who was in my building, which is kind of an interesting history for me. It really got me interested in cybersecurity. It was a really big deal at the time and it drew public attention and policymaker attention into the area of cybersecurity.

But fast-forward to today. Attacks have gotten a lot more sophisticated. We have Stuxnet, which was used to take down—I don't know the particular details, and no one really knows all the details in the

public—Iranian nuclear facilities, or a certain aspect of that.

Now, who is responsible for cybersecurity governance? This is an area that is both public and private. The private sector really does handle a lot of security. But there are also private/public institutions, like computer emergency response teams. I have a chapter on that in the book. I find it very interesting.

Then there's the issue of interconnection. This week, or in the past week, there has been a lot in the news about Netflix and Comcast directly interconnecting their networks. You've probably read about that. That has to do with interconnection.

Everyone in this room knows that the Internet is not a cloud. When we sometimes talk about it with students, we draw a cloud. That doesn't make any sense. I don't know why we do that. It's not actually a cloud. It has a physical architecture, it has transmission facilities and switches, it has equipment that's housed in buildings with a Coke machine and raised flooring and air conditioning and people.

The Internet is made up of interconnected networks. It's not one network. It's a series of networks, most of them private networks, that make agreements to connect and to conjoin, either bilaterally with each other or at shared Internet exchange points.

So this is a very important area of Internet oversight because it involves a lot of coordination and it typically exists outside of government view and inspection. It's mostly a private area. But it determines the physical infrastructure and the virtual infrastructure of the Internet. So I enjoy that area as well.

Now, here's one that you'll know about, the policy role of—I'll just use the term that I normally use—private information intermediaries. That's just a fancy way of saying Facebook, social media companies, search engines, reputational systems like Angie's List and Yelp and RateMyProfessor, which is one I like to go to. These are reading systems, they're search engines, they're social media, information aggregation sites like YouTube and like Flickr.

These are not providing content but they facilitate the sharing of content. Most of them provide free services and make money through systems of online advertising.

But all of them establish public policy. You can think about many examples of this.

One that I write about in the book is constantly changing privacy policies of social media. I have my students read all of the privacy policies every semester because often we just check and say "I agree." But it is really interesting when you read those.

They make decisions about hate speech and what should be removed, about cyber-bullying. They are in the front lines of intellectual property rights enforcement, like copyright and trademark issues. So all of them do establish policy. They're enacting governance.

There are many taxonomies for understanding the functions of Internet governance. This is just the one that I like to use, the issues that I mentioned.

And then, one other, the issue of the relationship between Internet infrastructure and intellectual property rights enforcement. Traditional online enforcement of protecting copyright by going after a person or by going after the content itself sometimes does not work in the digital environment.

So there has been a movement to have Internet service providers have something called "three strikes" approaches that can cut off access. There has been a notice-and-takedown procedure on YouTube. It's a very complicated area. But think about a time when you've been to YouTube and you've seen "this video has been taken down because of a copyright violation."

Google has some obligation to take it down under this notice-and-takedown. In exchange for that, they have immunity from liability for copyright infringement that occurs on their site.

This is a very interesting area.

And of course, there are intellectual property rights that are embedded within the technology itself, such as sometimes patents that can underlie standards; trade secrecy, where we don't see Google's search algorithms, for example; and then the trademark issues that I mentioned with the domain name system, like who has the right to various names.

My book addresses what is at stake in all of these areas. I find it incredibly fascinating. I can't get into all the issues, but what I wanted to do is provide some common themes among all of those.

The first theme among all of these examples is that arrangements of technical architecture are also arrangements of power in modern society. I've mentioned that the complex institutional and technical scaffolding is somewhat behind the scenes, but nevertheless they embed political and cultural concerns.

A second theme is that Internet governance infrastructure—the technologies, the architecture, the infrastructure—is increasingly becoming a proxy for broader political struggles and for control of content. Think about why that would be.

Nation-states around the world—and Internet governance is a global issue—have lost control over content. Repressive governments want to suppress the media, they want to censor information. They have to turn now to technical infrastructure to do that.

Media companies have lost control of the monetization of their own content to a certain extent because of piracy, so they are turning to infrastructure to do that.

