COLUMBIA | SIPA
School of International and Public Affairs

Global Commission on Internet Governance
ourinternet.org

Proceedings of the

Conference on Internet Governance and Cyber Security

Italian Academy
Columbia University, New York City
May 14-15, 2015

School of International and Public Affairs (SIPA), Columbia University
In collaboration with the
Global Commission on Internet Governance (GCIG)

Proceedings of the

Conference on Internet Governance and Cyber Security

Italian Academy, Columbia University Campus
May 14-15, 2015

Table of contents

Letter from the SIPA Dean

On May 14-15, 2015, the Columbia University School of International and Public Affairs held a **Conference on Internet Governance and Cyber Security** in collaboration with the Global Commission on Internet Governance. This document represents the summary Proceedings of this unique and important gathering.

Held at a critical juncture with respect to many Internet policy issues both within nations and globally, the Conference brought together one of the most important and varied groups of leaders in this field that has ever assembled in New York City.

Leading academics, influential policy makers, entrepreneurs, legal experts, technologists, and corporate executives assembled from around the world to explore the significant policy questions related to Internet governance and cyber-security, including issues of governance, security, privacy, freedom, innovation, trade, and many others.

Over the course of two days of keynote lectures, panel discussions, and networking sessions, the goal of this Conference was to stimulate thought, identify key issues in Internet policy, develop concrete recommendations around areas for research and policy action, and ultimately drive progress in the global public interest. The summaries herein were prepared by next generation scholars.

This Conference was hosted as part of SIPA's initiative, Tech & Policy @ SIPA, which is a multilayered engagement that includes: developing further a data and technology-focused curriculum for students, new academic research, challenge grants to support data and technology focused applied solutions to global urban problems, and a start-up lab for student entrepreneurs.

As a leading school of global public policy, situated in one of the world's great research universities, SIPA serves as an interdisciplinary hub for global public policy research, training, and engagement.

I wish to thank the generous support of our Conference sponsors, including Carnegie Corporation of New York, Microsoft, the Columbia Institute for Tele-information, and our co-host, the Global Commission on Internet Governance.

Merit E. Janow
Dean, School of International and Public Affairs
Professor of Professional Practice in International Economic Law and International Affairs
Columbia University

Executive Summary

CONFERENCE OVERVIEW

On May 14-15, 2015, the School of International and Public Affairs (SIPA) at Columbia University hosted a major conference in collaboration with the Global Commission on Internet Governance (GCIG) to examine critical issues associated with Internet governance and cyber security.

This *Conference on Internet Governance and Cyber Security* occurred at a time when policymakers are faced with pressing technology-related issues around privacy, security, innovation, international trade and cross border data flows, human rights, freedom of expression, among many others.

This conference brought together an outstanding group of individuals: leading Columbia University faculty from SIPA, Columbia Business and Law Schools, the School of Journalism, the School of Engineering, GCIG commissioners and affiliated researchers; influential U.S. and international policymakers, entrepreneurs, legal experts, technologists, and corporate executives from around the world.

What follows is a summary of each session produced by next generation scholars working at the intersection of technology and public policy. Conference participants were invited to identify a forward-looking agenda for policy and research in the areas of

 Day one of the Conference on Internet Governance and Cyber Security.

Internet governance and cyber security, the core ideas of which are summarized herein.

CONFERENCE TOPICS

As described below, the span of the topics discussed at the Conference on Internet Governance and Cyber Security was vast. This vastness reflects the need for a multidisciplinary approach so as to consider their political, economic and social dimensions and consequences.

Table 1. Panels and respective topics, May 14-15, 2015

	Day 1: Internet Governance	**Day 2: Cyber Security**
Morning	Opening keynote discussion: Internet governance and Cyber Security	Opening joint-keynote discussion: Cyber Security
	Plenary panel 1: Examining the Future of the Open and Universal Internet	Panel 5: Mitigating Cyber-risks in Critical Infrastructure: Private and Public Responses for the Financial Sector
	Plenary panel 2: The Future of Multi-stakeholder Internet Governance	Panel 6A: Nuclear vs Cyber: Conflict and Deterrence
Afternoon	Fireside Chat: An Examination of U.S. Policy and Law in a Global Landscape	Panel 6B: Cyber Security and the Internet of Things
	Panel 3A: Human Rights, Freedom of Expression and the Internet	
	Panel 3B: Trade, Internet Governance, and Cross-border Data Flows	
	Panel 4A: Privacy, Big Data and the Internet	
	Panel 4B: Innovation and the Internet	

* The full agenda, with speakers, is contained in Appendix 1.

AREAS FOR FUTURE POLICY RESEARCH

Several unifying topics or questions emerged over the course of the discussions: the consequences of further Internet fragmentation; the use of multilateral trade agreements as a vehicle for global Internet governance rules; security at different levels; defining and developing a multi-stakeholder approach to Internet governance; and maintaining the operationality of the Internet given the technical constraints.

Consequences of further Internet fragmentation

The future of an open and universal Internet is far from certain. At a global level, the model of governance that will define the Internet is still up for debate, which the delay in the IANA transition clearly demonstrates. At the national or regional level, a variety of policies are being implemented to require citizens' data to be held domestically (Russia), to require filtering of search results based on the 'right to be forgotten' (Europe) and attempts by law enforcement agencies to access data held in foreign jurisdictions (United States), among many other examples. These evolving domestic frameworks and the absence of a global framework were major focus areas throughout the conference.

The discussion revealed that it is still far from clear what the consequences of this fragmentation will prove to be. Part of this uncertainty derives from the various ways in which fragmentation might occur (at the infrastructure, logical or content layers), the various policies introduced at the national level that can result in fragmentation, and how different national legal systems might or might not interact given these diverging rules.

Indeed, there was no agreement as to whether further fragmentation would net costs or net benefits. For instance Eli Noam (Columbia University) opined that the creation of multiple Internets might result in loss of scale and technological efficiency in the short term but, in the long-term, these losses might be outweighed by additional technological dynamism. Other panelists cautioned that fragmentation could lead to several undesirable ends, such as erosion of trust in Internet institutions; reduced consensus among stakeholders; national law conflicting with Internet standards; and attempts to embed policy solutions into Internet protocols.

This debate is generally viewed as a very important one and far from settled. To provide a basis for more informed policy discussions, further research could usefully focus on the possible impact of Internet fragmentation on the basic functionality and the underlying principles of the Internet.

Use of the trade system and agreements to govern the Internet globally

One recurring idea at the conference was the notion that trade agreements could provide a promising avenue for maintaining an open and global Internet governance architecture.

At present, a number of multilateral trade agreements are under negotiation or ratification, including the Trans-Pacific Partnership (TPP), Trade in Services Agreement (TiSA) and the Trans-Atlantic Trade and Investment Partnership (TTIP). While the full contents of each agreement are not yet known, some include chapters relating to e-commerce, telecommunications and cross-border data flows.

These agreements are promising avenues for maintaining an open and global Internet. Trade agreements potentially provide benefits to those who partake in them. They allow for uniform laws and regulations to be implemented across several jurisdictions at once,

reaching into industries and sectors that are in many cases highly regulated on a national level, such as telecommunications. Achieving this level of uniformity and coordination would otherwise be extremely difficult if negotiated bilaterally or if left to the devices of national industry regulators.

Some argued that this approach, using a “carrot” of trade agreements, is more likely to bear more fruit that one involving a “stick,” in other words, punitive measures that coerce national governments into participating in and supporting a universal, global Internet governance regime. Indeed, punitive or coercive approaches used for this goal undermine the very values on which this system is meant to be built.

Ensuring security at multiple levels

Cyber security is commonly associated with addressing cyber-crimes by organized criminals, cyber-attacks between nation states and common hacking methods such as phishing. However, Conference discussions demonstrated that the common understanding of cyber security needs to widen.

For instance, Brad Smith (Microsoft) explained that the very conception of “security” has to go further to one that encompasses “safety” on the Internet. He urged policymakers to recognize the multiple objectives that need to be achieved: keeping the public safe, keeping data secure, and protecting people’s privacy.

Fadi Chehadé (ICANN) urged a greater focus on the “integrity” of the Internet, with security being just one aspect of integrity. He framed “integrity” as a combination of dexterity, stability, resilience and truthfulness. Not ensuring the “integrity” of information, identities and domains, would erode the complex web of trust and authenticity between people, institutions and information, which underpin the universal and open nature of the Internet.

In each case, policymakers must make trade-offs, as is the case with any policy issue, though at present these tradeoffs are not well enough understood to enable sensible policy decisions. Research is required to better understand a wider understanding of “security” and the trade-offs that must be reconciled due to the adoption of this wider understanding of “integrity.”

Developing a workable, multi-stakeholder governance system

The global Internet governance system must include a diverse range of interests. This has been termed a “multi-stakeholder” model up until present but, given this term’s political connotations, and the expanding scope of what are considered Internet governance issues, a recurring theme throughout the conference was that it might be time to jettison this term in favor of another one.

Putting the semantics aside, the more complex operational issues relating to the functioning of the governance system need to be resolved. Questions to which answers are required include:

- Which layers and organizations/mechanisms for decision-making require greater participation?
- Who decides who will participate in these mechanisms or organizations and according to what criteria?
- What will be the various participants' roles and responsibilities?
- What will participation entail?

Of particular concern is finding ways to include the views and interests of those who are not part of the system. For instance, Prof. Christopher Yoo (University of Pennsylvania) pointed out that needs are different for different populations connecting to the Internet. He contrasted the needs of the four billion people in the world who do not have Internet access (the "have-nots") with the three billion who do (the "haves").

This message was echoed by Dr. Fen Hampson (CIGI), who built on an earlier point about finding ways to include the human rights interests of those who are not yet connected to the Internet, by referring to the "fish swimming outside the net." In other words, national laws only apply to the citizens of the nation in question.

Finding clear answers to these questions is hard enough; finding workable solutions is even harder. However, both will be required if an open, universal Internet is to be achieved. Research in these areas would be helpful in developing answers and workable solutions.

Maintaining the operationality of the global Internet given national policy goals

At various points throughout the discussions, it became evident that there are many valid concerns – such as public safety – and values – such as freedom of expression – that need to be respected in how the Internet operates. However, it is also evident that respecting these concerns and values might not be technically feasible and – if technically implemented – could undermine the open and global characteristics of the Internet.

For example, the need to police content on social networks – in the context of the spread of radical, violent or libelous comments – certainly acts in the interest of public safety. However, at the same time, the implementation of measures to remove or moderate content – such as the "right to be forgotten" in Europe – can have negative effects on freedom of speech or access to information. Moreover, these policies act at a national level and, when governments attempt to apply their national laws outside of their own borders – as France has attempted to do with the "right to be forgotten" vis-à-vis Google – these policy decisions subsequently undermine the open global nature of the Internet.

Another example can be seen with attempts at data "localization," where governments mandate that technology companies operating within a given jurisdiction must physically store the data of the citizens of that country in data centers within the country. The common justification for these moves is to maintain the privacy and security of citizens' data. Even if this policy is politically feasible the technical implications are not. The entire architecture of a global technology company's operations must be altered to meet

these requirements, at great cost. This can have profound effects on innovation and international trade. The outcome of this kind of policy is to undermine an open and global Internet, as it explicitly involves discriminating between data based on national origin.

The challenge in any of these cases is developing and implementing policies that reconcile the diverse interests and needs of key stakeholders, and the resulting outcomes can put in tension the fundamental attributes of an open, universal Internet.

At this point in history, it is not clear how to reconcile these positions. Research is needed to better understand the interplay between the technical, economic, political and social factors at play to develop workable policy solutions that balance each stakeholder's interest at the national and global levels and that also consider the collective interest in maintaining an open and global Internet.

Opening Session, Day 1: Internet Governance

Drafted by Guilherme Alberto Almeida de Almeida

Moderator:

Merit E. Janow, Dean, SIPA, Columbia University

A conversation with:

Vinton G. Cerf, Vice President and Chief Internet Evangelist, Google

Lawrence Strickling, Assistant Secretary for Communications and Information, U.S. Department of Commerce

Laura DeNardis, GCIG Director of Research and Professor, American University

EXECUTIVE SUMMARY

The opening session examined fundamental questions surrounding Internet governance and cyber security. Panelists discussed current challenges in how the Internet is governed and considered different approaches to meet those challenges. The challenges included: the risk of losing the current universal Internet – as the one and only network-of-networks – to a more fragmented and segmented Internet of sub-networks; the loss of trust in the institutions that govern the Internet; and the need to build security into the very architecture of the Internet itself. Themes for future research include: 1. Exploring cyber security and issues of trust; 2. Considering Internet governance as an ecosystem; and 3. Exploring the threat of fragmentation.

BACKGROUND

The Internet is, by design, hard to govern. An intentionally decentralized, redundant network of networks, the Internet itself represents a type of ecosystem. As such, the best way to appropriately govern the Internet is to first understand the rules of the system, and then consider governance structures that support them.

A central challenge stems from the fact that not every nation agrees about what these structures should be. Moreover, after recent events such as the disclosure of the U.S. National Security Agency's global surveillance program and the cyber-attack against the movie studio Sony Pictures, there is a fierce debate around what rules or practices should govern. The public now understands that nation-states, not just hacker groups, carry out secret surveillance programs and massive cyber-attacks. After these

revelations, public trust in the institutions traditionally responsible for Internet governance diminished significantly. And trust between nations – suddenly aware that even allies leveraged the Internet against other allies – eroded as well.

This diminished trust between citizens and governments and also between governments themselves is mirrored among Internet governance institutions. For instance, at the 2012 World Conference on International Telecommunications, several countries supported a new form of Internet governance that would give their own governments far greater control over managing critical Internet resources through an increased role of the United Nations in Internet governance matters – a so-called multilateral model. However, just two years later, at the NetMundial conference, a majority of nations were in favor of continuing with the multi-stakeholder model of Internet governance.

Further complicating the picture, in 2014 the U.S. Department of Commerce announced it would waive its historical oversight position over the Internet's domain name body, ICANN – the Internet Corporation for Assigned Names and Numbers. While this move endorses a shift toward what has been called the global multi-stakeholder approach, it is unclear to what extent government-led or inter-governmental organizations will provide oversight of ICANN's functions.

All of these factors – a global sense of mistrust among the public, disagreements among nations over who is in charge and who should be – combine to form a complex battleground over Internet control that will require careful examination by experts in several disciplines. Issues that must be considered include privacy and extraterritorial reach; data residency and data retention practices; national regulatory initiatives and international legal frameworks, amongst others. Until these issues are addressed, the risk of a fragmented Internet increases, jeopardizing both its global nature and

Keynote speakers during the opening session (in order from left to right): Merit E. Janow, Vinton Cerf, Lawrence Strickling and Laura DeNardis.

undermining its basic functionalities.

DISCUSSION

Merit E. Janow, Dean of Columbia SIPA and panel moderator, opened the keynote discussion by asking participants to discuss what they felt were the most pressing and critical questions that require answers today in the areas of Internet governance and cyber security.

Cyber security and Internet safety

Vint Cerf, Chief Internet Evangelist for Google, opened the discussion by focusing on the need for collaboration among stakeholders in both cyber security and Internet safety. Cerf felt that collaboration is relevant because every single company is dependent on other companies' software. Since no one company can protect itself exclusively through its own actions, addressing security breaches requires combined effort. Laura DeNardis, Professor at American University and GCIG Director of Research, framed the Internet governance system, including Internet stability and security, as a global collective action problem, at the same level as governance of the environment and human rights. As the Internet reaches a greater portion of the world population, there is increasing global dependency on information technology. This means that Internet policy issues in many areas have taken on ever-greater relevance.

Cerf suggested that the discussions on cyber security should go beyond the traditional national security and defense issues. They should also focus on Internet safety, since safety is closer to the users' concerns. He described safety as both a technology issue and a law enforcement problem. Technical issues, such as bugs and bad design, lead to vulnerabilities, exposing users to threats and attacks. Efforts should be made to deal with the root causes of this problem, as opposed to the current approach of dealing with the symptoms.

Solutions must include: better environments for writing code and better programming assistance to detect problems before deployments; cryptographic methods for strong authentication of devices and people; and for stronger protection of information on the Internet. Cerf cautioned, however, against the development of 'backdoored' encryption technologies. He argued that they're not a good solution to prevent misuse, as backdoors could enhance vulnerabilities. Moreover, law offenders would keep using non-backdoored alternatives regardless.

Internet governance – an ecosystem

A broad concept, the multistakeholder model, as defined by DeNardis, describes the balance of power between private industry, international technical governance institutions, governments and civil society in Internet governance matters. The multi-stakeholder Internet governance model has served effectively since the initial creation of the Internet, particularly given the Internet's global nature. The multi-stakeholder model works through open meetings that engage hundreds of people in a transparent

and collaborative process. It has led to a powerful set of proposals delivered by the community.

DeNardis reminded the audience that there is not one single system of Internet governance: in effect, there is an ecosystem that involves different systems, such as critical Internet resources, standard settings and interconnection, among others. These systems comprise a number of different functions, performed by a large number of organizations, with different associated governance models. While technical issues are necessary to keep the Internet operational, political issues are also involved, because the decisions made within these governance structures may affect civil liberties. Thus, we should ask what the appropriate system of governance is within each function, rather than look for a homogenous system for all governance activities.

Because of this ecosystem structure, it is difficult to simply legislate the way it works: it is necessary to recognize that rules will be implemented in varied ways around the world, with different results. Cerf emphasized that the rules that derive most value from the Internet are as general, as implementable and as interoperable as possible. The multi-stakeholder model should be considered as a way to tackle varied controversial issues, such as the different international perspectives on privacy. It permits interchange and thus represents an effective governance model with higher chances of reaching a consensus.

Lawrence Strickling, Assistant Secretary for Communications and Information at the U.S. Department of Commerce, represented the institutional perspective, focusing on the challenges of global Internet governance. He underscored the dispute between those who believed that governance should be decided by national governments and the proponents of a multi-stakeholder approach. The success of the multi-stakeholder policymaking process is evidenced by the way the Internet has expanded and thrived. Its effectiveness will be tested once again by the full privatization of the domain name system. The main challenge of the community-developed ICANN transition plan is to establish a way to ensure that the involved actors will perform adequately and people will be protected in the absence of the U.S. national oversight of such functions.

Fragmentation: a threat to the Internet's principles and basic functionalities

The panel expressed deep concern over fragmentation – the idea that the current model of a single, universal Internet could splinter into several, smaller Internets. Fragmentation, should it occur, could, at least, create barriers to the free flow of information online and at worst, degrade or destroy the basic functionality of the Internet.

Panelists highlighted some of the potential causes of Internet fragmentation, such as: erosion of trust in Internet institutions; reduced consensus among stakeholders; national law conflicting with Internet standards; and attempts to embed policy solutions into Internet protocols. Individually or combined, these actions could, the panelists argued, jeopardize the Internet's integrity.

Politicization further heightens the potential for fragmentation. Governments, who have in some cases inserted themselves in Internet governance mechanisms, threaten its reliability where the technical community previously performed this role. Data localization policies are another example of fragmentation practices. Such practices often do not match the way technology works. As such, these localization practices could lead back to a world of proprietary and independent systems, to the detriment of a broader, universal Internet.

DeNardis expanded on this idea, noting that arrangements of technical architecture are arrangements of power in the public sphere. In this context, governments have used the infrastructure to cut off access to citizens, to enact surveillance, to promote denial of service attacks, to filter content, or to enforce intellectual property rights. Thus, politics influences the governance of critical Internet resources. As a result, some government interventions may be harmful to innovation and civil liberties, in addition to being a threat to the stability of Internet architecture.

NEXT STEPS FOR RESEARCH AND POLICY

Three key themes emerged from the panel discussion that would benefit from deeper research:

1. Cyber security and trust: Research questions might include:
   a. What mechanisms can be employed to restore trust among nations, citizens, and global institutions?
   b. What are the appropriate degrees of legal, technical, or institutional changes necessary and/or desirable to ensure data transaction and storage security?

2. Internet governance as ecosystem: Research questions might include:
   a. What are the outer limit parameters to ensure the functioning of a global Internet? Which structures within the Internet are “load-bearing walls” that Internet governance bodies must protect, and which are flexible structures that individual nation-states can adjust without threatening the functionality of the global system?
   b. In what ways can governing bodies such as ICANN define and enforce structural support rules to ensure the well-being of the Internet ecosystem?

3. Fragmentation as threat: Research questions might include:
   a. How can international Internet governance institutions influence or incentivize nations to invest in and protect the open, universal Internet? How can the private sector contribute to this goal?
   b. If influence and incentives fail, what mechanisms remain (for international governance bodies, nations, private sector, etc.) to protect the open, universal

Internet? How can such mechanisms be tested? What are the consequences of failure?

Plenary Panel 1: Examining the Future of the Open and Universal Internet

Drafted by Alexis Wichowski

Moderator:

Eli Noam, Professor, Columbia Business School

Panelists:

Leslie Daigle, former Chief Internet Technology Officer, Internet Society; GCIG Research Advisory Network member

Jacquelynn Ruff, Vice President, International Public Policy and Regulatory Affairs, Verizon Communications

Andrew Wyckoff, Director, Directorate for Science, Technology and Innovation, OECD; GCIG Research Advisory Network member

Christopher Yoo, Professor, University of Pennsylvania Law School; GCIG Research Advisory Network member

EXECUTIVE SUMMARY

This panel examined how current Internet regulatory structures allow for equal access to the Internet. Panelists discussed the benefits of an open and universal Internet, including fostering innovation and entrepreneurship as well as international trade, all which may be threatened in the event of further fragmentation. The challenge is to find a mechanism that ensures an open and universal Internet without adopting so many regulatory restrictions that the private sector would lose the incentive to engage in necessary investments in expanding broadband infrastructure. These mechanisms need not imply or mandate uniform technologies. Rather, the development and deployment of many different technologies, which achieve the open and universal properties of the Internet, would be preferable.

Themes for future research that emerged from the panel discussion include: 1. Identifying multi-stakeholder roles for Internet regulation; 2. Exploring ways to globally govern the Internet informed by better statistics on international data flows; and 3. Discovering mechanisms that support an open and universal Internet versus strict mandates.

BACKGROUND

The Internet has become, as Professor Eli Noam, the Director of the Columbia University Institute for Tele-Information and panel moderator, described it, “too important for governments to leave alone.” It supports the economies of nations. It hosts commerce, scientific research, social and community structures. And it does so both within and across national borders. Governments, private industry, individual citizens and social groups all have stakes in how information flows across the Internet, many of whose interest may at times be at odds with one another.

Who governs the Internet, then? Who should? These have become among the most pressing questions of our time. These questions frame the first panel discussion entitled, “Examining the Future of the Open and Universal Internet.” What an “open and universal Internet” actually entails, simply put, is that “consumers can go where they want, when they want” online, according to the Federal Communications Commission (FCC). As enshrined in the FCC’s recently adopted Open Internet rules on February 26, 2015, broadband providers cannot block, throttle, or permit paid prioritization for content on either fixed or mobile connections. In other words, everyone in the United States – the only citizens under the FCC’s jurisdiction – should be able to access the same content, at the same speed, as everyone else.