An extreme example is the Egypt example that I mentioned, where access was cut off entirely.

So that's the turn to infrastructure as a proxy for political disputes and problems.

Another theme, the final theme that I'd like to mention here today, is this issue of the privatization of Internet governance, the privatization of governance. So we have technologies that transcend borders, we have private companies that manage a lot of aspects of these technologies. But that's not all. It's not only private.

Governments perform antitrust. You want the government to come to your aid if you have been the victim of identity theft. They respond to Internet security threats. They enforce child protection measures. They enact privacy laws. But most of the functions of Internet governance that I mentioned, on the front lines at least, is the purview of private industry. So private companies manage the mapping of names into numbers. They make up the majority of the Internet's backbone. They set standards for the Internet. They are carrying out these core functions, not only in these functions, but also as actors that are forced to respond to political events on a global stage.

There is delegated censorship, where a country asks a private company to take down information.

They ask search engines to remove links. They approach social media platforms to delete defamatory material. And as we know, they approach Internet service providers and social media companies to turn over information about individuals for national security or law enforcement or other political reasons.

So what do we have here? We have delegated surveillance, delegated censorship, delegated copyright enforcement, delegated law enforcement in general. It has shifted governance, for better or worse, to the private sector, which creates challenging issues for the private sector that is forced to deal, not with one government, but with a hundred governments making requests in different legal structures, in different political contexts, and with different norms.

That's a challenging role to play. But the bottom line is that much of Internet governance does either originate in the private sector or is delegated to these private entities from governments.

What I would like to do is to highlight a few of what I see as some specific challenges to Internet governance and some of the debates that are going on now around the world.

One has to do with the possibility of Internet fragmentation. We think of the Internet as being one network, although you could easily argue that we don't have a universal Internet now, because if you are looking at the Internet and English is not your first language, it looks completely different to you than if English is your first language. There are digital divide issues. There are systems of filtering and censorship. So you could argue that we don't have a universal Internet. But, at the technical level, we have the building blocks of a universal Internet and we have a great degree of technical universality.

I am concerned about Internet fragmentation. This can be a very technical issue, but the easiest way to understand it is through a lens of something political, like the Snowden NSA disclosures.

There have been a lot of reactions to this. What were some of the initial reactions?

- Wanting to route around the United States, wanting to bypass Internet exchange points that are in the United States, walling off Internet services to try to stay within a country, either in cloud computing services or applications.

- There was an initial call in Brazil, as I understand it, to store Brazilian customer data within the Brazil borders.

- Some German telecommunication companies initially suggested walling off the Internet in a way that could stop the NSA's surveillance.

So you see these kinds of proposals, including cloud computing proposals, and it raises the question of whether we will have a universal Internet or whether we will move to a more fragmented environment. I raise this as a very real issue because, as I mentioned before, it was a very difficult move to go from lack of interoperability to having interoperability. So I'm very concerned when I hear about proposals that would fragment the Internet.

A closely related challenge is the question of—I'm going to use two strange words—whether we are going to continue to have multi-stakeholder Internet governance versus multilateral Internet

governance.

Right now there are layers upon layers of Internet governance functions. Some are done by these new institutions, like ICANN; some, as I mentioned, are the purview of government; some are done by private industry; some are done by all and are multi-stakeholder. But if you look at this in its entirety, that's called multi-stakeholder governance. It's what keeps the Internet running.

Well, there are also concerns and proposals, not just in response to the Snowden issue but other things in the world, to have greater government regulation of the Internet in a variety of different areas. It's very important to pause before having greater regulation because it's really not that easy, the engineering is really not that easy, to keep things running.

So the question has to be asked, not whether there needs to be more government oversight of Internet governance as if it's one thing, but looking at specific areas and seeing what is the problem that folks think needs addressing. So what is the problem in the area of surveillance or in privacy or in standard setting? What exactly is the problem to which these proposals are responding is what I like to say.

I will say a few caveats, though, about this term multi-stakeholderism.

Even though I'm an advocate for multi-stakeholderism, it's important to not elevate that as a value in and of itself, which sometimes happens, rather than as a possible approach to meeting a public-interest objective.