While the FCC’s Open Internet decision supports an open and universal Internet for people residing in the United States, the global debate on the issue is far from over. Authoritarian countries continue to block access to content deemed controversial within their own borders. Private industry continues to push for the right to prioritize some content delivery – with so-called “fast lanes” – over others. And while international Internet governing bodies such as ICANN and the United Nations’ International

Panelists (from left to right): Jacquelynn Ruff, Leslie Daigle, Eli Noam, Andrew Wyckoff and Christopher Yoo

Telecommunications Union (ITU) can convene leaders to debate the merits of an open and universal Internet, they cannot enforce all nations to adopt whatever guidelines they decide upon.

As a result, the Internet may become increasingly fragmented, providing users with different access to content at different speeds, depending on the users country of residence: the Internet in China would allow access to different content than the Internet in Finland than the Internet in Mexico than the Internet in Ireland, by way of a few examples. The notion of multiple "Internets" is a critical one, as it is increasingly a reality. Due to various factors – degree of government censorship, broadband infrastructure development, status of trade agreements, amount and kind of investment incentives for the tech sector – it seems increasingly possible that the Internet will become a different experience for citizens of different countries, depending on their nation's status along the aforementioned spectrum. How and why does this matter?

DISCUSSION

Role of the Internet in modern era

Noam opened the discussion with the idea of the existence of an Internet orthodoxy, with its associated dogmas, founding fathers, sacred texts, and belief systems. Internet advocates see the Internet as a force, one that disrupts the existing order, but also a force that disrupts itself over time. Yet this orthodoxy and the conformity that it requires is, in a way, a conservative position. The creation of multiple Internets, due to fragmentation, might result in loss of scale and technological efficiency in the short term but, in the long-term, these losses might be outweighed by additional technological dynamism.

As the Internet has become a central part of society, economics, and politics, Noam suggested, governments cannot simply allow the Internet to disrupt – instead, some sort of regulatory order becomes necessary. As different governments have different national priorities, it is, then, unsurprising that they might approach regulating the Internet in different ways. Noam posits that the fact that there is any uniformity in Internet regulation between countries at all is, in some ways, the real surprise.

The question, Noam proposed to the panel, is how can we deal with this challenge? Noam suggested that this problem is perhaps best viewed as a creative opportunity, rather than an intractable problem – the chance to find an overarching system in which different systems can co-exist.

Universal properties of the Internet

Leslie Daigle, former Chief Internet Technology Officer at the Internet Society and GCIG Research Advisory Network Member, asserted that the Internet is currently universal, given that this is less a function of a specific set of technologies, but rather properties, and that these properties should be preserved. It is the choices we make, Daigle proposed, that will determine whether we have a universal Internet going forward.

Daigle noted that openness and universality need not necessarily be preserved through uniformity. Rather, citing the example of possible new protocols (superseding TCP/IP), the global reach and integrity of the Internet could be improved upon without mandating the maintenance of existing technologies.

Serving as the unofficial representative of the private sector, Jacquelynn Ruff, Vice President, International Public Policy and Regulatory Affairs at Verizon focused her comments on how infrastructure and investment related to this debate. For the Internet to be truly globally accessible, Ruff argued, private companies need to invest in expanding the infrastructure for access. For instance, in a few years, half of the 4.5 billion mobile phones will be smart phones. This will requires companies to invest in upgrades to mobile networks. Ruff asserted that the investments would be most incentivized with a "light-touch" approach by government regulators. Ruff described the FCC's recently released 'Open Internet rules' in the United States as "unfortunate," and posited that the policy decision might have benefitted from a more multi-stakeholder decision-making process.

Trade & innovation

Andrew Wyckoff, the Director of the Directorate for Science, Technology and Innovation at the Organisation for Economic Co-operation and Development (OECD) and GCIG Research Advisory Network Member, addressed the question from the perspective of its impact on commerce. He urged the audience to examine the issue along the spectrum of development and consider the cost-benefit for 1. Innovation and entrepreneurship and 2. International trade.

On the technical characteristics of an open Internet, Wyckoff listed the end-to-end principle, intelligence residing on the edges of the network, and the network being "agnostic" in the way it treats data. These characteristics have impacts on science given that scientific research is increasingly making use of heavy data; and these large data flows are shared through the open Internet. Shutting down universal access would limit this flow of necessary data. Wyckoff also noted that scientific collaboration takes place over the Internet. With a fragmented Internet and increasingly federated Internets – plural – this would limit orthogonal thinking and thus impede scientific discoveries.

International trade is another area that would be damaged by losing an open Internet, Wyckoff contended. He argued that very little trade is done in final goods anymore, but rather through intermediaries as a part of complex global value chains. By limiting data flows, the trade benefits of an open Internet will decline quickly.

Internet "haves" and "have-nots"

Christopher Yoo, a professor at the University of Pennsylvania Law School and GCIG Research Advisory Network Member, pointed out that needs are different for different populations connecting to the Internet. He did this by contrasting the needs of the 4 billion people in the world who don't have Internet access (the "have-nots") with the 3 billion who do (the "haves").

The 3 billion Internet "haves" are more concerned with greater competition of connectivity, more forms of connectivity, and more applications, Yoo noted. They not only have access, but they have multiple, redundant avenues of access to the Internet – through phones, desktop computers, tablets, etc. For the 4 billion "have-nots", competition among access points is irrelevant; they're trying to get a single connection. Thus, Yoo argued, the regulatory response for the 4 billion "have-nots" should be focused on facilitating investment to get them connected.

This diversity of needs amongst several groups can also be seen in areas like financial services, where required levels of trust, bandwidth and reliability are well in excess of the capacities of the public Internet. As a result, many financial services companies have exited the public Internet and now operate private networks of their own.

The corollary of this is that an open and universal Internet is not the same to everyone. Very different and tailored regulatory responses are thus required to respond to the different needs of the heterogeneous groups that use the Internet.

NEXT STEPS FOR RESEARCH AND POLICY

The various contributions from the panel experts suggested that preserving an open and universal Internet in the future requires more research in three key areas:

1. Multi-stakeholder roles for Internet regulation: Research questions might include:
    a. How can governments incentivize private sector investment in infrastructure, especially in the rising mobile industry?
    b. How can governments develop and implement targeted policy agendas that accommodate the specific needs of different groups of Internet users (e.g. the financial industry's need for fast connections)?

2. Global-level policy: Research questions might include:
    a. How can existing data collected on a national or regional level be collected and analyzed to reveal the tangible values of a universal Internet (e.g. economic value generated from cross-border collaborations) and to better inform the government and private sector regulatory process?
    b. To what extent do trade rules or bodies potentially play a role in maintaining an open and universal Internet at a global level?

3. Mechanisms versus mandates: Research questions might include:
    a. What examples or mechanisms from other industries have been effective to encourage opt-in standard setting (e.g. standards associations) and how can they be applied to Internet regulation?
    b. What mechanisms would enable governments, international regulatory bodies, and the private sector to collaborate on infrastructure and standards development?

Plenary Panel 2: The Future of Multi-stakeholder Internet Governance

Drafted by Fernanda R. Rosa

Keynote and Moderator:

Ambassador David Gross, Partner, Wiley Rein

Panelists:

Kathryn Brown, President and CEO, Internet Society

Fadi Chehadé, CEO and President, ICANN

Beth Noveck, Director, NYU GovLab; GCIG Commissioner

Paul Twomey, former ICANN Chair, GCIG Commissioner

EXECUTIVE SUMMARY

This panel examined multi-stakeholder Internet governance from multiple angles. Panelists discussed the importance of including the range of key stakeholders in determining future Internet governance processes. Panelists also considered how the content layers (as opposed to the infrastructure or logical layers) pose new challenges to the governance system, highlighting the importance of maintaining "Internet integrity" in the face of these challenges.

Themes for future research include: 1. Developing inclusive models for Internet governance; 2. Accounting for cultural differences in deliberation; and 3. Mechanisms to ensure legitimacy in governance systems.

BACKGROUND

Multistakeholderism, as defined by Laura DeNardis, Professor at American University, describes the balance of power between private industry, international technical governance institutions, governments and civil society. However, as it is a broad concept, this term is at times associated with different entities: government-led, private sector-led, or simply diffused widely across various stakeholders. This term is flexible in that it can refer to decentralization – for instance, as a proxy to describe the diminishing role of the United States in Internet governance – or can refer to more centralized processes, depending on which group of stakeholders is being referenced.

The most pressing issues in Internet governance today are openness, collaboration, inclusiveness, and respect for human rights. (Verhulst, Noveck, Raines and Declercq, 2014). During the ITU Dubai meeting in 2012, stakeholders debated whether the Internet should be governed using the "multi-stakeholder" model or whether a United Nations based 'multilateral' model should be instituted instead.

The IANA transition – the transfer of the Internet Assigned Numbers Authority from a single country, the U.S., to an international body – lies at the center of this debate. Transferring ownership or management to a global multi-stakeholder community is one potential model for Internet governance in the future.

DISCUSSION

This discussion, moderated by Ambassador David Gross, Partner at Wiley Rein, centered on the meaning and utility of the term "multi-stakeholder," the cyber security risks to the logical and content layers of the Internet, the need for a more accurate composition of today's Internet users in the leadership of Internet governance organizations, and leveraging expert networks over the Internet.

Multi-stakeholder meanings

Panelists discussed the challenge of the term "multi-stakeholder." Used in different contexts and with different interpretations, the term itself makes debates over the future

of Internet governance even more challenging.

Kathryn Brown, President & CEO of Internet Society, described the multi-stakeholder model as a process. This process defines how to derive an Internet governance model that is sustainable, trusted and transparent. Brown argued that the groups defining Internet governance today involve many different players, including engineers, entrepreneurs, communities and civil society. As such, the current state of Internet governance is a product of collaboration. Since these groups all have legitimate stakes in the functions and processes of the Internet, Brown contended, the ecosystem has worked well until now.

Gross asked if the multi-stakeholder process, broadly defined, is working or if the rise of government regulation is a reaction to a perceived failure of the current processes? Brown argued that the processes have not failed. Rather, she suggested, while there are areas where governments should assume a role, it should be part of the existing, consensus-based, "bottom-up" and organic process of decision-making. They should not, she argued, impose a new, "top-down" model.

Fadi Chehadé, CEO and President of ICANN, claimed that since "multi-stakeholder" is more a label than a practical or useful concept, it had little value in actual policymaking for the Internet.

Questions over the role for governments

Chehadé described how, years ago, some stakeholders sought for the ITU to take over some of ICANN's functions. Today, however, this wave of calls for a multilateral governance system, led by governmental institutions, seems to have passed. He argued that there exists a general consensus that a multilateral governance system would not be the best alternative for a future Internet governance model. That said, he reaffirmed that it will be necessary to include governments in the future system.

Brown also spoke about roles that national governments should have in the Internet decision-making processes. Chief among these responsibilities are avoiding cyberwar and privacy across boundaries, where it is necessary to have interoperability and standards. However, even in these cases, it is crucial to consider other actors from outside the governments, who are relevant for the processes, she argued.

(Mis-)representation in Internet governance

Paul Twomey, former ICANN Chair and GCIG Commissioner, said that the multi-stakeholder groupings of today reflect the 1990s, when these organizations were created. While many aspects have changed since then, he argued, the strategies and the characteristics of Internet governance have not.

Twomey provided contextual background to support his argument. He explained that from the year 2000 to 2014, the proportion of global Internet users shifted. In the U.S.

Panelists (from left to right): David Gross, Kathryn Brown, Fadi Chehadé, Beth Noveck and Paul Twomey

and Europe, the proportion decreased: from 26% down to 9% for the U.S. and from 29% down to 16% for Europe. However in other regions, the proportions went up. China, for instance, went from representing 6% of global Internet users up to 21%.

Despite this shift in Internet users by country, Twomey noted, the composition of the ICANN board has yet to shift. Currently, 33% of the board is from the U.S., 27% from Europe, while less than 4% is from India and 1% from China. In other organizations, he noted, the US is even more prominently represented: 46% in the Internet Society, 60% in the Internet Architecture Board, and 56% in the Internet Engineering Task Force's board.

Twomey noted that the number of Internet users is not a perfect metric to assess representation. However, the figures do raise doubts about the ability of these organizations to respond adequately to the needs of the current composition of Internet users.

In addition to representation, the current ICANN bodies do not account for cultural differences between East and West. These governing groups he argued, tend to be modeled on Anglo-Saxon/Northern European processes and discussion formats. One of the great challenges for the multi-stakeholder organizations moving forward is to adapt to the needs of different cultures' approach to deliberation processes.

Ensuring Internet integrity

Chehadé emphatically argued that the logical infrastructure of the Internet remains safe, resilient, and well governed. The real problems will emerge, he suggested, on the content layer. This is the layer where applications are run and where most Internet users engage the network. The application layer, which is more open than other technical layers, will be difficult to control and govern. Using this perspective, Chehadé suggested that governments need to learn how to manage emerging challenges across various policy areas, such as new communication platforms (e.g. YouTube) or new business models (e.g. Uber).

Gross pressed the panelists to discuss the much-disputed topic of how applications should be regulated. He asked the panelists if they were concerned about global uniformity or fragmentation. Chehadé thought that the content layer should be governed by market forces first and foremost, and "top-down" standards or regulations should be avoided.

He also pointed out that security is just one aspect of integrity. As such, we must expand the conception of cyber security to look more broadly at Internet integrity. He described how people have begun to doubt the Internet and World Wide Web's dexterity, stability, resilience and truthfulness. As an example of the dissatisfaction with it today, Chehadé mentioned the purchase of a top level domain by the Catholic church: *.catholic* in Arabic, Chinese and Latin letters with the objective to guarantee the authenticity of the church-related websites.

Leveraging networks of experts online

Beth Noveck, Director of NYU's GovLab and GCIG Commissioner, explained how technology has changed governing around the world, citing examples in the United States, India and Brazil. She described how Internet-enabled technologies permit diverse, alternative and innovative approaches to deal with complex policy issues. These new tools permit the involvement of numerous stakeholders in a process that: a) identifies a problem and its potential solutions; b) decides on a solution; and c) implements the solution. In each of these stages, Noveck argued there exists opportunities to get more voices and people involved in this process. The legitimacy of this process increases due to the diversity and the additional knowledge involved in the decision-making level.

Noveck described how at GovLab, with the support of NetMundial Initiative, her team developed a tool based on these concepts: the NetMundial Solutions Map. This interactive infographic/map highlights different approaches that go with different issues[1]. Noveck suggested that this is part of a trend – such tools and cultural practices are being developed all around the world. With the emergence of open government practices, Noveck said, people are demanding to participate in new ways. This inclusion is not only important, but useful for decision makers as it allows them to hear from the "right people" in the "right moments" in time.

NEXT STEPS FOR RESEARCH AND POLICY

Three key themes emerged from the panel discussion that would benefit from deeper research:

1. Developing inclusive models: Research questions might include:
    a. Which layers and organizations/mechanisms for decision-making require greater participation?
    b. Who decides who will participate in these mechanisms or organizations and according to what criteria?
    c. What will be the various participants' roles and responsibilities? What will participation entail?
    d. What current experiences in national contexts can illuminate this debate at a global level?

2. Accounting for cultural differences in deliberation: Research questions on this issue might include:

[1] The alpha version of the tool can be found at https://map.netmundial.org/

a. How to differentiate between mechanisms of consultations and engagement and participatory mechanisms of decision-making? Who decides who gets to contribute to major Internet governance decisions?
b. What are the alternative mechanisms and tools that can improve the last step of decision-making and deliberation processes?

3. Mechanisms to ensure a legitimate Internet governance ecosystem: Research questions on this issue might include:

a. How to ensure participatory mechanisms that increase diversity also translate into the increased perceived legitimacy of those at the table?
b. How to balance legitimacy, representativeness, decentralization and distributed forms of Internet governance, while weighing the role of different sectors?

Fireside Chat: Examination of U.S. Policy and Law in a Global Landscape

Drafted by Guilherme Alberto Almeida de Almeida and Benjamin Dean

Moderator:

Merit E. Janow, Dean, SIPA, Columbia University

Speaker:

Brad Smith, General Counsel and Executive Vice President,

Legal and Corporate Affairs, Microsoft

EXECUTIVE SUMMARY

This “fireside chat” between Mr. Brad Smith, the General Counsel and an Executive Vice President at Microsoft, and Merit E. Janow, Dean of Columbia SIPA, considered United States policy and law in the global context. This wide ranging discussion examined numerous policy areas, a pending case between Microsoft and the U.S. government, and considered the evolving regulatory and cooperation frameworks in the world today.

Themes for future research include: 1. Reconciling heterogeneous national policies within a global Internet governance system; 2. Updating and streamlining the international frameworks and process for extra-territorial access to data by law enforcement, including through MLATs; and 3. Exploring policy options that can rebuild trust in technology by balancing the need for public security, data security and privacy protection.

BACKGROUND

In recent years there have been a number of events that have had profound effects on U.S. technology companies.

Firstly, the disclosure of the activities of the United States National Security Agency (NSA) by Edward Snowden in 2013 has triggered an erosion of trust that customers previously held in technology products themselves. NSA activities included the bulk collection and storage of all Internet data and communications information as well as the weakening of important cyber security standards and technologies. The commercial

impacts of this loss of trust are enormous and are reflected in the slowed transition to "The Cloud."

Secondly, in December 2014 there was a hacking incident experienced by Sony Pictures Entertainment and apparently perpetrated by a state, North Korea, which was termed as 'cyber-vandalism' by President Barack Obama. This government-sponsored attack on a private enterprise grabbed international headlines and cost Sony an estimated $45 million. This incident has ignited fears of additional attacks on private, multinational enterprises in the future.

Finally, the massacre of cartoonists at the Charlie Hebdo magazine in Paris early in 2015 has reinforced calls for law enforcement's access to the data and information of potential threats or suspects. Policy proposals to respond to this threat take many forms: examples include efforts to undermine encryption standards, efforts to access data held off-shore (extra-territorial) and calls for online content platforms to police their users and block extremist content.

DISCUSSION

Janow opened the discussion by inviting Smith to address the critical policy challenges that face a global technology company such as Microsoft, which operates around the world and under many different regulatory frameworks.

Erosion of trust and its impact on local regulations

Smith argued that this is an unprecedented time. He referenced the Snowden incident, the hack and other incidents that have brought to the fore attention by citizens and governments to security and privacy issues. He argued that that governments have responded to the erosion of trust and the potential use of the Internet to foment terrorism or other adverse actions by proposing policies that fall into six broad categories: 1. Data residency (rules that determine that data have to stay within the country's borders); 2. Data retention (companies have to retain user data for a period of time); 3. Local security standards (hardware and software should be designed in accordance to a country's unique security standards); 4. Encryption rules (particularly with respect to access to encryption keys); 5. Content rules (related to concerns of extremists' conduct); and 6. Extra-territorial reach (trying to access data in other jurisdictions).

These laws and regulations will have profound ramifications on how data and ideas move around the world, how technology companies provide services around the world, potentially have profound implications for whether companies can sell products around the world, and whether there will be a single Internet or there will be further fragment.

Janow asked whether there was anything developing akin to international norms around the world that could address some of these issues. Smith replied that an international norm is something that conforms with international principles. To date, the norms have been developing around transparency. Transparency is increasingly becoming an international norm and it wouldn't be surprising to see it become a requirement, he argued. Norms are also emerging around data residency, which involves stipulating

Fireside chat: Merit E. Janow and Brad Smith

that public sector data must remain in the home jurisdiction. While most tech sector executives do not like data residency, data residency is increasingly being pushed amongst public sector officials. However, we are still in the early stages of the establishment of international norms, like data residency. It is thus a subject of intense debate and controversy.

New demands for extraterritorial reach of governments

The issue of extraterritorial reach is of particular pertinence to Microsoft given its pending case against the U.S. government in the U.S. Supreme Court. Microsoft is currently pursuing a case against the U.S. government following a request from the FBI to access the email data of a Microsoft customer, which are held in a Microsoft data center in Ireland. Smith argued that the 1986 Electronic Communications Privacy Act (ECPA) has no provisions authorizing seizure of information outside of the country and therefore the warrant served upon Microsoft should in theory only be enforceable within the U.S. jurisdiction. It is this ambiguity that is presently being contested.

If the U.S. reaches simply because it can, and should Microsoft lose the case, and the U.S. government be granted the powers to access data held off-shore, there will be major consequences. How would Americans feel if their personal information is in a data center and a foreign government wants that data? Smith asserted that people want to be protected by their own law.

Many countries observe and follow the lead that the United States sets in these areas. If the U.S. demands access to data held in other countries, through the ECPA, it could trigger other governments to demand or legislate the same powers for data held in the United States. This would clearly not be in the interests of U.S. citizens as it would be detrimental to their data security and right to privacy, he argued.

Data localization and fragmentation

Dean Janow asked Smith to elaborate on the harms associated with data localization. To require that all data reside within their own country would surely undermine services, radically drive up costs and have many other unintended consequences. Requiring the construction of many data centers would also put information out of the hands of many populations. Fundamental to innovation, especially for start-ups, is the ability to create applications that can be distributed globally in a singular way and on a common operating system. Localized standards start to break this commonality down.

Extremely localized technology standards would reduce the ability of small firms to innovate, impose additional costs, and reduce small businesses' ability to access the global market. Looking ahead, regulators will probably try to thread the needle: not breaking global standards as a whole while ensuring some degree of security around which there can be confidence and trust.

In sum, Smith argued that disregard for jurisdiction and national sovereignty would further undermine trust and confidence in the use of technology – and in the companies developing and selling these technologies. It would also reduce the innovative potential

and value creation that entrepreneurs and start-ups might derive from the global reach of these Internet enabled technologies.

Legal framework for law enforcement's cross-border data access

In the search for solutions to this situation, Smith posited that the international legal framework for law enforcement's access to data held off-shore could be facilitated through a mix of international trade agreements, bilateral consultations, updates to mutual legal assistance treaties (MLATs), as well as other international mechanisms, such as the definition of standards.

The U.S. Congress has proposed one domestic legal solution by means of a bipartisan bill of law named the LEADS Act[2]. The bill aims to refine the ECPA to authorize the use of search warrants extraterritorially only where the Government seeks to obtain the contents of electronic communications belonging to a U.S. citizen or resident.

Smith argued that bilateral agreements are probably the most practical way to encourage international cooperation. This is because multilateral trade agreement obligations are frequently bypassed by carve-outs relating to national security exceptions made by individual countries.

Reforming and updating the MLAT process is another potential direction given that the process has worked well in the past. When governments work together through MLATs, it is possible to obtain results rapidly while respecting the laws and rights of each party. For instance, Microsoft was able to lawfully provide emails related to the Charlie Hebdo attacks to the French government upon an FBI request, in the context of an existing MLAT. Microsoft was able to do this quickly and efficiently. By contrast, a Microsoft officer is being prosecuted for misdemeanor charges in Brazil due to Microsoft's refusal to turn over to the Brazilian law enforcement authorities certain Skype chat data held in a server in the United States – a situation that would be a felony under the U.S. wiretapping legislation if it was turned over directly to the Brazilians. In this instance, the Brazilians are not working through a bilateral arrangement.

The only way to move technology forward is to have governments working together - bilaterally and multilaterally. There would seem to be scope for a next generation of agreements where governments of one country can serve a warrant on a service provider and notify the other country and things can move more quickly and effectively. Multilateral agreements can also be modified to bring them into the 21st century and also build capacity within countries from the ground up.

[2] LEADS stands for "Law Enforcement Access to Data Stored Abroad." The bill is available at http://www.hatch.senate.gov/public/_cache/files/1f3692d5-f41f-4c73-acf2-063c61da366f/LEADS%20Act,%20September%2018,%202014.pdf

Cyber security and restoring trust

In light of this complex landscape, Janow asked Smith how should governments and global firms increase trust? Smith noted that trust has indeed been put in jeopardy by many different developments. In the tech sector, the companies are using technology to instill trust through stronger encryption. Tech companies have to take steps but, in no small measure, it is up to governments to take steps, in the global public interest, to restore trust in technology.

Smith invited the researchers to consider: What does a world of "good regulation" look like? To give context to the current situation facing governments and multinational corporations like Microsoft, Smith stressed the importance of recognizing the historical evolution of information security:

- At first, information technology was created without the Internet in mind. It was focused on single individual or corporate use.
- The connection of these computers to the world, through the Internet, opened up a new set of vulnerabilities. From 2002-07, the focus was therefore on building an updated security infrastructure to the Internet era.
- A third phase, simultaneous to the development of cloud services, focused on hardening the exterior, by creating additional protection against attacks from the outside. This era was soon supplanted in 2010-2012 era, by the belief that the exterior was not sufficient and did not do the job without protecting the interior and internal processes as well.
- By 2014, a new era started with the Sony attacks, which differed from prior security issues due to its nature as a nation state attack, and unlike other attacks it was akin to an act of vandalism, designed to destroy the ability of the company to use its information infrastructure.

So where do we go from here? We will harden technology further, without question, but ultimately we are in an era where multiple values are at stake: keeping the public safe, keeping data secure, keeping peoples' privacy. Governments are not prepared to leave it to business or leave it to just one or two governments. This must be addressed by all governments. The question is: how will we advance this in a way that maintains the global character of the Internet and that meets these various needs within societies?

NEXT STEPS FOR RESEARCH AND POLICY

This discussion suggested that significant changes are needed in the international legal and policy frameworks. Research could contribute to this process in the following ways:

1. Reconciling national policies within a global Internet governance system: Research could include the following questions:
   a. What are drivers/forces behind the national policy initiatives that may further fragment the Internet?

   b. What policy solutions exist that resolve conflicts between national interests with global Internet governance?

2. Resolving the extra-territorial data access issue: Research questions in this area might include:
   a. What are the possible impacts of Internet fragmentation, particularly due to attempts at extra-territorial data access by governments?
   b. What solutions might be developed that balance the needs of governments, citizens and companies, in this area (e.g. updating of MLATs)?

3. Rebuilding trust: Research in this area might focus on questions such as:
   a. What policy options exist that balance the need for public safety, data security and privacy protection?
   b. How might global rules be developed to reconcile each individual country's incentive to undermine cyber security, which, collectively, results in losses for all parties involved?
   c. What might good regulation that instills trust look like?

Plenary Panel 3A: Human rights, Freedom of Expression, and the Internet

Drafted by Alexis Wichowski

Moderator:

Anya Schiffrin, Director, International Media, Advocacy and Communications specialization, SIPA, Columbia University

Panelists:

Agnes Callamard, Director, Global Freedom of Expression and Information @ Columbia

Fen Hampson, Distinguished Fellow and Director of Global Security and Politics Program, CIGI, Co-Director of GCIG, and Chancellor's Professor, Carleton University

Carolina Rossini, Vice President for International Policy and Strategy, Public Knowledge; GCIG Research Advisory Network member

Marietje Schaake, Member of European Parliament; GCIG Commissioner

EXECUTIVE SUMMARY

This panel examined the challenges of protecting human rights online and how the transnational nature of Internet activity calls into question which governments are ultimately responsible for enforcement of such protections. Panelists discussed possible mechanisms for enforcing protections, including social contracts, trade agreements, and reciprocal arrangements between like-minded countries.

Themes for future research include: 1. Determining appropriate and implementable mechanisms for enforcement; 2. Exploring means to incentivize national governments to enforce human rights protections online for both their own citizens and non-citizens using services housed in their national borders, and 3. Examining the impact of social contracts and reciprocal agreements in re-establishing trust among the global community of Internet users.

BACKGROUND

The drafters of the Universal Declaration of Human Rights, adopted almost 70 years ago, likely could not have envisioned what the world would look like in the Internet era.

Yet the principles enshrined within this document continue to apply today. “Everyone has the right to freedom of opinion and expression,” Article 19 declares. “This right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers.”

While people may still have the right to seek, receive and impart information and ideas, what exactly is meant by “frontiers” is difficult to pin down in the digital era. Citizens access the Internet within a specific country – their home, library, workplace, or mobile device, for instance – but their activities online may traverse several national borders. This leads to the as of yet unresolved question: how can the protection of human rights be preserved in the digital landscape? And who should be responsible for these protections?

Human rights protections have traditionally been the sole responsibility of a citizen’s government: a Chinese citizen’s rights fall under the jurisdiction of the Chinese government; a French citizen’s rights fall under the jurisdiction of the French government, and so on. But who is responsible for those same citizens’ rights when they access websites in the United States, Brazil, Turkey, or Japan? And what responsibilities do the technology companies who manage the platforms have in terms of protecting citizens’ human rights? Determining the answers to such questions will shape what human rights mean in the digital era.

DISCUSSION

Anya Schiffrin, Director of the International Media, Advocacy and Communications specialization at Columbia SIPA and panel moderator, opened the discussion by asking panelists to first define what we mean by “human rights online,” especially with respect to who is responsible for enforcing them. Schiffrin also called on panelists to distinguish between human rights enforcement and the broader issue of surveillance.

Human rights online

Marietje Schaake, Member of European Parliament and GCIG Commissioner, argued that the universality of human rights is under great pressure in the Internet era. National sovereignty issues in particular complicate matters. For instance, Schaake described that Ukraine recently approached the social networking platform Facebook with a request to take down what they deemed to be misinformation coming out of Russia. Given the current political hostilities between these two nations, such a request is understandable. Schaake raised the question, who judges what is illegal content versus simply undesirable content?

Schaake described another scenario from recent headlines. France, in the wake of the Charlie Hebdo attacks, passed strict new antiterrorism laws, which include monitoring and keeping track of citizens who accessed “dangerous” websites. This in itself may not be problematic, Schaake noted. But the process by which websites are deemed “dangerous” is not transparent. She questioned whether instituting such hidden measures, even for the sake of national security, are truly appropriate in a democratic society.

Panelists (from left to right): Anya Schiffrin, Marietje Schaake, Agnes Callamard, Carolina Rossini and Fen Hampson.

Agnes Callamard, Director, Global Freedom of Expression and Information @ Columbia, pointed out that preserving human rights in the digital era is especially challenging because of the complexities of the global order in this particular moment in history. Callamard suggested that the Universal Declaration of Human Rights, written at the close of the Second World War, was only possible because at that time, the international landscape enjoyed great consensus on issues such as the preservation of human rights. Callamard challenged the audience to imagine writing such a document today, suggesting it would be near impossible: the increasingly globalized world, with many countries eager to participate in global decision-making processes, would make consensus harder to achieve. Moreover, it is not only governments commenting on what constitutes and governs human rights online – the private sector is also playing an important role in defining the landscape.

Challenges of enforcement

Callamard continued by explaining why enforcement of human rights is a major challenge today. “Enforcement,” in the human rights context, she noted, usually means “protection.” But who is responsible for protection of individuals’ rights online? How far does the human rights obligation of governments extend – to just their own citizens, or anyone accessing websites hosted in their countries? Callamard offered an example to illustrate the challenges of enforcement and protection: the United States, she contended, is currently ordering Microsoft – an American company but with data centers located in Ireland – to hand over emails of a Microsoft customer who is not American. According to the United States’ view, Callamard explained, since the parent company, Microsoft, is incorporated in the United States, the government of the United States should have the capacity to access the data this company manages, regardless of the citizenship of the individual or the geographic location where it is housed.

Carolina Rossini, Vice President for International Policy and Strategy, Public Knowledge, and GCIG Research Advisory Network Member, focused on how human rights online are impacted by the recent loss of trust among users. After the Snowden revelations about government surveillance of online activity, Rossini said users no longer felt the same sense of security that they had in the past, which has had a significant impact on the online experience of the global community. Rossini argued that the greatest challenge we face today is to determine how to reestablish this sense of trust and community.

A new social contract?

This starts with a new form of social contract, Rossini suggested. While this concept may sound abstract, Rossini argued that this is far from the case. In fact, a global social contract is among the things that keep countries from going to war over every disagreement. If we need a new social contract, Rossini asked, what would this look like? Whatever the form, it would need to be transparent, she suggested. Rossini nominated trade agreements as the best avenue for securing a more open and transparent Internet. She explained that of the many venues in the Internet ecosystem,

trade agreements are among the most concrete, they're already in place, and they exist on both bilateral and multilateral levels. As such, Rossini suggested, they are the most likely means by which a concrete human rights assessment framework can be achieved.

Fen Hampson, Distinguished Fellow and Director of Global Security and Politics Program, CIGI; Co-Director of GCIG, and Chancellor's Professor, Carleton University said that the main problem with human rights protections online has to do with issues of national sovereignty. "Fish swim outside the net," he suggested, meaning that national laws only apply to their own citizens. Those "fish that swim outside the net" – the non-citizens – are not afforded the same privacy rights as citizens.

How do we deal with this? Regional bodies provide some solutions, Hampson said. For instance, if one lives in the European Union, directives exist that describe how to handle issues related to human rights for all Europeans. While this is beneficial for Europeans, Hampson acknowledged, it doesn't address the problem of how to deal with the "fish outside the net" – the many Internet users who are not Europeans and therefore are not subject to the same directives.

One possible solution that Hampson offered is to treat human rights issues as a matter of reciprocity that should be applied to all citizens. For instance, Hampson described how the "5 Eyes" – the U.S., U.K., Canada, Australia, and New Zealand – already have a reciprocal intelligence-sharing agreement. A similar agreement could be put in place with respect to protecting human rights online. Reciprocal agreements may start with only a few countries, but they could be a way to start operationalizing the enforcement of protections.

Schaake took this line of thinking one step further, suggesting that human rights protections online can be seen as a soft power opportunity. For instance, if countries with reciprocal protection agreements reached out to citizens in authoritarian governments by recognizing their rights online, it could help to lend legitimacy to their advocacy efforts in their own countries. In this way, Western democracies have an opportunity to act as global leaders in determining the meaning of human rights online.

NEXT STEPS FOR RESEARCH AND POLICY

The various contributions from the panel experts suggested that protecting and enforcing human rights online in the future requires more research in three key areas:

1. Mechanisms for enforcement: Research questions might include:
    a. What roles can international organizations and private sector entities, such as technology companies and broadband and wireless service providers, and others, play in enforcing human rights protections online?
    b. In cases where international organizations and private sector entities determine human rights violations online, what recourse do they have with respect to national governments?

2. Incentives. Research questions may include:
    a. In what ways might existing trade agreements be leveraged to enforce human rights protections online? Is this the correct mechanisms for that objective or are there others?
    b. What additional mechanisms could be introduced to incentivize national governments to enforce human rights protections online?

3. Social contracts & reciprocal agreements: Research questions might include:
    a. What kind of reciprocal agreements could like-minded countries with similar human rights protections engage in to ensure human rights protections online?
    b. What would a social contract or human rights declaration for the Internet era look like, and what would incentivize national governments to sign on to such an agreement?

Panel 3b: Trade, Internet Governance, and Cross-border Data Flows

Drafted by Wouter P. F. Schmit Jongbloed

Moderator:

Gordon Goldstein, Managing Director and Head of External Affairs, Silverlake

Panelists:

Nick Ashton-Hart, Executive Director, Internet and Digital Ecosystem Alliance (IDEA)

Susan Chalmers, Principal, Chalmers & Associates

Anupam Chander, Professor, University of California, Davis

Victoria Espinel, CEO & President, Business Software Alliance

EXECUTIVE SUMMARY

This panel examined how the digital economy has transformed the landscape of international trade, binding the world economy together more intricately than ever before. Panelists discussed the complexity of cross-border trade that has been made possible by the flow of immense amounts of data across borders and jurisdictions.

Themes for future research include: 1. Managing issues of privacy protection and industrial protectionism as they emerge from the governance of the public and private Internet in parallel (such as data localization); 2. Addressing national security concerns related to digital content and infrastructure; and 3. Consideration of the implications of perceived U.S. hegemony for the regulation and long-term stability of a unitary, global Internet.

BACKGROUND

By the beginning of 2015, Internet connectivity became a (daily) reality for approximately 47 percent of humanity – most of whom are located in developed economies (ITU, 2015).[3] This simple observation carries with it several consequential

[3] The ITU predicts that 3.2 billion people will be using the Internet by the end of 2015, of which 2 billion are from developing countries.

implications for the present and future geography of economic and social interests (focal points), patterns of international trade, cross-border data flows, and services industry that together make up the digital economy (OECD, 2014).[4] None of these aspects though is more revolutionary in scope and development potential than participation in the massive extension of cross-border trade through global value chains (GVCs), involving emerging markets and industrialized economies alike.

Cross-border data flows are both essential to and the by-product of the increased international disaggregation of production along GVCs and of the digital economy as a whole (Business Roundtable, 2015). As has been explored at length in the literature (Elms et al., 2013), integration into GVCs holds the potential to offer great advantages for inclusive growth and development. Due to the fundamental accessibility and visibility characteristics of the present Internet both larger, well established, and smaller, or start-up, enterprises have an *ex ante* chance to interact with all or part of the global economy.

At present, the Internet economy comprises three billion users and, were it an entity, would constitute the fourth largest economy in the world (behind the U.S., China and Japan). Trans-border flows of goods and services reached U.S.$26 trillion in 2012, according McKinsey, which will triple by 2025 (ibid). Cisco points out that the Internet-of-things will eventually comprise a U.S.$4 trillion economy (Bradley et al., 2013).

The conventional analysis of the structure of the digital economy suggests a bifurcation between business-to-business (B2B) traffic and business-to-consumer (B2C) interactions (Manyika, 2014). B2C transactions are growing rapidly, especially on

Panelists (from left to right): Gordon Goldstein, Nick Ashton-Hart, Anupam Chander, Susan Chalmers and Victoria Espinel

[4] The OECD observes that "[t]he digital economy extends beyond businesses and markets – it includes individuals, communities and societies. […] The majority of current ICT metrics focus on the role of ICTs in business performance and fall short in terms of measuring the social impacts of ICTs and their contributions to social outcomes."

mobile devices in China. A further bifurcation emerges when considering the data flows generated by and contained within multinational enterprises (MNEs) – especially those delivering services to end-consumers or harboring sensitive information. This has raised data custody questions across jurisdictions in new and meaningful ways. It is in this context that data protection breaches raise the ire of privacy minded publics as well as of governments seeking to safeguard the trade interests of domestic industries.

Divergent national and international responses to these and other commercial and infrastructural dynamics highlight differences not only in policy priorities, but also in answers to strategic questions of Internet interoperability. As questions of Internet governance are increasingly interwoven with the structure of international trade, consideration of the proper leeway for national security controls to impede and control cross border data flows are at risk of becoming ever more politicized.

In addition to inter-governmental negotiations, international bodies such as the World Trade Organization (WTO) and the United Nations Conference on Trade and Development (UNCTAD), together with non-governmental organizations such as the World Economic Forum, have entered the discussion. Various commissions, such as the Global Commission on Internet Governance and the E-15 Initiative on Strengthening the Global Trade and Investment System, also aim to contribute to thinking on the scope and substance of proper (international) regulation of the digital economy.

The very diversity of the stakeholders, and indeed of their interests, is a testimony to the importance of the ongoing technological shift – the full implications of which are still unclear and the limits of its benefits ill defined. Common ground seems to exist when all profess to the desirability of an “open, interoperable, secure, and reliable Internet.”

DISCUSSION

The panel was moderated by Gordon Goldstein, Managing Director and Head of External Affairs, Silverlake. Panelists discussed the respective roles of countries and companies in governance of digital trade and cross-border data flows, public trust and data localization, and the relationship between the United States and China and how data protection and national security plays into this relationship.

Role of countries and companies

Nick Ashton-Hart, Executive Director of the Internet and Digital Ecosystem Alliance (IDEA) noted that among the public and trade representatives alike the perception of the scope of the Internet economy centers on B2C transactions, even though the bulk of the economic value of the Internet is created by traditional industries. He stressed the important growth and development implications thereof. While every economy has its ‘bricks and mortar’ champions, business-to-consumer digital giants are headquartered in only a handful of countries. Focusing domestic economic policy on foreign B2C Internet services without considering the lion’s share of the value the Internet can provide to traditional sectors of the economy risks implementing policies that run directly counter to the national interest.

The seismic impact of the Internet in making services tradable should not be underestimated. As Ashton-Hart observed, manufacturing accounts for roughly 10 percent of economic activity on average worldwide, while the share of services is nearing 50 percent. Services passed agriculture as the largest segment of the economy on average worldwide at the dawn of the 21st century (Manyika, 2014). The Internet and cross-border data flows have made this spectacular growth in economic opportunities and employment possible. Since small and medium enterprises (SMEs) account for the vast majority of all countries' economies,[5] the benefits of the Internet are largely concentrated in these SMEs and overwhelmingly of benefit to traditional industries (European Commission, 2014).

Public trust and data localization

Victoria Espinel, CEO and President of the Business Software Alliance, pointed out that while much of the public's concern is concentrated on the protection of personal information, the large majority of B2B cross-border data flows in fact do not touch on such sensitive information. As market access barriers are addressed internationally, she highlighted that (international) trade policy is shaped not by a dispassionate analysis of economic flows alone, but also by political realities and perceptions. In this context the Snowden revelations and NSA spying accusations did considerable damage, shattering a measure of trust in the apolitical nature of the Internet.

Anupam Chander, Professor at the University of California, Davis, described this as a perfect storm of public anxiety and data localization policies for protection(ist) purposes. Together these form a serious threat to a truly global or unified Internet. The perceived dominance of U.S. companies in the digital economy, together with the breadth of U.S. governmental surveillance, suggests to some countries that "their" data is better secured (and utilized) within their own borders. Chander argued that data localization does not in fact create many domestic employment opportunities, nor does it fundamentally keep data more secure. Rather, it increases transaction costs and makes it more difficult for domestic firms to synergistically connect to the global Internet.

Susan Chalmers, Principal, Chalmers & Associates, however, made the point that encouraging the use of country code top-level domains (ccTLDs)[6] to keep data traffic local can have beneficial spillovers for national start ups in the digital economy, even though digital "borders" might simultaneously work to limit global visibility. She reflected that more international coordination and transparency could better connect the different

[5] For Europe (28), SMEs delivered 58.1% of the value added generated by the private, non-financial economy in Europe during 2013 and 66.8% of all European Jobs. These numbers are considerably larger in emerging markets and the least-developed economies.

[6] Country Code Top Level Domains (ccTLDs) are the two-letter Top Level Domains delegated to countries and some territories, for example .nz (New Zealand), .ar (Argentina), or .io (British Indian Ocean Territory). Correspondingly, ccTLD managers are trustees that supervise "the domain names and operate the domain name system in that country," see Jon Postel, RFC 1591: Domain Name System Structure and Delegation (March 1994), page 3, available at: https://www.ietf.org/rfc/rfc1591.txt.

stakeholder forums and regulatory debates. The different spheres of, for example, ICANN and international trade agreements should converge to safeguard the coherency of the debate and enforcement methods.

U.S., Europe and China: national security and data protection

The panelists expressed concern about U.S. technological hegemony in the digital economy. In particular, they addressed how industrial and privacy concerns might spur some of Europe's market dominance or antitrust enforcement actions – seen recently in action initiated against Google (European Commission, 2015). While the panel expressed hope that the high-level European Single Digital Market will prove a focal point for positive growth strategies, they noted that it might also become a springboard for regressive or trade-restrictive policies.

The panel expressed a deep worry that a tit-for-tat game could develop around national security policies, potentially damaging the international trading system. The effective exclusion of Huawei from some market procurement opportunities in the U.S. and elsewhere has been countered by removing Cisco from the list of "trusted" hardware providers in China for state-owned enterprises and government agencies. In addition to creating lose-lose retaliation spirals, Chalmers observes that national security legislation simultaneously raises regulatory compliance costs for domestic companies and thereby unintentionally provides an incentive to offshore research and development. While national security concerns are very real and pressing, the panel worries that over-focusing on those concerns has the potential to force a breakdown of the international trade system and thus fracture the global digital economy.

The panelists argued that establishing and maintaining a rule-based international trading system for the digital economy will be crucial to safeguard and deepen the many benefits that spring from free and vigorous cross-border data flows. At the same time, a rule-based international system allows national security and data privacy concerns to be narrowly delimited. This provides a maximum amount of policy transparency and legal certainty, which in turn instills confidence in the equitable functioning of the digital economy.

NEXT STEPS FOR RESEARCH AND POLICY

The contributions from the panel experts suggested that protecting and furthering an open and global Internet in service of the digital economy requires more research, especially in three key areas:

1. Managing public-private relations through international governance mechanisms: Research questions might include:
    a. How can demands for data localization and issues of vertical dominance, where control over the infrastructure (portal) coincides with content provision, best be addressed in a multilateral fashion?
    b. An exploration of global net neutrality issues and an assessment of its consequences in terms of the prevalent bottlenecks of the digital economy

such as market access (open access), content distribution (data flows), and content generation (information exchange).

c. What is the proper ambit of “national security”-related sovereign interventions pertaining to the digital economy and how are these best regulated within the international trade regime?

2. Review of international trade rules for digital economy: Research questions might include:
    a. What is the proper ambit and application of the GATS Telecommunication Annex and Reference Paper to the digital economy? Is there scope for a narrow or expansive interpretation thereof?
    b. How does the historical effort on audio/visual issues connect to the interaction of the GATS with the digital economy?
    c. When considering the international trade flows of intangibles, are these best classified as goods under the GATT, as services under the GATS, or perhaps as a hybrid category under a newly dedicated trade agreement (DETA)?

3. Top-level domain governance: Research questions might include:
    a. How might the dispute resolution mechanisms in trade agreements be extended to the field of ccTLDs?