Also, multi-stakeholderism is not appropriate in every one of the areas of Internet governance that I mentioned. I want the government to step in if I am the victim of identity theft. Other areas, things run very well with the private sector running it.

So this one-size approach of multi-stakeholderism does not apply in every environment. It's much more nuanced than the quick sound bite.

I also want to mention that sometimes the discussions about multi-stakeholderism are really just about how we talk about Internet governance rather than how Internet governance actually occurs—like who's allowed to come to a conference and discuss Internet governance. These discussions take place while the actual practice of Internet governance occurs. So that can be very interesting to follow, and I do go to a lot of the conferences, and I know some people here go to these conferences as well.

One final point that I'd like to make is just remember it's not a single system, it's very complicated. A lot of people like to describe it as an ecosystem, an Internet governance ecosystem. It's not a monolithic system, not a one-size approach.

Do we want to transform from multi-stakeholder governance to multilateral governance? It's not a given that things are going to remain secure and stable. So it's important to approach this in a nuanced way and to have it be in a functional way, based on function.

So there are a number of open issues to watch in the coming years. I'm going to be watching them. I'm very fascinated as an academic scholar, being a person who observes this and studies it. There are a number of open issues.

But the truth is that right now the Internet is governed. This governance has been in a constant state

of flux for decades. It's a very powerful area of authority because we have the technical mediation of the public sphere. So democracy takes place online, and then we have the privatization in some sense of the conditions of civil liberties within that public sphere.

So the governance is not fixed any more than architecture is fixed. It's constantly changing. It makes me uncomfortable but also excited about it.

I have used up my time. I hope I have provided some insights into the politics of how Internet governance already works, and I hope that my caveats about fragmentation, about multi-stakeholder governance, and some of the other caveats have contributed some food for thought about the relationship between the future of Internet governance and the future of innovation and Internet freedom.

This is an important issue. In my opinion, the stability of the Internet should rank among other collective action problems that involve the world, like environmental protection, human rights, and basic infrastructural systems of water and energy.

I appreciate the opportunity to speak here today about this because public engagement in the issues is critical considering what's at stake. Thank you very much for listening. I'm very much looking forward to the question-and-answer session. Thank you.

Questions

QUESTION: Allen Young.

Who finances all these private-sector initiatives and how can these private-sector initiatives be accountable? Who is accountable when they decide various issues?

LAURA DENARDIS: That's a very good question. I'll answer it in one area, to give an example, standard-setting. The truth is that private companies spend a lot of money sending their employees to standard-setting organizations. So there's a big investment that is paid for by those companies. Ultimately, that expense gets passed on to people who buy the products.

But the other part of your question is, where do you find the legitimacy for the privatization of these kinds of functions? In the area of standard-setting, I would say that legitimacy, in part, comes from expertise and from the experience of keeping things running.

But it also has to be procedural. What are the procedures that can create the legitimacy to have the private sector making decisions that affect all these public-interest areas?

One area of procedural legitimacy would be to have openness, open participation in the development of standards. So if you look at an organization like the Internet Engineering Task Force, which sets a lot of Internet standards, anyone can participate.

There is also a sense of legitimacy in that they publish the standards for people to see. That's an issue of economic liberty, where companies can take the ball and run with it and develop products based on those standards, and the public and policymakers have the ability—not many of us read standards, but we have the ability to see them. Having that openness and transparency is part of the accountability.

But it's a very complicated area, the question of legitimacy, and it varies from area to area.

QUESTION: Susan Gitelson.

As I listened to your very sophisticated analysis, my brain went in another direction. I couldn't help thinking about individuals in small countries out there. We're talking about the United States and China and Russia. What about the Netherlands or Cambodia or Peru or Belgium, which has a language conflict, and so forth? How do people have a chance to communicate with each other and not be affected so much by all these regulations?

Another question is, you're an academic. Google decided to reproduce so many publications without asking the authors and not paying that much attention to copyright. Now, what happens to writers and musicians and others who find it very difficult to get paid for their ideas because certain companies have just borrowed them wholesale?

LAURA DENARDIS: I'll tackle the last one first. I don't know that I have that much to say about the first question, but I'll try to respond to it because it's an important open question.