Panel 4A: Privacy, Big Data and the Internet

Drafted by Susan McGregor

Moderator:

Andrew McLaughlin, Senior Fellow, SIPA, Columbia University

Panelists:

Matthew Jones, James R. Barker Professor of Contemporary Civilization, Department of History Columbia University

Rebecca MacKinnon, Director, Ranking Digital Rights project, New America

Michael Nelson, Public Policy, CloudFlare

Nuala O'Connor, President & CEO, Center for Democracy & Technology

EXECUTIVE SUMMARY

This panel examined the rise of Big Data and its implications for personal privacy. Panelists discussed a need for scalable, concrete policies that can balance the Big Data interests of governments and businesses with the privacy and autonomy needs of individuals. Yet the appropriate jurisdictional scope and philosophical objective for such policies is unclear.

Panelists discussed issues including: 1. Using national or regional boundaries to determine individual rights around privacy, self-expression and information access; 2. How doing so could impact collaborative efforts that rely on Big Data, such as those in science, health and environmental impact; and 3. The effect of such an approach on today's growing cloud-based industries.

Recommendations for future research include: 1. Exploring how conceptualizing the Internet and Big Data as a social good could be used to share privacy protection frameworks, and 2. Investigating methods, such as building privacy protection encouragement into the technical layer of the Internet, as a means to incentivize regional compliance.

BACKGROUND

When first coined, the term 'Big Data' was conceived as that which, "required a super-computer to process" (boyd, et al. 2012). While size remains one facet of what today is

considered Big Data, it is perhaps more usefully categorized by its granularity, velocity, dimensionality and relationality (Kitchin, 2014). This is especially the case where the latter characteristics are not only supported but also generated by the Internet-based nature of the data itself.

The high bandwidth and interoperability of the Internet both augment and transmit the billions of individual data points generated by today's hardware and software sensors. They allow them to be quickly and efficiently connected, processed and analyzed. This both endows them with their insight potential and, by extension, their economic and social value. Big Data as a modern commodity, therefore, is, as panelist Nuala O'Connor, President and CEO for the Center for Democracy and Technology, said, "just a lot of little data put together."

This connectivity is also what gives rise to today's Big Data privacy risks and governance challenges. As panelist Michael Nelson of CloudFlare noted, the characteristics of more traditional Big Data resulted in privacy policies that focused on access restrictions. But mechanisms focused on controlled disclosure and use policies that are aligned with stated collection purposes do not scale effectively beyond the limited entities. These entities included governments and healthcare providers, which traditionally had the capacity to generate, process and store Big Data. In this older environment, privacy was defined by individuals' anonymity within a given data set. Privacy was then operationalized through the removal of sensitive data features that constituted Personally Identifiable Information.[7]

But as the technologies for collecting and analyzing data have entered the mainstream business and consumer spheres, such domain-specific policies cannot be effectively applied to the diverse and emerging sectors that are using – or are even built upon – the kind of Big Data generated by individuals in the course of their daily lives. Even before the turn of the century, the increased portability of data was generating

Panelists (from left to right): Andrew McLaughlin, Matthew Jones, Rebecca MacKinnon, Michael Nelson and Nuala O'Connor

[7] e.g. name, social security number or other government identifier

measurable privacy risks, through the combination of even relatively small, sparse data sets (Sweeney, 2002). This risk has been exacerbated by the increasing reach and speed of Internet technologies, as “individual” real-time data streams are now rich enough to identify individuals within a “single,” sufficiently-dimensional data set (Narayanan et al., 2010). Now that data generation, transmission and storage have become the default behavior of an increasing array of technologies, governing the use of data by such a broad variety of actors is a significant challenge for governance and policy (Mayer-Schönberger, 2011). An additional challenge will be to then reconcile the different concepts of privacy, security, freedom of expression and economic progress that may come into conflict in an inherently transnational space like the Internet.

DISCUSSION

The panel, moderated by Andrew McLaughlin, Senior Fellow at Columbia SIPA, explored the link between Big Data and the Internet, related privacy implications and the national and international context in which policy must operate.

Privacy in the Big Data era

In light of the acknowledged challenges to maintaining individual privacy in the context of today's technologies, panelists discussed the possibilities of techno-deterministic policies. They generally concurred that proactive policy-making, especially across cultures and borders, will always be more difficult than maintaining an even relatively recent established status quo.

At the same time, panelists acknowledged there was room for debate over both the desirability and efficacy of such an approach. As MacKinnon noted, the importance of privacy as a social good is deeply ingrained in the legal, social and political frameworks of many nations. To weigh this coherently and to express value equally with the *de facto* operation of a handful of technologies – even those as pervasive as Internet protocols – assumes that the Internet, in itself, constitutes a social good. As such, this would place the Internet on par with other social goods that have been preserved, refined and reaffirmed over decades and even centuries in the face of enormous technological and social change. However, there is plenty of evidence that in many places, the Internet and the Big Data it generates are used to support surveillance and censorship not more autonomy and freedom of expression.

Matthew Jones, Professor of Contemporary History at Columbia, noted that while it is, “unquestionable that technologies can make laws obsolete…they cannot cause laws to be made.” The failure to effectively use law and policy to bridge the gap between existing social, political and economic values and the operation of new technologies is, in fact, only a path to both economic and technological stagnation.

These tendencies are already somewhat in evidence today. As Christopher Yoo, University of Pennsylvania professor, stated in an earlier panel, the defaults of current Internet technologies have proved ill-suited to the needs of economic sectors like financial services. McLaughlin concurred that individuals are now moving more quickly

amongst applications towards those that favor an ephemerality, which is unsupported by the default behavior of most digital technologies.

Privacy policies in an international context

In order to support the development of tomorrow's technologies, policies supporting privacy, freedom of expression, and access to information strongly grounded in international law are essential. As David Kaye highlighted in his recent report to the United Nations High Commissioner for Human Rights, the right to form an opinion cannot exist outside of the technological capacity to do so privately. This is in part because technology is an essential support for advanced cognitive function (Norman, 1993). Likewise, the recently published Manila Principles offer a scalable, transparent, transnational set of mechanisms for information access on the Internet (EFF, 2015).

Finally, panelists questioned the assertion that greater data collection and effective surveillance by governments and commercial entities serve only to increase security and economic possibility. As described by Federal Trade Commission Julie Brill, "Just as we don't know what benefits might lie undiscovered in big data sets, so too we cannot realistically say that we understand the harms that may occur when the same data is in the hands of a determined adversary. But we do know that you can't lose what you don't have, and so you can't have a security breach of data that you don't collect in the first place" (Brill, 2015).

NEXT STEPS FOR RESEARCH AND POLICY

The various contributions from the panel experts suggested that protecting and enforcing personal privacy online in the Big Data era requires more research in two key areas:

1. <u>The Internet (and Big Data) as a social good:</u> Research questions on this topic might include:
    a. What specific characteristics of the Internet qualify it to as a "social good"? Likewise, which characteristics of Big Data might qualify it as a "social good"?
    b. Is conceptualizing the Internet and/or Big Data as a social good constructive for policy making? If so, how might existing social-good related policy frameworks be applied to structuring personal protections for the Internet and Big Data?

2. <u>Global vs regional policies regarding privacy</u>: Research questions might include:
    a. What kinds of mechanisms for encouraging protection of personal privacy could be built into global Internet frameworks? In other words, how can the technical infrastructure of the Internet be leveraged to encourage regional compliance with personal privacy protections?

b. What role can international governance bodies such as ICANN, or international economic bodies, such as the IMF, play to incentivize regional governments to adopt mechanisms for personal privacy protections?

Panel 4B: Innovation and the Internet

Drafted by Hollie Russon Gilman

Moderator:

Merit E. Janow, Dean, SIPA, Columbia University

Panelists:

Brad Burnham, Managing Partner, Union Square Ventures

Konstantinos Komaitis, Senior Policy Advisor, Internet Society; GCIG Research Advisory Network member

Ronaldo Lemos, Director, Institute for Technology and Society of Rio de Janeiro; GCIG Research Advisory Network member

Sharad Sanghi, CEO and Founder, Netmagic Solutions

EXECUTIVE SUMMARY

This panel examined the relationship between government regulation and innovation economies. The panelists discussed how existing regulatory frameworks necessarily vary, with basic IT infrastructure requiring different levels of oversight than more complex systems. The challenge for governments is to identify and implement a balance of sufficient regulatory constraints that also allows for an ecosystem that enables – and ideally, fosters – innovation.

Themes for future research include: 1. Gaining a deeper understanding of the relationship between regulation and innovation; 2. Helping governments strike the balance between over- and under-regulation; and 3. Clarifying who owns data under these regulatory structures.

BACKGROUND

Innovation in the digital era arises at a rapid pace. According to Lawrence Lessig, technologies evolved from being tools – a means to an end – to something people could use to create new tools. In other words, Information Age societies are no longer “read-only”; but rather “read/write.” This new schema also introduces new opportunities to share information, evidenced by the rise of practices such as open source, open standards, and creative commons.

However, many government policy and legal structures remain calcified in a previous era. As a consequence, innovators often find themselves inventing first and dealing with the legal and political ramifications later. Many policy makers remain unaware of the implications of their well-intended regulations and their impact to curb or stifle innovation. This is partially due to limited technology policy knowledge by some making these decisions.

This is more than the result of a cultural chasm between technology and policy. At times there can also be a clash of normative values. Legal and regulatory frameworks are often aimed to safeguard civil liberties and safety. Innovation, on the other hand, is often aimed to spur industry, which is accountable to stakeholders, not lawyers. Innovations with an eye to maximize profits can sometimes eschew questions critical to public policy.

Greater knowledge and dialogue are therefore needed between policy makers and technology innovators. Engaging citizens themselves in these discussions could lead to a more collaborative framework that fosters dialogue and discussion between innovators and policy makers themselves. The end result could be increased economic growth and social opportunities to strengthen communities – local or global.

DISCUSSION

The first part of the panel discussion, which was moderated by Merit E. Janow, Dean of Columbia SIPA, focused on the drivers of IT innovation and the current relationship between regulation and technology innovation.

Drivers of IT Innovation and the Relationship Between Regulation and Innovation

Brad Burnham, Managing Partner, Union Square Ventures discussed the need to recognize two types of IT innovation. Basic infrastructure, such as chips and routers, requires hard science. He contrasted this with applications that ride on top of the basic infrastructure, such as Tumblr or Foursquare. Recognizing this distinction is critical for understanding the types of laws that impact both.

Konstantinos Komaitis, Senior Policy Advisor, Internet Society; GCIG Research Advisory Network member, first discussed the term “permission-less innovation,” which was a recurring concept during the panel. There are two general regulatory dispositions toward innovation. On the one side are precautionary principles that new innovation should be curtailed or allowed until they are developed and their impact on laws and norms is understood. On the other side is permission-less innovation that is able to experiment with new business models where effects will be dealt with later. To illustrate this dichotomy, Komaitis asked, “Imagine if Google or Facebook had to ask permission before they created something?”

Ronaldo Lemos, Director, Institute for Technology and Society of Rio de Janeiro; GCIG Research Advisory Network member cited the example of Brazil to build on this concept. He discussed the early stages of the Internet in Brazil in 1995, which lacked

regulations and laws around Internet-enabled business activities. While this seemed like a sound policy decision, in reality, the absence of regulation left the judiciary feeling a lot of pressure given the legal uncertainty in the area.

Sharad Sanghi, CEO and Founder, Netmagic Solutions explained that even though India has a reputation for an entrepreneurial culture with high mobile penetration rates – soon to be second only to China – in reality it is also a difficult country for business because of weak data security. On the plus side, there is a large domestic market and many global firms use software talent located in India. There is a burgeoning venture capital (VC) market. So much so that multinational companies, such as Cisco, couple with VC funds entering India. Therefore, India has a winning combination of entrepreneurial mindset, talent pool, access to VC, and huge domestic market driving innovation. However, there is some ambiguity in the current laws and conflicting judicial opinions. As an example, he noted the unjustified 2004 arrest of the CEO of EBay in India over the sale of an illicit item by a member of the online marketplace. In general though, the government does not intervene in the IT sector and does not impose onerous regulations.

The remainder of the discussion revolved around two key issues: striking the right balance between over-regulation and under-regulation of the IT sector, including the concept of "intermediary liability"; and clarifying ownership of (or property rights for) data in the digital age.

Striking a balance between over-regulation and under-regulation

On the first issue, according to Burnham, the key is to reconcile permission-less innovation with a set of laws that foster innovation, thus creating the environment without defining outcomes. Lemos highlighted a Brazilian example: the creation of an Internet Bill of Rights, as opposed to a set of policy constraints. One such example of effective policy occurred in the U.S., mostly by accident. Section 230 of the

Panelists (from left to right): Merit E. Janow, Brad Burnham, Konstantinos Komaitis, Ronaldo Lemos and Sharad Sanghi.

Communications Decency Act protected Internet intermediaries from liability for what others say and do when using interactive computer services. This protection provided the space for companies to experiment without falling foul of restrictive liability laws.

This can be compared with the experience in Brazil where, in the 2000s, draconian laws were enacted criminalizing activity such as sharing MP3 files. After intense pressure, research, and civil society mobilization, in 2009 Brazil moved to discuss net neutrality. Amidst this pressure and after the Snowden revelations, in 2014 Brazil passed a new law upholding net neutrality and consumer data rights.

Komaitis clarified that permission-less innovation is not "anarchy." He said, in fact we want government to protect us as citizens. The question is not whether or not we should regulate. The question is how to address these problems effectively. Sanghi also noted that, "as long as there is a framework," without restrictive regulations and some stability, innovation will continue to occur. A well-balanced regulatory system rewards success based on merit as opposed to simply being a big corporation.

Stability in regulations also came out as an important attribute. Lemos built on this using the example of Uber in Brazil, which is on a legal roller coaster – one day it is prohibited, the next day it is allowed. Yet, in all these discussions about Uber, no one has asked the users themselves what they want. They need to be a part of this discussion.

At the close of the session, Burnham proposed "a carrot not a stick" approach to encourage more people in an ecosystem to share data with regulators. There could a type of data safe harbor – if you are sharing your data with regulators they will not prosecute you. The model works well with young companies without having the third employee be a lawyer. This approach would create an advantage for companies instead of requiring them to comply.

Ownership of data in the digital age

On the second issue, the ownership of data in the digital age, Burnham started by citing the legacy of legal battles related to intellectual property (IP) rights such as copyright and patents. A framework is needed to allow for innovation and to define user data rights. For example, he cited the Target data breach of user data where roughly 80 million records were lost. Target settled with the government for $10 million.

According to Burnham, this vastly underestimated the value of this data. Today, he argued, companies produce and retain an "unbelievable amount of data" about users. However, regulations are essentially working in an old, fairly constrained model. Somewhat linked to the first question, on ideal regulatory systems, Burnham said that there is a need for adaptive frameworks to establish what each individual's interest in their data was then to assign liability.

The outcome would be an emergent market. "We have an opportunity to construct new markets," Burnham suggested, given that data is a non-rival good (e.g. more than two people can use it without detracting from one another's utility). Right now, the service

provider has all the information. However, both the user and the service provider could have the information were it to be anonymized. This opportunity requires overcoming the practical difficulties in effectively anonymizing these data. Some type of legal framework, which assigns liability to attempts to de-anonymize data, might contribute to realizing this opportunity.

Citing Carolina Rossini's work, Lemos explained how the Internet is increasingly embedded in trade agreements, IP rights, and the remit of the World Trade Organization (WTO). He noted that we need to be careful of more and more decisions about Internet regulation occurring in a trade setting. Lemos advocated for a more mission-oriented participatory and collaborative process instead of making these decisions by a closed commission or by experts who often do not have all the information or engagement from a diversity of stakeholders.

Tangential to the issue of ownership of data is control over data. Lemos discussed a data protection law being crafted in Brazil to balance protection with innovation. He noted it is important that "citizens feel comfortable with the amount of monitoring." In developing countries, a bad credit score can ruin your life. There is a need to find a process for the review of these decisions, one with greater transparency, to ensure that we balance civil rights with economic promotion and innovation. Komaitis noted, "In Europe everything is about data." Europe is discussing the idea of privacy as an economic right and the implications of what this means in the context of data collection and data issues. He suggested that this is a place where regulation could be beneficial because the use of those data will trigger regulation.

NEXT STEPS FOR RESEARCH AND POLICY

Two key themes emerged from the panel discussion that would benefit from deeper research:

1. Balance between over- and under-regulation: Research questions might include:
    a. What mechanisms would enable governments to exchange best practices regarding regulatory frameworks surrounding IT innovation?
    b. What are the economic and political implications of heterogeneous regulatory frameworks on the local and national level?

2. Ownership of data in the digital age: Research questions might include:
    a. Given that data is a non-rival good, available to more than one stakeholder at a time, what kind of structures would adequately provide for the rights of the data owner while enabling access by data users?
    b. What aspects of current intellectual property frameworks remain applicable in the digital era? What updated mechanism could account for the needs of the diverse stakeholders – protecting the rights of content producers but also enabling open source innovation?

Opening Session, Day 2: Cyber Security

Drafted by Benjamin Dean

Moderator:
Merit E. Janow, Dean, SIPA, Columbia University

Speakers:
Michael Chertoff, former Secretary of the US Department of Homeland Security; GCIG Commissioner
Kevin Mandia, Chief Operating Officer and Senior Vice President, FireEye

EXECUTIVE SUMMARY

This panel discussed evolving cyber risks and the related threats that governments and private companies face. It addressed how governments might respond to these risks at a national and international level. Potential research directions include: 1. At an international level, how could a global mechanism for governing cyber security policy be developed? 2. At a national level, what might a centralized cyber security vision look like for the United States? and 3. What is the appropriate role for government and the private sector in addressing cyber threats?

BACKGROUND

The cyber threat landscape is constantly changing. A combination of individual hackers ('hacktivists'), organized criminal outlets and state-sponsored agencies make up the commonly understood threat landscape. Hacking has typically been a means by which to acquire information so as to commit fraud. The collection of the personal information of targets allows criminals to commit financial fraud through online credit card transactions and international money transfers.

Reliable statistics are difficult to find, but according to the Verizon Data Breach Investigation Report in 2014 fraud and financial gain dominate the motivations behind attacks (approx. 70%), followed by espionage, whether for state or commercial purposes (approx. 25%). The minority of attacks are perpetrated by individual 'hacktivists' for ideological reasons or for fun ('the lolz') (<5%) (Verizon, 2014).

However, in recent years, attacks by state-sponsored entities have been on the rise. Following the removal of a Soviet-era war memorial in 2007, Estonia found its government websites, national newspapers and banks dropping offline (Baraniuk, 2015). In 2008, Georgia experienced similar problems as Russian troops advanced across their border. Iran found hundreds of damaged nuclear centrifuges in 2014

following the deployment of the Stuxnet worm by the U.S. and Israel. Most recently, Sony Pictures Entertainment experienced destroyed computers and servers as well as the theft of hundreds of gigabytes of employee files and emails. The United States government claims that North Korea was the culprit.

In response to these evolving threats, public-private sector collaboration has characterized the response to cyber security demands. The skills and technical capabilities reside in the private sector, in addition to a substantial amount of threat intelligence information, while the funds and authority reside in the public sector, particularly in the Department of Defense (in the United States, at least).

Ensuring effective cyber security is complicated by the cross-border nature of the Internet. Organized criminal outfits residing in Eastern European countries have been among the most challenging threat actors to combat given their ties to the authorities in the countries that they reside in. The rules of espionage insulate countries from the negative consequences of their intelligence gathering exercises. So too does the difficulty in linking stolen data with the final recipient of the data. It was within this evolving context, and its associated challenges, that this keynote discussion took place.

DISCUSSION

Merit E. Janow, Dean of Columbia SIPA, framed the discussion around the evolving cyber risks and threats that governments and private companies face; how governments might respond to these risks through policy; how private companies might mitigate these risks; and finally, the need for international collaboration in addressing this issue and what concrete steps might be taken to foster better collaboration between

Keynote speakers on day two (from left to right): Michael Chertoff, Merit E. Janow and Kevin Mandia.

nation-states?

Evolving cyber threat landscape

The cyber threat landscape has evolved over the past decade. Today, nation-state actors are increasingly involved. In addition, the methods have changed as network defenses have improved, which has in turn pushed attackers to target individuals though methods like spear-phishing.

The major nation states involved in this arena include China, Iran, North Korea, Russia, Syria and the United States. These nation states typically seek to steal the intellectual property of companies (*sans* the United States) but are also testing and refining methods to disrupt the command and control systems of adversaries' militaries in the event of future conflict.

The difficulty in defending against cyber threats stems from the lack of any clear rules of engagement, the difficulty in establishing certain attribution (though attribution certainly isn't impossible), and the lack of any repercussions against those behind cyber-attacks. Perhaps as a consequence of the transition towards greater nation state involvement, the lines between nation states and organized criminals is somewhat blurred. Nation states might hire, protect or grant effective immunity to criminal hacking organizations.

Government and private sector responses

The difficulty in mounting an effective defense against adversaries in the cyber arena stems from its inherently asymmetric nature. "Out of 1000 computers, as an attacker, I only need to infiltrate one of them," in the words of Kevin Mandia, Chief Operating Officer and Senior Vice President, FireEye. Nevertheless, governments and private companies must still attempt some kind of defensive measures. The panelists subsequently provided some suggestions.

The best thing that governments could do to assist private industry in dealing with cyber threats and hacks, according to Mandia, is to clearly disclose when a successful hack of a company is perpetrated by a nation state. Michael Chertoff, former Secretary of the U.S. Department of Homeland Security; GCIG Commissioner also felt that governments should ensure that technological standards remain robust. Inserting backdoors into widely used technologies would not improve cyber security.

To prepare and respond to cyber threats, private companies could pursue a number of strategies and tactics. A shift to a risk-based decision making process, based on the identification of key threats and implementation of measures to mitigate these threats, is an effective strategy for firms to adopt. This top-down security posture is proving to be more effective than the bottom-up, compliance based strategies of the past.

Chertoff strongly discouraged any attempts to "hack back" and did not feel that governments should permit companies to legally pursue these tactics given the risk of collateral damage. Mandia concurred and felt that companies should use their limited resources and time to advance their security posture instead of tactics like "honey pots."

"Your whole network is one big honey pot," was his advice. He saw the biggest bang for the buck being in effective credential management.

Better-developed international and national cyber security policy

It became clear from the discussion that the cyber security policy framework is underdeveloped at a national level, in the United States, and globally. Further developing these frameworks will be challenging given the divergent interests of the parties involved at both levels.

In the United States, responsibility for cyber security policy is spread across a number of agencies. The Department of Defense has authority over the military and intelligence-related aspects, the Department of Homeland Security is tasked with coordinating with private sector and the Department of Justice has some authority. Chertoff and Mandia felt that ultimately, responsibility for robust cyber security lies with enterprises themselves. The involvement of regulators sometimes arises though regulators like the Securities and Exchange Commission and utility regulators don't necessarily have the requisite knowledge to deal with cyber security-related matters.

Going forward, according to Chertoff, the challenge will be to centralize cyber security policy responsibilities in a way that creates a unified, strategic vision. He suggested that the establishment of an agency, following the model of the National Counter Terrorism Center, would be an effective way to bring the intelligence on cyber security together at a Federal level.

There is little collaboration and coordination of cyber security a global level. The challenge in establishing an effective system of global governance lies in reconciling legitimate national interests and sovereignty with a global Internet. Chertoff felt that trade policy and rules might represent one set of tools that could be used to set "rules of the game" at a global level. Finding areas of collaboration between nation states, such as the United States and China in the areas of combatting financial crimes and setting rules of engagement in conflict, were also thought to be potentially effective next steps.

NEXT STEPS FOR RESEARCH AND POLICY

The discussion between Chertoff, Mandia and Janow pointed to promising future research directions in:

1. Developing a global system for governing cyber security: Research questions might include:

    a) What international mechanisms exist concerning cyber security and where might gaps lie?

    b) How might bilateral corporation or collaboration pave the way towards a more coherent global governance mechanism?

2. A centralized cyber security vision: Research questions on this topic might include:

a) What are the different responsibilities for cyber security policy and where do these responsibilities reside at a Federal level? How might these responsibilities be centralized and which agency model would be most appropriate?

b) What would a unified vision be for cyber security policy at a national level? What components would be involved and which policy options might exist under each component?

3. Determining the appropriate role for government and the private sector in addressing cyber threats: Research questions on this topic might include:

a) What would be the benefits and costs associated with policy initiatives such as intelligence information sharing between the public and private sectors?

b) What would be the consequences of a policy that permits private entities to 'hack back'?

c) Should limits be placed on the espionage and intelligence gathering activities of governments given the negative consequences of these activities on private entities?

Panel 5: Mitigating Cyber-risks in Critical Infrastructure: Private and Public Responses for the Financial Sector

Drafted by Peter Roady

Moderator:

Jason Healey, Senior Research Scholar, Cyber Policy, SIPA, Columbia University

Panelists:

Steven Bellovin, Percy K. and Vidal L. W. Hudson Professor of Computer Science, School of Engineering, Columbia University

Paul Bracken, Professor, Yale School of Management

Louis Modano, Senior Vice President and Global Head of Infrastructure Services, NASDAQ

Elizabeth Petrie, Director, Strategic Intelligence Analysis, Citigroup Information Protection Directorate

EXECUTIVE SUMMARY

Participants in this panel provided an overview of cyber threats to the financial sector, ranging from nation-state affiliated hackers with ambiguous intentions to criminals seeking financial gain, and outlined steps the financial sector has taken to deal with them. Because it is subject to near constant probing and attacks, the financial sector provides particular insight into the broader cyber environment. The analytical, organizational, and technological innovations the financial sector has adopted to deal with these threats represent the leading edge of cyber security and provide models for other sectors to emulate.

Research recommendations included: 1. How to share information in low-trust environments; 2. Creating oversight of private-sector cyber intelligence brokers; and 3. How to build in cyber-familiarity among senior decision-makers in both the public and private sector?

BACKGROUND

The financial sector has been for many years the principal battleground of cyber warriors of all stripes. The sector's position in the crosshairs has pushed it to the leading

edge of cyber security. For instance, in 1995, Citigroup created what many consider the world's first Chief Information Security Officer position as part of its response to a high-profile cyber incident the previous year. In 1999, the financial sector created the Financial Services Information Sharing and Analysis Center (FS-ISAC) to gather and share threat, vulnerability, and risk information. Throughout the 2000s, the financial sector adopted an increasingly intelligence-driven approach to its cyber security operations and risk management.

Today, concepts commonplace to cyber security analysts have become well known in other sectors as well. One example is cyber kill-chain analysis – a phase-based model describing the stages of and responses to an attack. Another is presumption of breach – an approach to cyber security that starts with the assumption that a network has already been infiltrated as a means to detect intentionally hidden entities within a system. Industries outside strict cyber security sectors – such as the financial sector – are now beginning to incorporate these concepts into their understanding of managing cyber risks and defending critical infrastructures.

DISCUSSION

The panel discussion, moderated by Jason Healey, Senior Research Scholar at Columbia SIPA, focused on four topics: assessing the threat landscape; working to reduce vulnerabilities and minimize the attack surface; challenges in information sharing between the public and private sectors; and the value of simulations, games and exercises in better preparing for cyber-events.

Assessing the threat landscape

When determining whether an actor or action presents a threat, analysts normally consider three factors: intent, capability, and opportunity. Healey opened the panel by asking the panelists to provide an overview of the intent and capability of the threat

Panelists (from left to right): Steven Bellovin, Paul Bracken, Jason Healey, Louis Modano and Elizabeth Petrie

actors arrayed against the financial sector. Elizabeth Petri, Director of Strategic Intelligence Analysis at Citigroup, provided a sketch of five primary actors –a conceptualization that her fellow panelists largely agreed with:

1. Nation State / Advanced Persistent Threat: These actors are highly motivated, but their intentions are often ambiguous. They possess nearly unlimited capabilities and are usually able to gain unauthorized access to even the best protected systems.

2. Criminals: These actors are motivated by money, and their intentions are therefore usually clear. Their capabilities range widely. They can be highly skilled, particularly when they are able to hire nation-state actors as moonlighters. But they can also be effective even when relying on far less skilled hackers who employ tools purchased from underground markets.

3. Hacktivists: These actors are motivated by a cause and their intent is usually easy to discern; disruption rather than destruction or theft are common objectives. Their capabilities range from the sophisticated to the mundane.

4. Terrorists: These actors are motivated by a cause and their intent is typically to cause as much damage as possible. To date, their capabilities have appeared limited.

5. Insiders: These actors have the potential to cause grave damage, and their intent and capability vary widely. Many organizations deal with the insider threat separately from external threats.

There is potential for and some evidence of cross-pollination of tools and tactics, techniques, and procedures among these actors. Nevertheless, it is important for organizations to determine with some level of confidence who is attacking them. Attribution matters because if organizations understand an actor's intent and know what he is capable of they can tailor responses accordingly.

To aid attribution, financial institutions work with many vendors to obtain cyber threat information. There is a booming market for cyber intelligence, and cyber security firms are pushing the envelope to obtain the type of information that their customers need to build and maintain effective defenses. Attribution – long one of the great challenges in the cyber domain – is getting easier as analysts adopt an all-source intelligence approach. Many cyber consultancies are trying to extend their situational awareness as far as possible into “gray” (neutral) and “red” (adversary) space, including by developing human intelligence sources. Legal questions remain, and panelists noted that some companies have recently found that they need to put processes in place to determine

how these firms are collecting information to ensure that they are not engaged or complicit in unethical or illegal activity.

Panelists agreed that destructive malware attacks are everyone's worst nightmare, but had differing views on emerging problem areas. One panelist felt that mobile is the next big problem area. Another panelist worried about the big institutional links, which constitute a less stressed channel with an assumed level of trust. If an intruder gained access to one institution, he might be able to perpetrate an insider attack by presenting himself as a peer financial institution. Although there was not consensus about the relative risk associated with emerging threats, everyone agreed that the financial sector will continue to exist in the crosshairs of cyber actors everywhere.

Working to reduce vulnerabilities and shrink the attack surface

Even with demonstrated intent and sufficient capability, actors need opportunities to strike. The persistence of exploitable vulnerabilities in software provides a large attack surface. Panelists laid much of the blame for this situation on software makers. Steve Bellovin, Professor at Columbia School of Engineering, noted that the software industry is unique in its ability to get away with expansive disclaimers of liability, usually presented in the form of end user license agreements (EULAs), that are not tolerated in other industries. As long as the software industry is not held responsible for the security of its products, panelists expect the status quo of ubiquitous software vulnerabilities to persist.

Another reason vulnerabilities are likely to persist is that the growth rate of ambition, which often manifests itself in the complexity of software, has outpaced the ability to produce tight code. The prevailing culture of ship first, test later compounds this problem. It is expensive for software companies to assure a piece of complex software. Since they are not held liable for the security of their products, software companies pass the costs associated with software assurance along to their customers, including those in the financial sector, who have to conduct extensive and expensive testing to vet and validate software and fix vulnerabilities they discover.

In this environment, Louis Modano, Senior Vice President and Global Head of Infrastructure Services at NASDAQ, said that it is particularly important for customers to have a deep level of trust and close relationships, including at the developer level, with their software vendors and to do extensive testing. Even though it can sometimes cost more to fix and assure a piece of software than it did to acquire it in the first place, the costs of not doing the code assurance can be greater still in the event of a breach. To short-circuit the inevitable arguments between the business and security sides of a company over the cost of testing and fixing vulnerabilities in software, Modano said that companies have to educate everyone in an organization about what a breach means from a brand-impact perspective.

Information sharing: private sector successes and public-private challenges

The financial sector's status as a top target of cyber actors has pushed institutions to the leading edge of information sharing with regard to cyber threats. It is perhaps ironic that in a sector where information advantage is often the generator of profits that information sharing has become the key to improving cyber security. Yet, as Paul Bracken, Professor at the Yale School of Management, observed, sharing information in low-trust environments can be challenging. Panelists explained how the financial sector has solved this problem amongst competitors and rivals within the private sector by making cyber security a non-competitive space. It creates no advantage for Bank A to see a competitor taken down, because the actor could turn attention to Bank A next. That reality makes financial institutions want to share any vulnerabilities that they find with their competitors. The dynamic of being counterparts as opposed to competitors has helped improve cyber security in the financial sector. Panelists praised FS-ISAC as a valuable forum for sharing data with other financial institutions to fill gaps.

Sharing between the government and private sector is a bit more complicated. Panelists acknowledged that there is more skepticism about government actions and motives in the wake of Edward Snowden's disclosures. Some people feel that information sharing is a vehicle for increased surveillance. Others feel that although it can be helpful to have access to government information, which is often classified, to assist in attribution and the development of effective cyber defenses, that the government actually needs access to private sector data even more desperately than the private sector needs access to government data. Panelists noted that the private sector has more data than the government and often sees malicious activity before the government sees it. But the private sector does not have always the technical means to expedite the sharing of that data with the government. One workaround has been to collaborate in person in forums where information sharing is done on site, like the National Cyber Forensics and Training Alliance in Pittsburgh.

The value of simulations, gaming, and exercises

Simulations, war/business games, and table-top exercises can provide additional venues for information sharing and help build trust between participants, which can be helpful in crisis situations. Bracken noted that these types of exercises are also useful because they tend to reveal how little both public and private sector decision makers know and understand about the cyber domain. As a result, decision makers tend to defer to technical or legal experts who themselves are often neither qualified nor appropriately placed to make decisions on behalf of their organizations. In the private sector, legal teams often play a middle-man role in formulating responses to cyber events, but they rarely understand the dynamics of the issue outside of compliance concerns.

At the practical level, Modano explained how organizations can use the lessons learned from exercises to help manage a breach once it has happened. If companies can think through the steps they will need to take once a breach happens, they can then work backwards and try to take as many of those steps as possible before a breach to reduce

the risk of compromise. In the end, the response to cyber events is a problem of crisis management, and many companies – and governments – do not know what their objectives are. Is the goal to look steadfast? Preserve market capitalization? These are questions that senior decision makers need to consider, and exercises can help them think through the issues in advance of a crisis.

Once a breach happens, organizations need to learn as much as possible about what happened and why and share that information with other potential targets. To that end, Bellovin advocated for a cyber analog to the National Transportation Safety Board, which has a well-established investigative process that promotes learning and helps prevent future incidents. Cyber professionals, Bellovin said, could learn more from failures and apply that knowledge to build better defenses.

NEXT STEPS FOR RESEARCH AND POLICY

This panel discussion highlighted the need for additional research in the following areas:

1. Sharing information in low-trust environments: Research questions might include:
    a. Since it is often easiest to collaborate and share information in person, are there ways to expand cross-detailing within the private sector and between the public and private sectors?
    b. Are there more ways to bring private and public sector officials together before a crisis, recognizing that they will both be involved in real-world crisis responses?

2. Oversight of private-sector cyber intelligence brokers: Research questions might include:
    a. What type of public and/or private oversight of cyber intelligence brokers is warranted?
    b. How can companies become more informed consumers of private-sector cyber intelligence?

3. Building familiarity with cyber issues among senior decision makers in both the private and public sectors: Research questions might include:
    a. How to stimulate development, promulgation, and adoption of easy-to-understand frameworks to evaluate cyber events and guide responses to them?
    b. How best to increase familiarity with cyber issues among senior decision makers in both the private and public sectors?

4. Shrinking the cyber attack surface: Research questions include:

a. How can companies and the government work more closely with developers to improve software assurance?
b. Is there a role for Congress to play, for example by mandating changes to software EULAs to hold software companies liable for security issues associated with their products?

Panel 6A: Cyber vs. Nuclear: Conflict and Deterrence

Drafted by Peter Roady

Moderator:

Austin Long, Assistant Professor of International and Public Affairs, SIPA, Columbia University

Panelists:

Robert Jervis, Adlai E. Stevenson Professor and Professor of International and Public Affairs, Columbia University

Herbert Lin, Senior Research Scholar for Cyber Policy and Security, Center for International Security and Cooperation, Stanford University

Joseph Nye, University Distinguished Service Professor, Harvard University

EXECUTIVE SUMMARY

The motivating question behind this panel was: are lessons from the nuclear age, particularly with regard to conflict and deterrence, applicable to the cyber age? All three panelists – Robert Jervis, Herbert Lin, and Joseph Nye – have thought, spoken, and written extensively about what those thinking about cyber issues can learn from the nuclear age. Their conclusion is that the comparison is productive by virtue of the questions it surfaces, even though the nuclear and cyber answers to the questions differ dramatically. Research recommendations include: 1. Effective management of escalation ladders; 2. Deterrence – both cyber-domain specific and cross-domain; and 3. Arms control in the cyber domain.

BACKGROUND

The overarching question of this panel has to do with how states respond to disruptive new technologies. As cyber issues have become increasingly important in national security strategy, policy, and operations, decision makers have looked to some of the same people who helped them reason through the emergence of another disruptive technology: nuclear weapons. When viewed this way, as disruptive technologies, there are indeed overarching questions that transcend the vast differences in the specifics of the two technologies. Should this technology be used? If so, how, under what circumstances, by whom, and to what end? How would the use of this technology alter existing conflict escalation ladders? Should limits on this technology be sought?

Multiple generations of national security policy makers, strategists, and thinkers have confronted those questions in the nuclear context. The contours of those previous debates can help their successors think through the complexities associated with the cyber domain, even if the answers to these questions are very different in the cyber age. There is one caveat: effective reasoning by analogy requires a baseline level of understanding of both topics under comparison. Panelists noted that senior decision makers and their advisors would benefit from additional foundational education on cyber issues to enable them to make sound comparisons.

DISCUSSION

Referencing the lessons of the nuclear age, Joseph Nye, Distinguished Service Professor at Harvard University, counseled a degree of humility when forming judgments about the nature of the cyber domain, particularly as technology continues to change. Prevailing assumptions today, for instance, that offense dominates defense, may not hold in ten years. Strategy and policy may continue to lack empirical content because we have little to no information about what serious cyber conflict looks like.

Conflict: escalation ladders

During the Cold War, Nye described how strategists and policymakers spent a lot of time thinking about escalation ladders, the series of steps by which a conflict would unfold. The consensus by the 1960s was that the escalation ladder was fairly well defined and understood by both the United States and its principal rival, the Soviet Union, and that the use of nuclear weapons sat at the top. That is, using nuclear

Panelists (from left to right): Austin Long, Robert Jervis, Herbert Lin and Joseph Nye

weapons was the most escalatory step a belligerent could take in a conflict. The phrase “going nuclear” still connotes an extremely escalatory move.

By contrast, Herb Lin, Senior Research Scholar for Cyber Policy and Security at Stanford University, pointed out that “going cyber” seems to be at or near the bottom of the escalation ladder. Indeed, there have been occasional indications over the past decade that some decision makers see the potential for the use of cyber capabilities to be pre-escalatory or even de-escalatory. Kim Zetter's book on Stuxnet, the cyber capability that security researchers believe targeted the Iranian nuclear program, and the chapter on the same topic in David Sanger's book *Confront and Conceal*, show that senior decision makers may have considered the use of a cyber capability to achieve physical destruction to be far less escalatory than achieving the same result through boots-on-the-ground sabotage or aerial bombardment.

In principle, then, cyber capabilities may be just another tool in the foreign policy toolkit, at least in some instances. Yet the tight compartmentalization surrounding Stuxnet, as reported by Sanger, and the suggestion in the media and noted by panelists that the use of cyber capabilities requires Presidential authorization makes clear that, at present, decision makers consider cyber capabilities to be special.

The widely-reported struggle to promulgate rules of engagement for U.S. cyber operations belies the open question of whether cyber capabilities will be treated more like conventional capabilities, use of which can be delegated down to operational commanders, or more like nuclear or other special capabilities, use of which typically requires Presidential approval. The answer to this question has wide-ranging implications for military planning. Yet, as Robert Jervis, Professor of International and Public Affairs at Columbia, noted, the reported super compartmentalization of cyber issues makes the formulation of strategy and policy more difficult. The people tasked with developing cyber strategy and policy – many of whom are themselves quite senior -- may not know what the U.S. Government is capable of doing, is doing, and has done in the cyber domain.

Deterrence: cyber domain-specific vs. cross-domain

Jervis provided an eloquent synopsis of the underpinnings of deterrence and, in so doing, explained why cyber domain-specific deterrence is so difficult. The basic principle is that all participants in a state of conflict can restrain mutually destructive behavior by threatening to retaliate, which one can do by making credible threats and promises. The threats and promises do not have to be 100% credible. In many cases, 5% credibility is enough to deter an adversary, but 95% credibility may be needed to reassure allies. Credibility of promises — as Thomas Schelling pointed out long ago — is important. A truly credible threat includes a credible promise not to employ the threat if certain conditions are met.

Therein, Jervis explained, lies a problem for cyber domain-specific deterrence. The nature of cyber activity makes it very difficult, if not impossible, to make credible promises. One can imagine the difficulty of defending as harmless and promising not to

use a series of potentially crippling penetrations into critical systems intended for intelligence gathering that have been discovered by an adversary. The line between computer network exploitation (CNE) and computer network attack (CNA) can be thin indeed, a point echoed by Lin.

Another challenge for cyber domain-specific deterrence stems from the absence of the "crystal ball effect" of the nuclear age, wherein everyone knew what total war would look like. Despite Hollywood's valiant efforts (see the cyber-focused *Die Hard 4: Live Free or Die Hard)* no one is quite sure what total cyber war would look like or feel like. Many cyber experts think that the nuclear concept of Mutually Assured Destruction translates to, at best, Mutually Assured Disruption in the cyber domain, which does not generate the same fear factor.

Panelists felt that there is more potential for cross-domain deterrence and took heart that the U.S. Government seems headed in that direction, based on its response to the hacking of Sony in 2014. Nye asserted that of the dimensions of deterrence, entanglement is perhaps the most important, both generally and for cross-domain deterrence. Accepting that we do not know the full collateral effects of what it would mean to have cyber war, entanglement expands our perspective beyond the cyber domain. Jervis and Lin agreed, but noted that not only do we not understand the entanglement issue on the other side – we do not even understand it on our side. Whether such lack of understanding acts to increase or decrease the deterrent effect of entanglement is an open question.

Panelists challenged several assumptions that have long prevailed in the discourse on cyber deterrence, most notably that attribution is prohibitively difficult. Over the past five years, the ability to attribute cyber activity has improved considerably, because of technical advances, a move towards all-source attribution, and five more years of history to which today's hostile activity may be compared. The ability to attribute cyber activity with higher levels of confidence mitigates one of the principal barriers to deterrence in the cyber age. Nye noted that the increasing abilities of private sector companies to attribute cyber events with high levels of confidence constitutes a substantial change with implications for policymakers who can now publicly assign blame without necessarily having to compromise government sources and/or methods. As was discussed during the panel on cyber threats to the financial sector, however, there are some potential issues associated with how the booming private sector cyber intelligence industry is obtaining some of its information. Some level of scrutiny may be warranted, particularly when making use of intelligence collected by private sector entities.

Arms control

Panelists differed slightly on the prospects for arms control in the cyber domain. For Lin, the absence of verifiability would render futile any sort of traditional cyber arms limitation effort. Nye was more sanguine, and suggested that the evolution of nuclear arms control efforts show that the key is to start with a positive sum game. In the nuclear context, all parties to the Limited Test Ban Treaty – the first step in nuclear arms control

– saw it as in their interests to reduce the environmental degradation caused by nuclear testing. Nye suggested that rampant cyber crime might provide states with opportunities for positive sum negotiations.

A good next step, according to Nye, would be to consider cyber exclusion zones. The simple version would be that hospitals and schools are off limits. Then parties could build to things like civilian nuclear plants and the power grid, which is dual use. At some point, parties may be able to have a separate agreement that no one will attack nuclear command and control (C2) systems. While acknowledging that these agreements are not verifiable, Nye observed that sometimes non-verifiable agreements create moods that inhibit action and that it is not out of the question that exclusions could make some normative sense. Lin agreed that the principle of exclusion zones has merit but noted that the entangled nature of cyberspace makes establishing exclusion zones difficult.

Among the highlights of the discussion:

1. Cyber strategy and policy lack empirical content because we do not understand what cyber conflict looks like – something that was also true of nuclear strategy and policy. Unlike nuclear issues, however, panelists noted that senior decision makers appear to have limited knowledge of cyber issues. Panelists agreed that this combination of a lack of empirical content and limited knowledge could breed tremendous confusion in cyber crises. There is therefore a need for more education on cyber issues, including through exercises, for senior decision makers.

2. Panelists showed to be false the long-held assumption that cyber deterrence is impossible because attribution is impossible. The trend towards all-source intelligence attribution, relying in particular on human intelligence to supplement technical intelligence, and the growing involvement and capabilities of the private sector have combined to make attribution less of a challenge than in the past. With that barrier overcome, panelists suggested that deterrence might indeed be possible under some circumstances – and possibly more so if cross-domain deterrence were considered.

NEXT STEPS FOR RESEARCH AND POLICY

This panel discussion highlighted the need for additional research and work in the following areas:

1. Building a cyber baseline: Research questions in this area include:
   a. At the foundational level, what frameworks or schemas can policymakers use to understand the differential impacts of cyber events?
   b. What are the most effective ways to provide senior decision makers and their advisors with the foundational cyber knowledge they need to make informed policy choices? Are there roles for simulations, games, and exercises?

c. How can public policy schools help to build capacity in this area?

2. Deterrence: Possible research questions include:
   a. Is it possible to establish deterrence when there are multiple centers of power in the cyber domain, all of which have leverage and not all of which are nation states?
   b. Without a clear picture of the U.S. Government's cyber capabilities and track record, how best to develop a clearer understanding of escalation ladders in both cyber-specific and cross-domain contexts?