Piracy is rampant. When I am in a roomful of students, I often ask this question: How many of you in the room have never illegally downloaded a song? Nobody raises their hand.

I will say that I have never illegally downloaded a song. But I think I'm an anomaly. Part of that is because I am an Internet governance scholar; part of it is because I'm a musician. There are a lot of issues here.

But the truth is that there is a lot of leakiness of information. In intellectual property rights the pendulum has swung really far, I think, in terms of protecting the creators of a work, in terms of law. But the technology, because it's so easy to replicate and distribute information, has swung in just the opposite direction. All the laws of copyright, of trade secrecy, and trademark apply online.

And they apply to Google. Google actually spends a lot of time taking down information that violates copyright if they are notified that they have to take something down.

On this issue of openly publishing academic documents, I'll just give you my own personal feeling about that. I think it's crazy that I write an article and people peer review it and then my institution has to pay for it and the public can't read it. I don't think that makes any sense.

Models need to change. Music needs to adapt to the new leakiness environment. There are new business models that are cropping up to protect musicians and artists and creators. But I think it hasn't caught up yet.

So you raise a very real dilemma. You can understand why the owners of copyright want to go to technical infrastructure to block sites.

An example of that: I mentioned the domain names mapping into Internet addresses before. That's a simple system that involves—I say "simple" in a really sarcastic way, because there are 100 billion of these resolutions a day, more than 100 billion. Well, now there is interest in going to the system that maps Internet addresses to domain names to block sites like—I'm just making up one—louisvuittonknockoffs.com, to use the domain name system to block these trademark-infringing sites. So it's a game of Whac-A-Mole, where you have new ways of leakiness and piracy, and also creative fair use of media that's manipulated in some way, and then the technology trying to keep up with it.

It's going to go around and around for a long time. Thank you for raising that issue.

QUESTIONER: And what about the poor people in Belgium who might want to communicate or not communicate with their neighbors?

LAURA DENARDIS: I think the Internet has worked really well in most of the world. I travel all over the world and I enjoy the fruit of that and get online in all parts of the world.

They are affected by some of these things but not all. But I think some of the debate that I have raised, like Internet fragmentation, for example, could affect people in all parts of the world.

They would be affected very much, for example, if we suddenly go to an environment where content companies have to pay to connect in parts of the world. Some large content companies might decide, "I don't want to do that in the developing world because it's not lucrative." So you can see how they could be affected to a greater extent than the West.

But I feel like the Internet has worked fairly well and is growing. There are huge digital divide issues that are being addressed by national governments and non-profit organizations, but a lot more work has to happen in that environment.

QUESTION: My name is Mike Koenig, Long Island University.

You mentioned the issue of fragmentation. In the literature I see that frequently described as the walled garden problem, that the Internet is likely to become a set of walled gardens. When I look at those articles and editorials, they seem to cluster into two groups: one group is concerned about national governments, and the other group is concerned about the Googles and the Yahoos and the other corporate organizations. Where do you think the largest danger lies?

LAURA DENARDIS: I think that right now there are some threats to interoperability that come from the private sector, if you look at some of the things that are happening on the ground, because there are new models that are not geared towards universal openness and interoperability.

I would actually say that something simple like a social media platform, if you look at how the social media platforms operate—and I'll just overstate this—it reminds me of those proprietary online systems where sometimes you don't have the same interoperability that you do with email and other traditional applications.

There also is sometimes a turn toward proprietary standards that are based on a corporate standard rather than through standard-setting organizations. So there are issues there.

But in terms of looking forward into the future, I think that the biggest threat will come from governments who are trying to address—policymakers are trying to address a lot of these challenges and catching up to the fact that the Internet is now so important for our economic and political life, and that there is a risk of them going too far to protect and to set up national walled gardens.

I don't want to live in an environment where we have a national internet as opposed to a universal Internet. So, thank you.

QUESTION: Daniel Stein.

I'm wondering if you could expand a little bit on the privacy aspects of it. People in different countries have different relationships with their government in terms of what privacy is protected, and if you are

talking about international Internet, where those privacy controls, as more of our lives are going online, how that relates for people in America versus anywhere else.