3. Arms control: Research questions might include:
   a. Are there positive sum games that can get the cyber arms control ball rolling?
   b. What work needs to be done - technical, policy, and legal - to understand and mitigate the entanglement issues that make formulating policy and strategy in the cyber domain so difficult?

Panel 6B: Cyber security and The Internet of Things

Drafted by Seda Gürses

Moderator:

Henning Schulzrinne, Professor, School of Engineering, Columbia University

Panelists:

James Kaplan, Partner, McKinsey & Company

Tobby Simon, Founder and President, Synergia Foundation; GCIG Commissioner

Rima Qureshi, Senior Vice President, Chief Strategy Officer and Head of M&A, Ericsson

EXECUTIVE SUMMARY

The panelists discussed the challenges of ensuring cyber security in an era where the Internet expands to every "thing." Questions covered include: When everyday objects are networked and are run by third parties, who defines what counts as threats, how are these threats prioritized, and how are appropriate measures to mitigate them decided upon? What are the challenges of remotely running computational services integrated into things, or vice versa, and what are the challenges of running things when the service providers are no longer present? Would regulation, standards or best practices be most effective in ensuring that security is not an afterthought when it comes to the Internet of Things (IoT)? Areas for future research include: 1. How to achieve cyber security in IoT; 2. Ways to apply cyber security measures to IoT; and 3. Means for balancing influences in cyber security policies between business and consumers.

BACKGROUND

The Internet of Things (IoT) is a computational paradigm built upon a vision of things or of an environment embedded with electronics, software, sensors, and actuators. These things use a local network or the existing Internet infrastructure to communicate with each other and cooperate with their surroundings to reach common goals. The term "Internet of Things" was first documented in 1999 by Kevin Ashton who suggested a shift from an Internet based on ideas about the world to an Internet based on information collected by things around people. By sensing the world through things, these technologies would be able to overcome the limitations of humans having to enter data about the world.

Historically, the IoT can be traced back to proposals for ways of organizing the world using cybernetic principles. Most evidently, Ashton's descriptions have vestiges of a 90s reiteration of these principles known as the "mirror world": as "reality" is captured in holistic information models, the mirror world can provide a total picture that can be manipulated for the benefit of the public (Gelernter, 1991). From this perspective, the IoT can be seen as a variation on ubiquitous, calm or pervasive computing, all popularized in the 90s. What differentiates Ashton and his colleagues at MIT's Auto-ID Center, however, is their explicit emphasis on the organizational control potential that could be brought to life through an IoT in the context of supply chains (Agre, 1997).

Fast forward 15 years and the Internet of Things has become the term of art to indicate the integration of sensors, actuators and distributed computational capabilities into different application domains. The associated services have entered the vernacular as "smart services." "Things" in this intelligent universe vary from insulin pumps, biochips for animal tracking, and thermostats to automobiles with built-in sensors. In addition to tracking, sensing their environments and automating actions, intelligent things are increasingly being used to co-organize people's everyday activities.

Depending on how present an embedded device is, people may be cognizant of their interactions with smart things in their environment. This makes it important to distinguish between owners of devices, users, and those who are functional subjects of these devices. For example, patients in a hospital may not be the users of smart devices but serve as their functional subjects, while the personnel at the hospital may not be the owners of the devices but use them. All three parties can be seen as stakeholders in the IoT and may have important security, privacy and safety interests.

In addition to user-facing interfaces, networked devices can be connected to a larger

Panelists (from left to right): Henning Schulzrinne, James Kaplan, Rima Qureshi and Tobby Simon

infrastructure over which they communicate with other devices or Internet based services. This allows devices to coordinate activities and make use of services that process the environmental data to respond to the needs of people in a smart environment. While such cooperation among devices is expected to make certain activities easier, it also raises concerns with respect to human agency.

Finally, the assemblage of service providers behind one or more things may complicate the concept of ownership of a device. This may raise further questions about responsibilities and liabilities. The complexity of such matters may have consequences for the quality of these services and civil liberties. Security can play a double role here: it may help ensure the quality of these services, which, depending on the mechanisms used, may have positive or negative impacts on civil liberties, e.g., privacy.

DISCUSSION

James Kaplan of McKinsey, Rima Qureshi of Ericsson, and Tobby Simon of the Synergia Foundation, in the panel moderated by Professor Henning Schulzrinne of Columbia University, focused their collective attention on the way in which existing security engineering paradigms, risk management, threat modeling, and software/hardware development must shift with the IoT and how this shift could be made.

Security in the era of IoT

Security in the context of an IoT requires manufacturers of smart things to think beyond securing a device. Manufacturers need to foresee ways to securely integrate these devices into smart environments. This is not trivial: in some cases, the device may move across security domains, in other cases it may be passed on from one owner/user/subject to another. The flexibility with which smart things may be put to use raises questions about how the system should be bootstrapped and who is responsible for the security of a device in different (trust) domains.

Here, better process integration in the production of smart devices, e.g., breaking away from product team silos, and improved communication across an organization deploying the IoT, e.g., in a hospital, were viewed by the panelists as essential to achieving better security in smart environments. Further, security in the IoT may be an emergent property of the production and deployment of these technologies. This requires end-to-end supply chain transparency and application of security mechanisms at each step of production.

Given the distributed nature of devices and IoT services, it is difficult to rely on physical proximity for achieving security. Smart devices will be integrated into smart environments, and hence are vulnerable to physical attacks. Data generated by these devices can be managed by multiple cloud services, which may not be aware of the sensitivity of the incoming data and lack the necessary security measures. Long-term security needs may also be a challenge: a device integrated into a smart building may have to be maintained over decades, while the company providing the services may not

be able to sustain maintenance over such long time intervals. Networked smart devices, absent service providers, may turn into security vulnerabilities. Furthermore, individually securing devices and services may be insufficient to understand the emergent behavior of systems that may provide additional attack surfaces. It may be a challenge to communicate these issues to users and subjects, especially if the devices are made invisible to their constituents, or "things" simply do not look like computers.

Risk management and threat modeling

The way in which security is addressed should not render the Internet of Things into an Internet of Fears. The panelists warned against over-securing and called for nuanced risk management, threat modeling and adversarial analysis. For example, domain specific threat models should drive the evaluation measures necessary to protect against nation-state attacks on critical infrastructure, rogue attacks on medical devices and potential violations of user privacy by service providers. Information sharing about attacks can be a valuable part of this process and should include informal channels, professional organizations and members of civil society. Panelists also emphasized that information sharing should not be limited by national security interests, and should be better organized to allow organizations to share security information across international supply chains.

To systematically address security, companies that only focus on securing their devices should be encouraged to think of the bigger picture. Given the cost of securing systems later in the development process, providers should be encouraged to integrate security into their product development models. Security on a device is bounded by the processing power of the underlying chips, meaning cheaper chips will not be conducive to high levels of security. The desire to push production costs down should not come at the cost of secure engineering.

IoT hardware and software

The panelists agreed that greater emphasis should be put into quality hardware and software development. These matters can be addressed through a combination of contracts, standards, common architectures, best practices and regulation. The panelists weighed the effectiveness of these different approaches. They agreed that all of these methods might fall short of ensuring better development models in smaller (start-up) companies. These companies may not be able to apply standardized development models and may disappear from the market before fulfilling basic safety and security requirements.

Here, the role of open source software for the IoT and open source communities in developing common standards could play a positive role. The panelists saw the potential for industry to make their resources more accessible to open source communities. This, they argued, could help bring open source practices in the IoT up to par with proprietary security and safety standards. Software and negative testing, i.e., testing devices to fail, were mentioned as security best practices. Skepticism was expressed towards checklists and regulation. The former was seen as unlikely to affect

the culture change necessary to achieve good security, while the latter was criticized for becoming obsolete by the time of implementation. In the worst case, one of the panelists emphasized, “compliance and security may evolve into two different things.” Instead, it was suggested that regulation can provide guiding principles or can be used to incentivize the use of best practices.

NEXT STEPS FOR RESEARCH AND POLICY

Three types of challenges can be identified from the panel discussion: the challenge of achieving cyber security in the IoT; the challenge of applying proposed cyber security measures to secure the IoT; and, finally, the challenges not addressed through either.

1. Achieving cyber security in the IoT: Research questions might include:
    a. What are the implications for safety and security issues as technology is increasingly designed in the context of “everyday things”?
    b. What kind of security measures can be built into technology designed for long-term use or as a component of a “smart environment”?
    c. How can a secure infrastructure for the IoT be developed so that it avoids known security vulnerabilities e.g., the Object Naming Service proposed for the IoT leverages the Domain Name System (DNS) and in the process replicates all of its vulnerabilities?

2. Applying cyber security measures to the IoT: Research questions in this area might include:
    a. How to make sure that even the weakest link is minimally secure and that ‘things’ are compartmentalized?
    b. How could taking a differentiated approach to threat modeling and risk management help avoid creating an “Internet of Fears”?
    c. What incentives can be offered to software and hardware manufacturers to encourage cooperation with other players in the supply chain (e.g., chip manufacturers as well as app developers)?

3. Balancing influences in cyber security policy: Research questions in this area may include:
    a. How can businesses address liability concerns for business-to-business relationships while also protecting customer needs?
    b. How can conflicts between security and safety requirements be addressed in such a way as to respect civil liberties?
    c. How will the development of a cyber security insurance market address liability issues for both businesses and consumers?

References

Plenary Panel 2: The Future of Multi-stakeholder Internet Governance

DeNardis, L. (2014). *The global war for Internet governance.* New Heaven: Yale University Press.

Goldsmith, S., & Eggers, W. D. (2011). *Governar em rede: o novo formato do setor público.* Brasília: ENAP.

ICANN. (2014). Towards a Collaborative, Decentralized Internet Governance Ecosystem.

Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance*, Cambridge: The MIT Press.

Verhulst, S. G., Noveck, B. S., Raines, J., & Declercq, A. (2014). *Innovations in Global Governance: Toward a distributed Internet Governance Ecosystem.* Ontario: Global Commission on Internet Governance.

Panel 4A: Privacy, Big Data and the Internet

Boyd d. and Crawford K. (2012), Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon, Information, Communication and Society, Vol.15 (5): 662-679.

Brill J. (2015), It's Getting Real: Privacy, Security, and Fairness in the Internet of Things, Keynote Address at Carnegie Mellon University Data Privacy Day (Jan. 28, 2015), available at https://www.ftc.gov/system/files/documents/public_statements/621381/150128dataprivacyday.pdf (accessed 12 September, 2015).

Electronic Frontier Foundation (EFF) (2015), Manila Principles on Intermediary Liability, available from: https://www.manilaprinciples.org (accessed 12 September, 2015).

Kitchin R. (2014), Big Data, new epistemologies and paradigm shifts, Big Data and Society, April–June 2014: 1–12.

Mayer-Schönberger V. (2011), *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press: Princeton, NJ, USA.

Narayanan A. and Schmatikov V. (2010), Myths and fallacies of "Personally Identifiable Information", Communications of the ACM, Vol. 53 (6), June 2010: 24-26.

Norman D. (1993), Things that make us smart: defending human attributes in the age of the machine, Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA.

Sweeney L. (2002), *k*-anonymity: a model for protecting privacy, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol 10 (5), October 2002: 557-570.

United Nations High Commissioner for Human Rights (2015), Report on encryption, anonymity, and the human rights framework, available from: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx (accessed 12 September, 2015).

Opening Keynote Discussion, Day 2: Cyber Security

Baraniuk C. (2015), Ghosts in the machines, New Scientist, Vol. 227 (3028), 4 July 2015, pp 38-41.

Verizon (2014), Data Breach Investigations Report, available from: http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf (accessed 6 August, 2015).

Panel 6B: Cyber security And The Internet Of Things

Agre P. E. (1997), Beyond the mirror world: Privacy and the representational practices of computing. In Philip E. Agre and Marc Rotenberg, editors, *Technology and Privacy*, pages 29–61. MIT Press, Cambridge, MA, USA, 1997.

Ashton K (2009), In the real world, things matter more than ideas. RFID Journal, 22. June 2009.

Gelernter D. (1991), *Mirror Worlds: or the Day Software Puts the Universe in a Shoebox... How It Will Happen and What It Will Mean*. Oxford University Press, 1991.

Appendix 1: Full Conference Agenda

Day 1: Thursday 14 May, 2015

Start	End		
			Thursday 14 May, 2015
8:00	9:00		**Registration & Breakfast** *(Foyer)*
9:00	10:00		**Opening** *(Theater)* **Welcome**: ***Merit E. Janow***, Dean, SIPA, Columbia University **A conversation with:** ***Vinton G. Cerf****, Vice President & Chief Internet Evangelist, Google;* ***Lawrence Strickling****, Assistant Secretary for Communications and Information, U.S. Department of Commerce* ***Laura DeNardis***, GCIG Director of Research & Professor, American University
10:00	11:15		**Plenary Panel 1: Examining the Future of the Open and Universal Internet** *(Theater)* *Moderator: **Eli Noam**, Professor, Columbia Business School* ***Leslie Daigle****, former Chief Internet Technology Officer, Internet Society; GCIG Research Advisory Network member* ***Jacquelynn Ruff****, Vice President, International Public Policy & Regulatory Affairs, Verizon Communications* ***Andrew Wyckoff****, Director, Directorate for Science, Technology and Innovation, OECD; GCIG Research Advisory Network member* ***Christopher Yoo****, Professor, University of Pennsylvania Law School; GCIG Research Advisory Network member*
11:15	11:30		Coffee Break
11:30	12:30		**Plenary Panel 2: The Future of Multi-stakeholder Internet Governance** *(Theater)* *Keynote & Moderator: **Ambassador David Gross**, Partner, Wiley Rein* ***Kathryn Brown****, President and CEO, Internet Society* ***Fadi Chehadé****, CEO & President, ICANN* ***Beth Noveck****, Director, NYU GovLab; GCIG Commissioner* ***Paul Twomey****, former ICANN Chair, GCIG Commissioner*
12:30	1:15		Lunch in Theater
1:15	2:00		**Fireside Chat: An Examination of US Policy and Law in a Global Landscape** *(Theater)* ***Brad Smith*****,** *General Counsel & Executive Vice President, Legal and Corporate Affairs, Microsoft* *Moderator: **Merit E. Janow**, Dean, SIPA, Columbia University*
2:00	2:30		Coffee Break

Start	End			
2:30	3:30		**Panel 3A: Human rights, Freedom of Expression and the Internet** *(Library)* *Moderator:* ***Anya Schiffrin****, Director, International Media, Advocacy and Communications specialization, SIPA, Columbia University* ***Agnes Callamard****, Director, Global Freedom of Expression & Information @Columbia* ***Fen Hampson****, Distinguished Fellow and Director of Global Security & Politics Program, CIGI, Co-Director of GCIG, and Chancellor's Professor, Carleton University* ***Carolina Rossini****, Vice President for International Policy and Strategy, Public Knowledge; GCIG Research Advisory Network member* ***Marietje Schaake****, Member of European Parliament; GCIG Commissioner*	**Panel 3B: Trade, Internet Governance, and Cross-border Data Flows** *(Theater)* Moderator: ***Gordon Goldstein***, Managing Director & Head of External Affairs, Silverlake ***Nick Ashton-Hart***, Executive Director, Internet & Digital Ecosystem Alliance (IDEA) ***Susan Chalmers***, Principal, Chalmers & Associates ***Anupam Chander,*** *Professor, University of California Davis* ***Victoria Espinel,*** *CEO & President, Business Software Alliance*
3:30	3:45		Coffee Break	
3:45	5:00		**Panel 4A: Privacy, Big Data and the Internet** *(Theater)* *Moderator:* ***Andrew McLaughlin****, Senior Fellow, SIPA, Columbia University* ***Matthew Jones****, James R. Barker Professor of Contemporary Civilization, Department of History Columbia University* ***Rebecca MacKinnon****, Director, Ranking Digital Rights project, New America* ***Michael Nelson****, Public Policy, CloudFlare* ***Nuala O'Connor****, President & CEO, Center for Democracy & Technology*	**Panel 4B: Innovation and the Internet** *(Library)* *Moderator:* ***Merit E. Janow****, Dean, SIPA, Columbia University* ***Brad Burnham****, Managing Partner, Union Square Ventures* ***Konstantinos Komaitis****, Senior Policy Advisor, Internet Society; GCIG Research Advisory Network member* ***Ronaldo Lemos****, Director, Institute for Technology & Society of Rio de Janeiro; GCIG Research Advisory Network member* ***Sharad Sanghi****, CEO & Founder, Netmagic Solutions*
5:00	5:30		**Concluding Observations**	
5:30	6:00		Break	
6:00	6:30		**Cocktail reception (Invitation only)** *(International Affairs Building, 15th floor)*	
6:30	9:00		**Dinner & Fireside Chat with Policy Makers (Invitation only)** *(International Affairs Building, 15th floor)* ***Christopher Painter****, Coordinator for Cyber Issues, U.S. Department of State* ***Marietje Schaake****, Member of European Parliament; GCIG Commissioner* ***Grant Aldonas****, former U.S. Under Secretary of Commerce for International Trade* *And other invited guests*	

Day 2: Friday 15 May, 2015

Start	End			
8:00	9:00		**Registration & Breakfast** *(Foyer)*	
9:00	9:45		**Joint-keynote** *(Theater)* ***Michael Chertoff***, former Secretary of the U.S. Department of Homeland Security; GCIG Commissioner ***Kevin Mandia,*** *Chief Operating Officer & Senior Vice President, FireEye* *Moderator:* ***Merit E. Janow****, Dean, SIPA, Columbia University*	
9:45	11:00		**Panel 5: Mitigating Cyber-risks in Critical Infrastructure: Private and Public Responses for the Financial Sector** *(Theater)* *Moderator:* ***Jason Healey****, Senior Research Scholar, Cyber Policy, SIPA, Columbia University* ***Steven Bellovin****, Professor, School of Engineering, Columbia University* ***Paul Bracken****, Professor, Yale School of Management* ***Louis Modano****, Senior Vice President & Global Head of Infrastructure Services, NASDAQ* ***Elizabeth Petrie****, Director, Strategic Intelligence Analysis, Citigroup Information Protection Directorate*	
11:00	11:15		Coffee Break	
11:15	12:30		**Panel 6A: Nuclear vs Cyber: Conflict & Deterrence** *(Library)* *Moderator:* ***Austin Long****, Assistant Professor, SIPA, Columbia University* ***Robert Jervis****, Adlai E. Stevenson Professor of International Politics, Department of Political Science & SIPA, Columbia University* ***Herbert Lin****, Senior Research Scholar for Cyber Policy and Security, Center for International Security and Cooperation, Stanford University* ***Joseph Nye****, Professor, Harvard Kennedy School; GCIG Commissioner*	**Panel 6B: Cyber-security and the Internet of Things** *(Theater)* *Moderator:* ***Henning Schulzrinne****, Professor, School of Engineering, Columbia University* ***James Kaplan****, Partner, McKinsey & Company* ***Tobby Simon****, Founder & President, Synergia Foundation; GCIG Commissioner* ***Rima Qureshi****, Senior Vice President, Chief Strategy Officer and Head of M&A, Ericsson*
12:30	12:45		Break	
12:45	2:00		**Concluding Luncheon with Keynote and Discussion** *(Theater)* ***Gregory Rattray****, Global Chief Information Security Officer, JP Morgan Chase & Co.* *Moderator:* ***Merit E. Janow****, Dean, SIPA, Columbia University*	

Appendix 2: Speaker Bios

DAY ONE: INTERNET GOVERNANCE

OPENING JOINT-KEYNOTE

***Merit E. Janow**, Dean, SIPA, Columbia University*

Merit E. Janow is an internationally recognized expert in international trade and investment, with extensive experience in academia, government, international organizations, and business. She has been a professor of practice at Columbia University's School of International and Public Affairs (SIPA) and affiliated faculty at Columbia Law School since 1995. Currently, in addition to being dean of SIPA, she is co-director of the APEC Study Center and, until recently, chair of the faculty oversight committee of Columbia Global Centers | East Asia. In December 2003, Janow was elected for a four-year term as one of the seven members of the World Trade Organization's (WTO) Appellate Body—the first female to serve on the Appellate Body. From 1997 to 2000, she served as the executive director of the first international antitrust advisory committee of the U.S. Department of Justice. Prior to joining Columbia's faculty, she was deputy assistant U.S. trade representative for Japan and China (1989–93). Janow is on the board of directors of several corporations and not-for-profit organizations. In 2009, she became a charter member of the International Advisory Council of China's sovereign wealth fund, China Investment Corporation or CIC.

***Vinton G. Cerf**, Vice President and Chief Internet Evangelist, Google*

Vinton G. Cerf is vice president and chief Internet evangelist for Google. Cerf is the codesigner of the TCP/IP protocols and the architecture of the Internet. He has served in executive positions at ICANN, the Internet Society, MCI, the Corporation for National Research Initiatives, and the Defense Advanced Research Projects Agency. He is the past president of the Association for Computing Machinery and is a member of the National Science Board.

Cerf is a recipient of numerous awards for his work, including the U.S. Presidential Medal of Freedom, the U.S. National Medal of Technology, the Queen Elizabeth Prize for Engineering, the Prince of Asturias Award, the Tunisian National Medal of Science, the Japan Prize, the Charles Stark Draper Award, the ACM Turing Award, the Legion d'Honneur, and 24 honorary degrees.

***Laura DeNardis**, Director of Research, Global Commission on Internet Governance; Professor, American University*

Laura DeNardis is a scholar of Internet architecture and governance and a professor in the School of Communication at American University in Washington, D.C. The author of *The Global War for Internet Governance* (Yale University Press, 2014) and other books, her expertise has been featured in *Science Magazine*, *The Economist*, *National Public Radio*, *The New York Times*, *Time Magazine*, *Christian Science Monitor*, *Slate*, *Reuters*, *Forbes*, *The Atlantic*, and *The Wall Street Journal*. Dr. DeNardis is an affiliated fellow of the Yale Law School Information Society Project and previously served as its executive director. She is a senior fellow of the Centre for International Governance Innovation and holds an international appointment as research director for the Global Commission on Internet Governance. She holds an AB in Engineering Science from Dartmouth College, a Master of Engineering from Cornell University, and a PhD in Science and Technology Studies from Virginia Tech, and was awarded a postdoctoral fellowship from Yale Law School.

***Lawrence Strickling**, Assistant Secretary for Communications and Information, U.S. Department of Commerce*

Lawrence E. Strickling was sworn in as assistant secretary for communications and information at the Department of Commerce in June 2009. In this role, Strickling serves as administrator of the National Telecommunications and Information Administration (NTIA), the Executive Branch agency that is principally responsible for advising the President on telecommunications and information policy. A technology policy expert with more than two decades of experience in the public and private sectors, Strickling's focus at NTIA includes leading initiatives to expand broadband Internet access and adoption in America and to ensure that the Internet remains an engine for continued innovation and economic growth.