LAURA DENARDIS: Every government and region has a different approach to privacy and there are different norms, even when law doesn't address it, to privacy. So, for example, in the European Union, there are very strong privacy protections. Sometimes that is more of a cultural norm than freedom of expression. So protecting the individual, the right to delete yourself from the Internet, is very, very important culturally and it is enshrined in law to a certain extent.

In the United States, it's a very different environment, where freedom of expression is a value that is privileged in some ways over other values.

So it varies from country to country. This presents a complex dilemma because businesses that do their business in all of these different regions and countries have to figure out how to do that.

It's the same thing, I would add, with censorship and with what information is allowed to be online and what isn't. So for example, in parts of the world it's not okay, if I'm stating this correctly, to sell *Mein Kampf*, I believe, or to deny the Holocaust. In other countries, hate speech is opposed by the full force of the law. In other countries, including in the United States, we have the right to say some real—we're being videotaped right now, so I won't say some of the things that are privileged that would be illegal in other countries. But it's very malleable. So you have all of these different laws.

And then you also have norms having nothing to do with the law, where different platforms have different norms about how to manage content and the privacy of individuals. Are we allowed to have anonymity in a platform? That's platform-specific. Do we need a real name identification? Do we have options to turn off the gathering of data about us, like our location, based on the iPhone or phone number?

I would encourage everyone to go back and read the privacy policy of the social media application you use the most, whether Twitter or Facebook or WhatsApp or any of these, and see the types of information that is gathered about us.

A lot of that happens in the platform as well as having the regional and national differences.

QUESTION: Thank you very much for your presentation. My name is Eduardo Ulibarri. I am the ambassador of Costa Rica to the UN. So I represent one of those small countries that the lady had in mind when she made her interesting question.

I must say that from our national point of view—and of course Costa Rica is one country and there are other countries—we feel better with the current system than with the government-governed system in Internet, because we have followed the discussion over the years and we have come to the understanding that some countries are interested in the regulation of Internet not necessarily for having a better order but sometimes for control. But the fact that we feel better with the current system doesn't mean that we feel good at all.

So my question is whether you foresee some sort of ideal way of governing the Internet, especially in the future, so that it could be technically feasible, that it could be sustainable, and it could be open, as it has been so far, to the changes that might occur in the future?

LAURA DENARDIS: Can I ask you a question before I answer?

QUESTIONER: Sure, of course.

LAURA DENARDIS: What do you see as your number one concern in Internet policy from your perspective in your country?

QUESTIONER: I would say basically privacy is one, the fact that it's very permeable to the efforts of different countries in order to get data, and also the private sector as well. The major challenge that we foresee, which is a national challenge, is how to bridge the so-called gap of the people who have access and those who don't have it, and in the future the possibility that there might be control of the free flow of information and exchanges. Those would be the major challenges.

LAURA DENARDIS: Thank you.

My personal opinion is that the way that the universal Internet should be governed is through multi-stakeholder governance. If you think about Internet governance the way I do—and there are many other ways to think about it—I include the design of technology, the administration of critical Internet resources, all kinds of public policy issues, ranging from the protection of children to privacy issues, defamation—a whole host of issues.

I think that the reason that the Internet has been successful has been because it hasn't been developed by governments, it has been developed by the private sector in cooperation with and sometimes with funding of governments, and then the ecosystem of Internet governance that has arisen over time has been multi-stakeholder.

Again, depending on which area we're discussing, there is input of civil society, citizens are engaged in some way. You can raise the question of how can citizens be meaningfully engaged. But I think we saw with the SOPA (Stop Online Piracy Act) example that citizens can make a difference. And then having the private sector lead in certain areas.

So I think that keeping a balance of powers is the best way to preserve the stability of the Internet. Again, though, it depends on what area of Internet governance we are talking about.

The big question for the world is: What does multi-stakeholder governance look like in each of these areas? It's a very big question. And then, how do you provide legitimacy in the different areas and get input and have adequate transparency where necessary? Really, that's the crux of the difficult question in Internet governance, is what is the balance of powers in any one particular area?

QUESTION: Edward Marschner.

I have to ask you the question that your students must ask you after you've made them read all those privacy policies: What do we do with this information that we've just obtained? We learn that they are sweeping up all this stuff and we are supposedly agreeing to let them sweep it all up. What can we do? Do we *not* click and refuse to accept it and then plan to negotiate with them on a better privacy policy?

LAURA DENARDIS: This is a much more difficult-question crowd than I normally get. That is a very hard question.

I think individuals don't have very much power at all to push back against privacy. What we used to hear is "well, just don't use that." But now, in order to participate in social life and economic life and political life, we need to use platforms. Many of them have the same types of privacy issues.

What's the limit? What's the limit of the data that can be collected? I think we're almost at the point where we don't have the option of reasonable anonymity online, but we're not there yet.

In parts of the world, there are real name identification requirements to use a cybercafé. Countries are talking about having a real name identification, like a user ID, to get online. We can stop those types of things and provide for the possibility of anonymity.

But I feel like the best that we can do is to have traceable anonymity, where data is gathered about us and law enforcement can request it with a judicial order, with some kind of due process, and having a system where there are constraints and checks and balances. I think that's the best that we can do at this point.

Why is all that data gathered about us, by the way? The reason all that data is gathered about us is because of the Faustian bargain that we've made. We use everything for free—I use free email, I use free search, I use free social media, I use free information aggregation devices.

But it's not that money is not changing hands. There is an enormous amount of money changing hands. It's online advertising. Because of that system of online advertising that is the business model that provides all this great access to knowledge, that's why the information is gathered, that's why governments can come in and request that information.

I think part of the solution is in some of these efforts that are being undertaken in the private sector in cooperation with civil society to say, "What does corporate social responsibility mean and what kind of user choice can there be?" A very complicated area.

I think that I should have some right to turn off some of the tracking. That's my personal opinion, and I know a lot of people agree with me. But on the other hand, I do realize that the business models depend upon a certain amount of data gathering.

But when it starts to get into tracking our location, the creepiness factor goes up—I just call it the creepiness factor. So there have to be some limits and some choice.

Are there any easy questions?

QUESTION: Yes, a really easy question. My name is Eva Schweitzer. I write for German newspapers.

I have been following this whole debate about the NSA in Germany. The debate is not so much *whether* Germany can wall off the Internet but if Europe *can* do it because it is, of course, something that needs to be done. Is it even possible? And if so, what would be the consequences? Is it possible to have a European Internet which is walled off, totally walled off of course from America, so that nobody even needs to use an American server anymore?

LAURA DENARDIS: I don't think it's technically possible. That's my honest opinion. I don't think it's something that should be desired in the first place. There might be other ways to do it.

But why can't it be walled off? Because there is a distinction between physical infrastructure and logical infrastructure or virtual. So what you can do is you can have tight controls around the physical infrastructure, but ultimately, if someone wants to use Google or gmail, that information is going to eventually get to other servers elsewhere. So I just don't see how it's possible. I would love to look into that issue in greater detail.

But I don't think a European Union-centered Internet is possible. I think that there are some possibilities for things like data protection for data storage in particular areas, whether that's e-health or things that are of a very sensitive nature that can be stored and localized on servers at the application level.

But if you look at the Internet in total, I don't think it's possible. But it will be interesting to see where the debates go.

QUESTION: My name is Amr Aljowaily. I am an Egyptian diplomat and I participated in both phases of the World Summit on the Information Society[WSIS].

With the title of your lecture, one would have expected at least an addressing of the outcome of that summit, for the simple reason that it is the first time, and probably the only time, unfortunately, where governments have come together with a wider multi-stakeholder environment to speak about the political aspects, the economic aspects, the social aspects, more or less the "information society," as the title of the summit is.

Reading the two outcomes of the two phases of the summit—it took about five years of negotiations, very, very arduous negotiations, where the consensus outcome of the United States and Egypt and other countries gave their approval for it.

This hype about "governments want to take over the Internet" and so on just becomes—I think, if one reads the 20 or 25 pages that the world has reached as a set of principles, the set of principles and two plans of actions—very reasonable ideas where the multi-stakeholderism is recognized but also it is recognized that on some public policy issues the legitimate role of government is there.