After joining NTIA, Strickling oversaw the development of an approximately $4 billion Recovery Act broadband grants program and now manages the rigorous oversight of these nationwide broadband projects to ensure they deliver timely and lasting benefits to the American public. Additionally, under Strickling's leadership, NTIA launched America's first public, searchable nationwide map of consumer broadband Internet availability and crafted a ten-year plan that the agency is now implementing to nearly double the amount of commercial spectrum available for wireless broadband, as directed by President Obama. Strickling also oversees NTIA's efforts on a host of domestic and global Internet policy and administrative issues, including playing a key role in the Commerce Department's Internet Policy Task Force, advocating the U.S. government's policy positions abroad, and promoting the stability and security of the Internet's domain name system through its participation on behalf of the U.S. government in Internet Corporation for Assigned Names and Numbers (ICANN) activities.

Previously in government, Strickling served at the Federal Communications Commission as Chief of the Common Carrier Bureau from 1998 to 2000, working to promote competition and protect consumers in the telecommunications sector and implement many of the key provisions of the Telecommunications Act of 1996. Prior to that, Strickling was associate general counsel and chief of the FCC's Competition Division. In the private sector, Strickling was chief regulatory and chief compliance officer at telecommunications service provider Broadwing Communications, LLC, from 2004 to 2007. His private sector experience from 2000 to 2004 included serving in senior roles at competitive communications service providers Allegiance Telecom, Inc., and CoreExpress, Inc., and as a member of the Board of Directors of Network Plus. From 1993 to 1997, Strickling was vice president of public policy at Regional Bell operating company Ameritech Corp., where he was responsible for developing and implementing Ameritech's state and federal regulatory and legislative agenda. Strickling was also a litigation partner at the Chicago law firm of Kirkland & Ellis. Strickling earned his JD from Harvard Law School and is a Phi Beta Kappa graduate of the University of Maryland with a degree in economics.

PLENARY PANEL 1: EXAMINING THE FUTURE OF THE OPEN AND UNIVERSAL INTERNET

***Moderator: Eli Noam**, Professor, Columbia Business School*

Eli Noam is professor of economics and finance at the Columbia Business School since 1976 and its Garrett Professor of Public Policy and Business Responsibility. He served for three years as a commissioner for public services of New York State. Noam was appointed by the White House to the President's IT Advisory Committee. He is director of the Columbia Institute for Tele-Information, a research center focusing on management and policy issues in communications, Internet, and media. He has also taught at Columbia Law School, Princeton University's Economics Department and Woodrow Wilson School, and the University of St. Gallen, and is active in the development of electronic distance education. Noam has published 30 books and over 300 articles in economics journals, law reviews, and interdisciplinary journals, and is a regular columnist for the *Financial Times* online edition. His recent books include *Who Owns the World's Media?* (Oxford, forthcoming), *Media Ownership and Concentration in America* (Oxford); *Peer-to-Peer Video* (Springer); and *Media Management* (four volumes, forthcoming); and his recent projects include A National Initiative for Next Generation Video, Ultrabroadband, and Next Generation Wireless.

Noam was the chairman of the International Media Management Academic Association, 2012–2014. He has been a member of advisory boards for the federal government's telecommunications network, the IRS computer system, the National Computer Systems Laboratory, the National Commission on the Status of Women in Computing, the Governor's Task Force on New Media, and Intek Corporation. His academic, advisory, and nonprofit board and trustee memberships include the Nexus Mundi Foundation (chairman), Oxford Internet

Institute, Jones International University (the first accredited online university), the Electronic Privacy Information Center, the Minority Media Council, and several committees of the National Research Council. He served on advisory boards for the governments of Ireland and Sweden and is a member of the Council on Foreign Relations. He is a commercially rated pilot, served in the Israel Air Force in the 1967 and 1973 wars, and is currently a search and rescue pilot with the Civil Air Patrol (1st Lt.). He is married to Nadine Strossen, a law professor and national president of the American Civil Liberties Union for 18 years. He received the degrees of BA, MA, PhD (Economics), and JD from Harvard University, and honorary doctorates from the University of Munich (2006) and the University of Marseilles (2008).

***Leslie Daigle**, Former Chief Internet Technology Officer, Internet Society; GCIG Research Advisory Network Member*

Leslie Daigle has been actively involved in shaping the Internet's technical evolution for more than a dozen years. Her role with the Internet Society (ISOC) was to provide strategic leadership on important technical issues as they relate to ISOC's ongoing programs. She has worked with the Internet Engineering Task Force (IETF) since 1995 and was an appointed member of the related Internet Architecture Board (IAB) from March 2000 to March 2008. As the elected chair of the IAB from 2002 to 2007, Leslie steered the IAB and the related IETF through a period of important industry and institutional change by working with diverse technical groups to align their interests and develop sustainable relationships.

Apart from her leadership role with the IAB, Leslie has been a strong promoter of the development of Internet identifiers and directory systems, which allow for the creation of standards-based, interoperable application protocols to support end-users across the Internet in their use of remote resources. She recently published standards for DNS-based application service discovery. Leslie has served as a panelist with the National Science Foundation review committee, evaluating Internet-related research proposals submitted for funding. She holds an MSc in Computing and Information Science from the University of Guelph and a BSc in Math and Computer Science from McGill University. Leslie was most recently a consulting engineer at Cisco Systems. Previously she held the position of director of directory research at VeriSign and vice president for research at industry pioneer Bunyip Information Systems, among others. Leslie left the Internet Society in May 2014.

***Jacquelynn Ruff**, Vice President, International Public Policy and Regulatory Affairs, Verizon Communications*

Jacquelynn (Jackie) Ruff is vice president for international public policy and regulatory affairs at Verizon Communications. She leads the group that is responsible for global public policy development, advocacy, and guidance. She directs activity in U.S. and international forums, such as the International Telecommunication Union, the OECD, APEC, and the Internet Governance Forum. She is a member of federal advisory committees to the Department of State

and to the U.S. Trade Representative, and a member of the boards of the U.S. Telecom Training Institute and the Trans-Atlantic Business Council.

Ms. Ruff joined Verizon from the International Bureau of the Federal Communications Commission. Previously, she practiced with the communications and the Latin America groups of an international law firm and served on the staff of a United States Senate Committee. Ms. Ruff holds a JD from the Georgetown University Law Center, an MA from Harvard University, and a BA from Radcliffe College/Harvard University.

***Andrew Wyckoff**, Director, Directorate for Science, Technology and Innovation, OECD; GCIG Research Advisory Network Member*

Andrew W. Wyckoff is the director of the OECD's Directorate for Science, Technology, and Innovation (STI) where he oversees OECD's work on innovation, business dynamics, science and technology, and information and communication technology policy, as well as the statistical work associated with each of these areas. Mr. Wyckoff was previously head of OECD's Information, Computer and Communications Policy (ICCP) division, which supports the organization's work on information society as well as consumer policy issues. Before heading ICCP, he was the head of STI's Economic Analysis and Statistics Division, which develops methodological guidelines, collects statistics and undertakes empirical analysis in support of science, technology, and innovation policy analysis.

His experience prior to the OECD includes being a program manager of the Information, Telecommunications and Commerce program of the U.S. Congressional Office of Technology Assessment (OTA), an economist at the U.S. National Science Foundation (NSF), and a programmer at The Brookings Institution. Mr. Wyckoff is a citizen of the United States and holds a BA in Economics from the University of Vermont and a Master of Public Policy from the JFK School of Government, Harvard University.

***Christopher Yoo**, Professor, University of Pennsylvania Law School; GCIG Research Advisory Network Member*

Christopher Yoo has emerged as one of the nation's leading authorities on law and technology. His research focuses on how the principles of network engineering and the economics of imperfect competition can provide insights into the regulation of electronic communications. He has been a leading voice in the "network neutrality" debate that has dominated Internet policy over the past several years. He is also pursuing research on copyright theory as well as the history of presidential power. He is the author of *The Dynamic Internet: How Technology, Users, and Businesses Are Transforming the Network* (AEI Press, 2012), *Networks in Telecommunications: Economics and Law* (Cambridge Univ. Press, 2009) (with Daniel F. Spulber), and *The Unitary Executive: Presidential Power from Washington to Bush* (Yale University Press, 2008) (with Steven G. Calabresi). Yoo testifies frequently before Congress, the

Federal Communications Commission, and the Federal Trade Commission.

PLENARY PANEL 2: THE FUTURE OF MULTI-STAKEHOLDER INTERNET GOVERNANCE

***Keynote and Moderator: Ambassador David Gross**, Partner, Wiley Rein*

David is one of the world's foremost experts on international telecommunications and Internet policy, having addressed the United Nations (UN) General Assembly and led more U.S. delegations to major international telecommunication and Internet conferences than anyone else in modern history. Drawing on his more than 30 years of experience as a lawyer, global policy maker, and corporate executive, he assists U.S. companies seeking to enter or expand international businesses; and non-U.S. companies and organizations seeking to invest in, monitor, and understand the U.S. and international markets, as well as national governments. David advises companies and others on international and domestic telecoms, Internet, and high-tech strategy focusing on both specific markets and international organizations such as the International Telecommunication Union (ITU), Organization for Economic Cooperation and Development (OECD), and Asia Pacific Economic Cooperative (APEC), as well as many regional organizations.

***Kathryn Brown**, President and CEO, Internet Society*

Kathryn C. Brown joined the Internet Society as president and chief executive officer on January 1, 2014. She is a veteran of Internet policy development and corporate responsibility initiatives that have aided in the Internet's global expansion. At Verizon, she helped identify and navigate emerging digital issues and led its global corporate responsibility initiatives. In her policy role, she led the company's international public policy engagement through a period of dynamic change. She represented the company in the successful adoption by the OECD of principles for Internet policymaking and was a member of the U.S. delegation to the ITU World Conference on International Telecommunications treaty negotiations.

As leader of Verizon's corporate responsibility initiatives, she served on Verizon's corporate councils for the development of the company's online privacy and content policies and promoted Verizon's Human Rights Statement and Supplier Code of Conduct. Additionally, she oversaw an investment of more than $60 million a year in programs and grants from the Verizon Foundation that helped support Internet development. In 2010 she partnered with the Internet Society to launch a highly successful forum on the Internet and higher education in East Africa. Kathy joined Verizon from the Washington D.C. law firm Wilmer, Cutler & Pickering, where she was a partner specializing in legal and regulatory communications policy.

Earlier in her career, Kathy served in President Clinton's administration where she was deeply involved in policy development that was instrumental to the deployment and adoption of the

global Internet. She served as head of the Office of Policy and Development at the National Telecommunications Information Administration and then as chief of staff to Federal Communications Commission Chairman William E. Kennard. At the FCC, she managed the staff supporting Chairman Kennard's historic decision to keep the Internet unregulated, to fund the E-rate, and to increase radio spectrum availability to fuel wireless technology innovation. Before moving to Washington D.C., Kathy held senior roles for 15 years in government service in New York.

Most recently, Kathy was a senior advisor at global strategy firm Albright Stonebridge Group. Kathy received her JD, summa cum laude, from Syracuse University College of Law and her BA, magna cum laude, from Marist College. She spent one year studying at Makerere University in Kampala, Uganda, and in Leeds, United Kingdom. Kathy has served on the advisory boards of the Public Interest Registry (.ORG), the mPowering Development Advisory Board of the ITU, and the USC Annenberg Innovation Lab.

***Fadi Chehadé**, CEO and President, Internet Corporation for Assigned Names and Numbers (ICANN)*

Mr. Chehadé is president and chief executive officer of the Internet Corporation for Assigned Names and Numbers (ICANN). He has more than 25 years of experience in building and leading progressive Internet enterprises, and leveraging relationships with senior executives and government officials across Asia, Europe, the Middle East, and the United States. Mr. Chehadé is a citizen of Egypt, Lebanon, and the United States. He was born in Beirut, Lebanon, to Egyptian parents and left the then war-torn country in 1980 at the age of 18. He speaks fluent Arabic, English, French, and Italian. Most recently, he served as CEO of Vocado LLC, a U.S. firm that is a provider of cloud-based software for the administration of educational institutions. Prior to Vocado, Mr. Chehadé was CEO of CoreObjects Software, Inc., a leader in new product software development services for both large and growing companies. He oversaw the expansion of the company to include more than 400 engineers and its successful acquisition by Symphony Services.

Earlier in his career, Mr. Chehadé was the general manager for IBM's Global Technology Services in the Middle East and North Africa. Based in Dubai, he led a team across an emerging region experiencing high growth, built a new global business for IBM, and provided managed services to large clients in telecommunications, aerospace, and retail to improve the accuracy, depth, and timeliness of business information visibility across demand and supply chains.

Mr. Chehadé has founded three companies since 1987: Viacore, a B2B process integration hub offering a complete solution of specialized software and services, which was acquired by IBM; RosettaNet, a nonprofit multi-stakeholder company; and Nett Information Products, an Internet-based content management and sharing solution, which was acquired by Ingram Micro.

Mr. Chehadé is a graduate of Stanford University, where he earned a master's degree in engineering management and of Polytechnic University in New York, where he graduated

summa cum laude with a bachelor's degree in computer science.

***Beth Noveck**, Director, NYU GovLab; GCIG Commissioner*

Beth Simone Noveck directs The Governance Lab and its MacArthur Research Network on Opening Governance. Funded by the John D. and Catherine T. MacArthur Foundation, the John S. and James L. Knight Foundation, and Google.org, the GovLab strives to improve people's lives by changing how we govern. The GovLab designs and tests technology, policy and strategies for fostering more open and collaborative approaches to strengthen the ability of people and institutions to work together to solve problems, make decisions, resolve conflict, and govern themselves more effectively and legitimately.

The Jerry Hultin Global Network Visiting Professor at New York University's Polytechnic School of Engineering, she was formerly the Jacob K. Javits Visiting Professor at the Robert F. Wagner Graduate School of Public Service and a visiting professor at the MIT Media Lab. Beth is a professor of law at New York Law School and a senior fellow at the Yale Law School Information Society Project. She served in the White House as the first United States Deputy Chief Technology Officer and director of the White House Open Government Initiative (2009–2011). UK Prime Minister David Cameron appointed her senior advisor for Open Government, and she served on the Obama-Biden transition team. Among projects she's designed or collaborated on are Unchat, The Do Tank, Peer To Patent, Data.gov, Challenge.gov, and The GovLab's Living Labs and training platform, The Academy.

A graduate of Harvard University and Yale Law School, she serves on the Global Commission on Internet Governance and chaired the ICANN Strategy Panel on Multi-Stakeholder Innovation. She is a member of the Advisory Board of the Open Contracting Partnership. She was named one of the "Foreign Policy 100" by *Foreign Policy*, one of the "100 Most Creative People in Business" by *Fast Company*, and one of the "Top Women in Technology" by *The Huffington Post*. She has also been honored by both the National Democratic Institute and Public Knowledge for her work in civic technology.

Beth is the author of *Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful*, which has also appeared in Arabic, Russian, and Chinese, and in an audio edition, and coeditor of *The State of Play: Law, Games, and Virtual Worlds*. Her next book *Smart Citizens, Smarter State: The Technologies of Expertise and the Future of Governing* will appear with Harvard University Press in 2015. She tweets @bethnoveck.

***Paul Twomey**, Former Chair, ICANN; GCIG Commissioner*

Paul Twomey was the CEO and president of the Internet Corporation for Assigned Names and Numbers (ICANN) from 2003 to 2009. He was the initial chairman of ICANN's Governmental Advisory Committee from 1999 to 2003. Prior to that, Paul was the Australian Government's

Special Adviser for IT and Information Economy and CEO of its National Office for the Information Economy. He has held executive positions within the Australian Government's foreign trade organization. He is a former senior consultant with McKinsey & Company. Paul is also the founder of Argo Pacific, a high-level international advisory and cyber security firm.

LUNCH AND FIRESIDE CHAT: AN EXAMINATION OF U.S. POLICY AND LAW IN A GLOBAL LANDSCAPE

Moderator: Merit E. Janow, *Dean, SIPA, Columbia University*

Brad Smith*, General Counsel and Executive Vice President, Legal and Corporate Affairs, Microsoft*

Brad Smith is Microsoft's general counsel and executive vice president of legal and corporate affairs. He leads the company's department of Legal and Corporate Affairs (LCA), which has approximately 1,100 employees located in 55 countries. Mr. Smith is responsible for the company's legal work, intellectual property portfolio, and patent licensing business, as well as its government affairs and philanthropic work. He also serves as Microsoft's corporate secretary and its chief compliance officer. Mr. Smith currently cochairs the board of directors of Kids in Need of Defense (KIND) and is the chair-elect of the Leadership Council on Legal Diversity. In Washington State, Mr. Smith has served as chair of the Washington Roundtable, a leading Washington State–based business organization, and he has advanced several statewide education initiatives.

PANEL 3A: HUMAN RIGHTS, FREEDOM OF EXPRESSION, AND THE INTERNET

Moderator: Anya Schiffrin*, Director, International Media, Advocacy and Communications Specialization, SIPA, Columbia University*

Anya Schiffrin is the director of the International Media, Advocacy and Communications specialization at Columbia University's School of International and Public Affairs. She teaches courses on media and development and innovation as well as the course Media, Human Rights and Social Change. Among other topics, she writes on journalism and development as well as the media in Africa and the extractive sector. Schiffrin spent 10 years working overseas as a journalist in Europe and Asia and was a Knight-Bagehot Fellow at Columbia University's Graduate School of Journalism in 1999–2000. Schiffrin is on the advisory board of the Open Society Foundation's Program on Independent Journalism and of Revenue Watch Institute. Her

recent book is *Global Muckraking: 100 Years of Investigative Reporting from Around the World* (New Press, 2014).

***Agnès Callamard**, Director, Global Freedom of Expression and Information @ Columbia*

Dr. Agnès Callamard took up the post of executive director for ARTICLE 19, the international human rights organization working globally for freedom of expression in October 2004. She has had a distinguished career in human rights and humanitarian work. Agnès is a former chef de cabinet for the secretary general of Amnesty International and, as the organization's research policy coordinator, she led Amnesty's work on women's human rights. Agnès has conducted human rights investigations in a large number of countries in Africa, Asia, and the Middle East. She founded and led HAP International (the Humanitarian Accountability Partnership), where she oversaw field trials in Afghanistan, Cambodia, and Sierra Leone, and worked extensively in the field of international refugee movements with the Center for Refugee Studies in Toronto.

Agnès has written and been published widely in the fields of human rights, women's rights, refugee movements, and accountability, and holds a PhD in political science from the New School for Social Research in New York.

***Fen Hampson**, Distinguished Fellow and Director of Global Security and Politics Program, CIGI; Co-Director, GCIG; and Chancellor's Professor, Carleton University*

Fen Osler Hampson is a distinguished fellow and director of CIGI's Global Security and Politics Program, overseeing the research direction of the program and related activities. He is also co-director of the Global Commission on Internet Governance. Most recently, he served as director of the Norman Paterson School of International Affairs (NPSIA) and will continue to serve as chancellor's professor at Carleton University in Ottawa, Canada.

Fen holds a PhD from Harvard University, where he also received his AM degree (both with distinction). He also holds an MSc (Econ.) degree (with distinction) from the London School of Economics and a BA (Hon.) from the University of Toronto. A fellow of the Royal Society of Canada, he is the past recipient of various awards and honors, including a Research and Writing Award from the John D. and Catherine T. MacArthur Foundation, and a Jennings Randolph Senior Fellowship from the United States Institute of Peace (a nonpartisan, congressionally funded think tank) in Washington, D.C. He has also taught at Georgetown University as a visiting professor.

Fen is the author or coauthor of 10 books and editor or coeditor of more than 26 other volumes. In addition, he has written more than 100 articles and book chapters on international affairs. His most recent books are *The Global Power of Talk* (coauthored with I. William Zartman),

published in March 2012, and *Brave New Canada: Meeting the Challenge of a Changing World*, coauthored with Derek Burney.

Fen is a frequent commentator and contributor in the national and international media. His articles have appeared in *The Washington Post*, *The Globe and Mail*, *Foreign Policy Magazine*, the *Ottawa Citizen*, *iPolitics*, and elsewhere. He is a frequent commentator on the CBC, CTV, and global news networks.

***Carolina Rossini**, Vice President for International Policy and Strategy, Public Knowledge; GCIG Research Advisory Network Member*

Carolina Rossini is a Brazilian lawyer with 15 years of experience in Internet and intellectual property law and policy. She currently serves as the vice president for international policy and strategy at Public Knowledge. Previously, Carolina was a project director at New America's Open Technology Institute, the international intellectual property director at Electronic Frontiers Foundation (EFF), and a fellow at the Berkman Center at Harvard University. Back in Brazil, she worked at Terra Networks S/A (the ISP of Telefónica Group) and for the Center of Technology and Society (CTS) at FGV Law School. Alongside her work at Public Knowledge, she is a global partners digital international associate and an X-Lab fellow for New America. She sits on the advisory boards of Open Knowledge Foundation for both the United Kingdom and Brazil, Instituto Educadigital, and InternetLab. Carolina has an LLM in Intellectual Property from Boston University, an MBA from Instituto de Empresas–Spain, an MA in International Economic Negotiations from UNICAMP/UNESP, and a JD from University of São Paulo–USP.

***Marietje Schaake**, Member, European Parliament; GCIG Commissioner*

Marietje Schaake has been serving as a member of the European Parliament for the Dutch Democratic Party (D66) with the Alliance of Liberals and Democrats for Europe (ALDE) political group since 2009. Marietje Schaake is her political group's coordinator of the International Trade Committee (INTA) and the spokesperson on the Transatlantic Trade and Investment Partnership (TTIP). Marietje additionally serves on the committee on Foreign Affairs (AFET), where she focuses on strengthening Europe as a global player. She works on the European Union's neighborhood policy, notably on Turkey, Iran, North Africa, and the broader Middle East. In the subcommittee on Human Rights (DROI) she speaks on human rights and coordinates the monthly human rights resolutions for ALDE. Her work has sought to include digital freedoms in E.U. foreign policy.

She is a vice president of the delegation for relations with the United States and a substitute member on the delegation with Iran. Marietje has pushed for completing Europe's digital single market and is strongly committed to an open Internet in discussions about Internet governance and digital (human) rights. Marietje is a member of the European Council on Foreign Relations, a commissioner on the Global Commission on Internet Governance, and a WEF Young Global Leader in the class of 2014. She serves as vice president of the supervisory board of Free Press

Unlimited.

PANEL 3B: TRADE, INTERNET GOVERNANCE, AND CROSS-BORDER DATA FLOWS

***Moderator: Gordon Goldstein**, Managing Director and Head of External Affairs, Silverlake*

Gordon M. Goldstein joined Silver Lake in 2010. He is a managing director with responsibility for global external affairs, including government relations, public policy, strategic communications, and media relations issues for Silver Lake, as well as key public affairs issues for the firm's portfolio companies. In 2012 Mr. Goldstein represented Silver Lake as a member of the United States government and industry delegation to the World Conference on International Telecommunications. Mr. Goldstein previously served as a managing director at Clark & Weinstock, a government relations, corporate communications, and strategy consulting firm.