An example for that would be cybersecurity, or ICT security, as now being addressed by governments, including the United States and others, within the UN framework under the so-called Governmental Group of Experts on ICT Security Issues, which has been a member in the last session and will be a member in the upcoming session.

So I think there is also some need for reason when addressing the issue of what governments can do and what the private sector can do and what the civil society can and should do. Rather than eliminating one particular set of actors, we should look at what the appropriate role of each set of actors is. I was wondering if you have any further thoughts on that.

LAURA DENARDIS: I'll be very happy to comment on that. I address WSIS extensively in the book. It's not something that I mentioned here today in 30 minutes. But I gave a whole list of things that are appropriate for the government here, and that's my opinion.

I will say I don't agree with you that governments handle cybersecurity. I just don't. Companies handle their own cybersecurity. There are some regulations about that, like in finance, but the banking industry secures the banking industry. And telecommunication companies, at least in an environment where it's private telecommunication companies—it would be different if it's a state-owned company—they're securing their networks. And even private citizens have to constantly upgrade their software.

So I would say I don't think that is a government area. I think it's much more nuanced.

QUESTION: Yu Bum Kim, grad student at NYU.

As an aside, as a South Korean, I think using sensitive personal information to identify yourself to use Internet services is a terrible idea because there have been a lot of data leaks in Korea.

But back to the question. When we talk about governance, a big part of governance obviously, intuitively, is establishment of laws and standards and the enforcement of said laws and standards. In my classes when we discuss this sort of subject, we have always discussed the hypothetical universal global standard of laws for conduct in cyberspace.

We see that people use cyberspace differently. You mentioned that you see it as an international and global network, whereas certain nations are more inclined to view even cyberspace as a sovereign space essentially, where a part of what happens on Russian sites, say, is Russian prerogative.

So with these conflicting views in mind, do you think we can really approach any sort of universal legal standard for conduct in cyberspace, with trolling, denial-of-service attacks, hacking all becoming more and more prominent?

LAURA DENARDIS: What's your field of study?

QUESTIONER: Transnational security, and I'm concentrating on cybersecurity matters. I'm still a little bit new at it, so I don't have all the nuances down yet.

LAURA DENARDIS: Excellent. Great. That's an excellent question and another difficult question.

I think that it depends on if you are talking about content or technology. I think that there can be a lot of universal agreement about the nature of the technology and the possibilities for interconnection and interoperability and security. I think security is an area where there can be a lot of agreement. How you implement that is another question.

At the level of content, though, the nation-specific laws really do come into play in a big way. There are different amounts of censorship in certain countries from other countries; there are the surveillance issues; intellectual property rights enforcement is another area that's a little bit more harmonized. So for security and intellectual property rights enforcement we have seen some harmonization and norms in that area.

But on the content-specific issues—and if you go to work for Google, for example, you may be in a situation of, wow, we have all of these different countries and you have to be operating under the laws of those different countries.

But if you look at the transparency reports of companies, they sometimes publish statistics about the kinds of requests that they get. You'll see that there is a disconnect between the number of requests for personal data information, for example, and how much they actually turn over. That's another area. It's a lever of power that can be implemented, sometimes for very good reasons.

JOANNE MYERS: I have to thank you for really introducing us to this very complicated topic.

Audio

Who controls the Internet? Internet governance is so technically and institutionally complex that it takes place mostly out of public view. But Internet control points do exist, and they affect civil liberties, national security, and global innovation policy. Laura DeNardis explains how the inner workings of online governance and discusses its future.

Video Clip

Who controls the Internet? Internet governance is so technically and institutionally complex that it takes place mostly out of public view. But Internet control points do exist, and they affect civil liberties, national security, and global innovation policy. Laura DeNardis explains the inner workings of online governance and discusses its future.

TV Show

Who controls the Internet? Internet governance is so technically and institutionally complex that it takes place mostly out of public view. But Internet control points do exist, and they affect civil liberties, national security, and global innovation policy. Laura DeNardis explains the inner workings of online governance and discusses its future.

Read More: Corporations, Business, Ethics in Business, Global Governance, New Media, Private Sector Development/Corporate, Technology, Global, United States