Mr. Goldstein is a former senior adviser to the Strategic Planning Unit of the Executive Office of the United Nations Secretary General and previously served as codirector of the Council on Foreign Relations Project on the Information Revolution and as codirector of the Brookings Institution Project on Sovereign Wealth Funds and Global Public Investors. Mr. Goldstein is a former Wayland Fellow and visiting lecturer at the Watson Institute for International Studies at Brown University and was a visiting lecturer at the U.S. Defense Intelligence Agency. He is the author of *Lessons In Disaster: McGeorge Bundy and the Path to War in Vietnam*, a study of national security strategy and White House decision making, which was a *Foreign Affairs* bestseller published by Times Books. He has appeared on the ABC, CNN, MSNBC, and BBC television networks and his articles and book review essays have appeared in the *New York Times*, *Washington Post*, *Newsweek*, *Financial Times*, and other publications. Mr. Goldstein is a graduate of Columbia University, where he was an International Fellow and was awarded a BA and MIA as well as the MPhil and PhD degrees in political science and international relations.

***Nick Ashton-Hart**, Executive Director, Internet and Digital Ecosystem Alliance (IDEA)*

Nick is the senior permanent representative connected to the for-profit technology sector to the UN and its member-states, and the international organization's resident in Geneva. He has been an active part of multilateral policy development, starting with the sustainable development agenda for the world's cities (HABITAT 11) in 1992. Nick has been an active part of the Geneva community for 14 years and resident for the past eight.

He came to international policy from a successful private sector career in both the entertainment and ICT sectors, starting in the music industry managing some of the world's most successful and influential artists like the "Godfather of Soul" James Brown, as well as multiplatinum artists Heaven 17. In the tech sector he went from a systems administrator post to CIO/ CTO in five years and has broad, hands-on technology experience from running a small local area network to designing multi-country wide area networks.

Prior to founding IDEA he was Geneva representative of the Computer and Communications Industry Association (CCIA), director at-large and senior director for participation and engagement with the Internet Corporation for Assigned Names and Numbers, Inc. (ICANN) and executive director of the International Music Managers Forum (IMMF), the international nongovernmental organization representing the interests of music managers and their clients.

***Susan Chalmers**, Principal, Chalmers & Associates*

Susan Chalmers is the principal of Chalmers & Associates, an Internet policy consulting firm based in Wellington, New Zealand. She conducts research and analysis on Internet law and policy issues, particularly in the domains of intellectual property, privacy and surveillance, and trade.

Ms. Chalmers is an active member of the Multistakeholder Advisory Group to the Internet Governance Forum at the United Nations. From 2011 to 2013 she served as the policy lead for Internet New Zealand, a charitable, nonpartisan organization whose dual mandate is to (1) administer the .nz ccTLD; and (2) promote the Internet's benefits and uses, and protect its potential. During her time at InternetNZ, Susan worked closely with the local community to develop policy positions on Internet issues, learning how to reconcile technical concerns into public policy discourse and open Internet advocacy.

Ms. Chalmers worked as a sound recording licensing agent at the Old Town School of Folk Music in Chicago. While in law school, she held internships at Lawyers for the Creative Arts, the World Intellectual Property Organization, the United States District Court for the Northern District of Illinois, and the Cook County Circuit Court. Before attending law school and following college, she served as the executive director of the Cape Cod Chamber Music Festival. She holds a Master of Laws from the University of Auckland and a Juris Doctor from Loyola University Chicago, as well as a Bachelor of Music in Piano Performance and a Bachelor of Arts in French and Francophone Studies from the University of Michigan.

***Victoria Espinel**, CEO and President, Business Software Alliance (BSA)*

BSA President and CEO Victoria A. Espinel is a respected authority on the intersection of technology innovation, global markets, and public policy. After a decade of White House service in both Republican and Democratic administrations, she is now the software industry's leading champion, overseeing BSA programs and initiatives in 60 countries through its 10 offices around the world.

Prior to heading BSA, Espinel was nominated by President Barack Obama and unanimously confirmed by the Senate to serve as the first U.S. Intellectual Property Enforcement Coordinator. In that pioneering role, she conceived the first ever government-wide strategy on intellectual property enforcement and implemented it by prioritizing $100 million in resources and the activities of 800 employees across federal agencies.

Espinel also was the first assistant United States trade representative for intellectual property and innovation. As the chief U.S. trade negotiator on these issues, she developed the department's mission, directed ongoing bilateral discussions with more than 60 countries, and led an interagency team in authoring a new chapter on intellectual property that has been used in every U.S. free trade agreement negotiated since 2002.

Between her roles at the Office of the U.S. Trade Representative and White House, Espinel was a professor of international trade and intellectual property at the George Mason School of Law and served as an adviser to congressional committees. Earlier in her career, she was an attorney in private practice focused on global policy issues.

Espinel was appointed by President Obama to serve on the Advisory Committee on Trade Policy and Negotiations (ACTPN), the principal advisory group for the U.S. government on international trade. A frequent keynote speaker at conferences worldwide, she also chairs the World Economic Forum's Global Agenda Council on the Future of IT Software.

Espinel holds an LLM from the London School of Economics, a JD from Georgetown University Law School, and a BS in Foreign Service from Georgetown University's School of Foreign Service.

***Anupam Chander**, Professor, University of California: Davis Law School*

Professor Anupam Chander is the director of the California International Law Center and Martin Luther King, Jr. Hall Research Scholar. His research focuses on the regulation of globalization and digitization. His new book, *The Electronic Silk Road: How the Web Binds the World Together in Commerce*, was released in June 2013 by Yale University Press.

He has been a visiting professor at Yale Law School, the University of Chicago Law School, Stanford Law School, and Cornell Law School. He has published widely in the nation's leading law journals, including the *Yale Law Journal*, the *NYU Law Journal*, the *University of Chicago Law Review*, *Texas Law Review*, and the *California Law Review*.

A graduate of Harvard College and Yale Law School, he clerked for Chief Judge Jon O. Newman of the Second Circuit Court of Appeals and Judge William A. Norris of the Ninth Circuit Court of Appeals. He practiced law in New York and Hong Kong with Cleary, Gottlieb, Steen & Hamilton.

He serves as a judge and commentator at the Harvard-Stanford Junior International Law Faculty Forum. His writing has received honors from the American Association of Law Schools and

been selected for presentation by the Stanford-Yale Junior Faculty Forum.

PANEL 4A: PRIVACY, BIG DATA, AND THE INTERNET

***Moderator: Andrew McLaughlin**, Senior Fellow, SIPA, Columbia University*

Andrew McLaughlin is currently CEO of Digg and Instapaper and a partner at betaworks. From 2009 to 2011, he was a member of Obama's senior White House staff, serving as deputy chief technology officer of the United States, responsible for advising the president on Internet, technology, and innovation policy. Previously, he was director of global public policy at Google, leading the company's work on issues like freedom of expression and censorship, surveillance and law enforcement, privacy, and Internet regulation. McLaughlin has lectured at Stanford Law and Harvard Law, and held fellowships at Stanford's Center for Internet & Society, Princeton's Center for IT Policy, and Harvard's Berkman Center for Internet & Society. He helped launch and manage ICANN, the Internet's technical coordinating organization, and has worked on Internet and telecom law reform projects in a number of developing countries. After clerking on the U.S. Court of Appeals for the 8th Circuit, he started his career as a lawyer in Washington D.C., where he focused on appellate and constitutional litigation.

***Matthew Jones**, James R. Barker Professor of Contemporary Civilization, Department of History, Columbia University*

A historian of science and technology, Matthew L. Jones was a Guggenheim Fellow for 2012–13 and is a Mellon New Directions Fellow for 2012–15. He is currently writing two books: *Great Exploitations: Data Mining, Legal Modernization, and the NSA*, and the first history of data mining from the 1960s to the present. He has previously written *The Good Life in the Scientific Revolution* (Chicago).

***Rebecca MacKinnon**, Director, Ranking Digital Rights Project, New America*

Rebecca MacKinnon is director of the Ranking Digital Rights Project at New America, developing a methodology to rank Internet, telecommunications, and other ICT sector companies on free expression and privacy criteria. A pilot study was conducted in 2014, and an annual index or ranking of companies will be launched in 2015. MacKinnon is also a visiting affiliate at the Annenberg School for Communication's Center for Global Communications Studies and was a 2013 adjunct lecturer at the University of Pennsylvania Law School. Previously a senior research fellow and Bernard L. Schwartz Senior Fellow at New America, MacKinnon is author of *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books, 2012) and cofounder of the citizen media network Global Voices Online. She serves on the board of directors of the Global Network Initiative and the Committee to Protect Journalists.

Fluent in Mandarin Chinese, MacKinnon was CNN's bureau chief and correspondent in China and Japan in the late 1990s and early 2000s. In 2007–08 she taught online journalism and conducted research on Chinese Internet censorship at the University of Hong Kong's Journalism and Media Studies Centre. She has held fellowships at Harvard's Shorenstein Center on the Press and Public Policy, the Berkman Center for Internet and Society, the Open Society Foundations, and Princeton's Center for Information Technology Policy. MacKinnon received her AB magna cum laude from Harvard University and was a Fullbright scholar in Taiwan. She lives in Washington, D.C.

***Nuala O'Connor**, President and CEO, Center for Democracy and Technology*

Nuala O'Connor is the president and CEO of the Center for Democracy and Technology. She is an internationally recognized expert in Internet and technology policy, particularly in the areas of privacy and information governance. Nuala has experience in both the public and private sectors. She was the global privacy leader at General Electric (GE), where she was responsible for privacy policy and practices across GE's numerous divisions. Prior to joining CDT, she worked at Amazon.com as vice president of Compliance & Consumer Trust and associate general counsel for Data and Privacy Protection. Nuala's time in the technology sector began at DoubleClick, where she was part of a team of professionals brought in to address public outcry over the advertising giant's proposal to merge on- and offline data sets. Later, Nuala served as deputy director of the Office of Policy and Strategic Planning, as chief privacy officer, and as the chief counsel for technology at the U.S. Department of Commerce, where she worked on global technology policy including Internet governance and industry best practices. She became the first statutorily appointed chief privacy officer in federal service when she was named as the first chief privacy officer at the Department of Homeland Security.

PANEL 4B: INNOVATION AND THE INTERNET

***Moderator: Merit E. Janow.** Dean, SIPA, Columbia University*

***Brad Burnham**, Managing Partner, Union Square Ventures*

Brad Burnham is a managing partner at Union Square Ventures. He started working in information technology with AT&T in 1979. Brad spun Echo Logic out of Bell Laboratories in 1989 and joined AT&T Ventures in 1993. Brad cofounded TACODA in 2001 before joining Fred Wilson to create Union Square Ventures in 2003. Brad majored in political science at Wesleyan University. He is married with two children and lives in New York City.

***Konstantinos Komaitis**, Senior Policy Advisor, Internet Society; GCIG Research Advisory Network Member*

Konstantinos Komaitis is a senior policy advisor at the Internet Society, focusing primarily on the field of digital content and intellectual property. Before joining the Internet Society in July 2012, he was a senior lecturer at the University of Strathclyde in Glasgow, United Kingdom. Konstantinos holds a PhD in law, and his thesis focused on issues of intellectual property and the Internet, with particular focus on the intersection of trademarks and domain names. Between 2010 and 2012, Konstantinos served as the chair of the Non-Commercial Users Constituency at ICANN and he was a member of ICANN's Special Trademark Issues (STI) team, which drafted the recommendations for the rights protection mechanisms for new gTLDs. He is the author of the book *The Current State of Domain Name Regulation*, and he also serves as a domain name panelist for the Czech Arbitration Court.

***Ronaldo Lemos**, Director, Institute for Technology & Society of Rio de Janeiro; GCIG Research Advisory Network member*

Ronaldo Lemos is an internationally respected Brazilian academic, lawyer, and commentator on intellectual property, technology, and culture. Lemos is the director of the Institute for Technology and Society of Rio de Janeiro (ITSrio.org), and professor at the Rio de Janeiro State University's Law School. He is also a board member of various organizations, including the Mozilla Foundation, Accessnow.org, and Stellar. He was nominated a Young Global Leader by the World Economic Forum in 2015. Lemos was one of the creators of the Marco Civil da Internet, a law enacted in April 2014, creating a comprehensive set of rights for the Internet in Brazil, including freedom of speech, privacy and net neutrality. Lemos' academic qualifications include a Master of Laws degree from Harvard Law School, and a Doctor of Law from University of São Paulo. He is currently a nonresident visiting scholar at the MIT Media Lab and writes weekly for *Folha de São Paulo*, a major newspaper in Brazil.

***Sharad Sanghi**, CEO and Founder, Netmagic Solutions*

Sharad Sanghi is the CEO of Netmagic Solutions, an organization that he founded in July 1998 and now an NTT Communications Company. Sharad is responsible for growing Netmagic to be India's fastest growing datacenter, cloud, and managed services company, with eight datacenters spread across India. Netmagic delivers services to over 1,400 enterprise customers across the globe. Sharad has played an active role in Internet exchanges, both in the early days of the NSFNET in the United States and also more recently in the National Internet Exchange of India. He is also actively involved in the ISP Association of India.

On the business side, Sharad led Netmagic through three successful VC funding rounds with Nexus Venture Partners, Fidelity, Cisco Systems, and Nokia Growth Partners. He led the 2012 acquisition of the company's majority stake by NTT Communication Japan—a first in the Indian datacenter market. Sharad is an industry veteran with over 20 years of extensive experience in developing Internet backbone infrastructure. He is one of few Indians to have worked as a backbone engineer on the NSFNET in the U.S. During a six-year stint in the US, Sharad worked for Unified Network Management Architecture Group at AT&T Bell Labs, the Backbone

Engineering Group of NSFNET (ANS), and the Router Systems Development Group of Advantis (IBM Global Network). Sharad is an electrical engineer from IIT Bombay and holds a master's degree from Columbia University.

DAY TWO: CYBER-SECURITY

OPENING JOINT-KEYNOTE

Moderator: Merit E. Janow, *Dean, SIPA, Columbia University*

Michael Chertoff*, Former Secretary, U.S. Department of Homeland Security; GCIG Commissioner*

As Secretary of the U.S. Department of Homeland Security from 2005 to 2009, Michael Chertoff led the country in blocking would-be terrorists from crossing U.S. borders or implementing their plans if they were already in the country. He also transformed FEMA into an effective organization following Hurricane Katrina. His greatest successes have earned few headlines - because the important news is what didn't happen.

Before heading up the Department of Homeland Security, Mr. Chertoff served as a federal judge on the U.S. Court of Appeals for the Third Circuit. Earlier, during more than a decade as a federal prosecutor, he investigated and prosecuted cases of political corruption, organized crime, corporate fraud, and terrorism - including the investigation of the 9/11 terrorist attacks.

At The Chertoff Group, Mr. Chertoff provided high-level strategic counsel to corporate and government leaders on a broad range of security issues, from risk identification and prevention to preparedness, response, and recovery. In addition to his role at The Chertoff Group, Mr. Chertoff is also senior of counsel at Covington & Burling LLP, and a member of the firm's White Collar Defense and Investigations practice group.

Mr. Chertoff is a magna cum laude graduate of Harvard College (1975) and Harvard Law School (1978). From 1979 to 1980 he served as a clerk to Supreme Court Justice William Brennan Jr.

Kevin Mandia*, Chief Operating Officer and Senior Vice President, FireEye*

Kevin Mandia is SVP and COO of FireEye and the former founder and CEO of cybersecurity and forensics company Mandiant. In 2004, Mandia founded Mandiant to focus on helping organizations detect, respond to, and contain computer intrusions - making Mandiant the first company with incident response as its core competence. He has spent over 20 years in information security, and has been on the front lines helping organizations respond to computer security breaches for nearly 15 years. Mandia holds a BS in Computer Science from Lafayette College and an MS in Forensic Science from The George Washington University. In 2011, he was named Ernst & Young Entrepreneur of the Year for the Greater Washington area.

PLENARY PANEL 5: MITIGATING CYBER-RISKS IN CRITICAL INFRASTRUCTURE: PRIVATE AND PUBLIC RESPONSES FOR THE FINANCIAL SECTOR

***Moderator: Jason Healey**, Senior Research Scholar, Cyber Policy, SIPA, Columbia University*

Jason Healey has recently joined Columbia SIPA as its new senior research scholar in cyber policy. He was formerly the director of the Cyber Statecraft Initiative of the Atlantic Council, focusing on international cooperation, competition, and conflict in cyberspace, and the editor of the first history of conflict in cyberspace, *A Fierce Domain: Cyber Conflict, 1986 to 2012*. He has worked on cyber issues since the 1990s and is the only person to be both a policy director at the White House and a review board member of the DEF CON global hacker conference.

***Steven Bellovin**, Percy K. and Vidal L. W. Hudson Professor of Computer Science, School of Engineering, Columbia University*

Steven M. Bellovin is the Percy K. and Vidal L. W. Hudson Professor of Computer Science at Columbia University, where he does research on networks, security, and especially why the two don't get along, as well as related public policy issues. In his spare professional time, he does some work on the history of cryptography. He joined the faculty in 2005 after many years at Bell Labs and AT&T Labs Research, where he was an AT&T Fellow. He received a BA degree from Columbia University, and an MS and PhD in Computer Science from the University of North Carolina at Chapel Hill. While a graduate student, he helped create Netnews; for this, he and the other perpetrators were given the 1995 Usenix Lifetime Achievement Award (The Flame). Bellovin has served as chief technologist of the Federal Trade Commission. He is a member of the National Academy of Engineering and is serving on the Computer Science and Telecommunications Board of the National Academies, the Department of Homeland Security's Science and Technology Advisory Committee, and the Technical Guidelines Development Committee of the Election Assistance Commission. He has also received the 2007 NIST/ NSA National Computer Systems Security Award and has been elected to the Cybersecurity Hall of Fame.

Bellovin is the coauthor of *Firewalls and Internet Security: Repelling the Wily Hacker* and holds a number of patents on cryptographic and network protocols. He has served on many National Research Council (NRC) study committees, including those on information systems trustworthiness, the privacy implications of authentication technologies, and cybersecurity research needs; he was also a member of the information technology subcommittee of an NRC study group on science versus terrorism. He was a member of the Internet Architecture Board from 1996 to 2002; he was codirector of the Security Area of the IETF from 2002 through 2004.

Paul Bracken*, Professor, Yale School of Management*

Paul Bracken is professor of management and political science at Yale University. He is a leading expert in global competition and the strategic application of technology in business and defense. He is a consultant to private equity funds, accounting, and insurance companies as well as several arms of the U.S. government. Professor Bracken often leads business war games for companies facing complex new problems. He has led games on the future of European asset management, U.S. financial services re-regulation, and strategies of technological competition with China.

A member of the Council on Foreign Relations, he serves on the Chief of Naval Operations Executive Panel. His BS is from Columbia University in engineering and his PhD is from Yale University in operations research. His most recent book is *The Second Nuclear Age: Strategy, Danger, and the New Power Politics* (Henry Holt).

Louis Modano*, Senior Vice President and Global Head of Infrastructure Services, NASDAQ*

Louis Modano is senior vice president and global head of infrastructure services for Nasdaq. In this role, he is responsible for the development and implementation of Nasdaq's global technology infrastructure and services, including networks, systems, storage, databases, cloud computing, office automation, and data center facilities. Mr. Modano and his global team support the underlying infrastructure behind Nasdaq's trading and market systems, as well the market technology and corporate solutions businesses within the global technology group.

Mr. Modano has more than 25 years of experience in building business value through strategic and innovative product development and information technology initiatives within the financial services industry. Prior to joining Nasdaq in August of 2009, Modano served as senior vice president at NYSE Euronext, where he held various senior leadership positions in operations, engineering, business development, sales, and product development, and as head of the Sector/SFTI technology subsidiary. Mr. Modano earned a Master of Business Administration from St. John's University and a Bachelor of Science in Electrical Engineering from

Polytechnic University.

***Elizabeth Petrie**, Director, Strategic Intelligence Analysis, Citigroup Information Protection Directorate*

Elizabeth (Beth) Petrie manages Citi's Strategic Intelligence Analysis Group, which produces actionable intelligence assessments on the cyber threat to inform decisions made by executives on information security practices. Beth joined Citi in January 2014 with more than 15 years of experience as an intelligence analyst. Prior to Citi, Beth was the head of Cyber Intelligence for the Federal Bureau of Investigation. Beth oversaw production of threat analysis for senior policymakers and led development of a threat prioritization methodology, which changed the way the FBI measures intelligence program management. Her career at the FBI also included authoring intelligence assessments on financial crime trends impacting global financial institutions and working as a tactical analyst supporting espionage cases. Beth is a certified intelligence officer, holds a master's degree in technology management from Georgetown University, a master's degree in criminal justice from George Washington University, and a bachelor's degree in psychology from Saint Mary's College, Notre Dame.

PANEL 6A: NUCLEAR VS CYBER: CONFLICT AND DETERRENCE

***Moderator: Austin Long**, Assistant Professor, SIPA, Columbia University*

Austin Long is an assistant professor, teaching security policy. Long previously worked as an associate political scientist for the RAND Corporation, serving in Iraq as an analyst and adviser to the Multinational Force Iraq and the U.S. military. He also worked as a consultant to MIT Lincoln Laboratory on a study of technology and urban operations in counterinsurgency.

Long is the author of *Deterrence—From Cold War to Long War: Lessons from Six Decades of RAND Research* and *On "Other War": Lessons from Five Decades of RAND Counterinsurgency Research*.

Long was cofounder of the Working Group on Insurgency and Irregular Warfare at the MIT Center for International Studies and is a participant in the RAND Counterinsurgency Board of Experts. He has also taught on international security at Clark University.

Long has a BS from the Georgia Institute of Technology and a PhD from the Massachusetts Institute of Technology (MIT).

***Robert Jervis**, Adlai E. Stevenson Professor of International Politics,*

Department of Political Science and SIPA, Columbia University

Robert Jervis is the Adlai E. Stevenson Professor of International Politics at Columbia University. Specializing in international politics in general, and security policy, decision making, and theories of conflict and cooperation in particular, his *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* was published by Cornell University Press in April 2010. Among his earlier books are *American Foreign Policy in a New Era* (Routledge, 2005), *System Effects: Complexity in Political and Social Life* (Princeton, 1997); *The Meaning of the Nuclear Revolution* (Cornell, 1989); *Perception and Misperception in International Politics* (Princeton, 1976); and *The Logic of Images in International Relations* (Columbia, 1989). Jervis also is a coeditor of the *Security Studies Series* published by Cornell University Press. He serves on the board of nine scholarly journals and has authored over 100 publications.

Dr. Jervis is a fellow of the American Association for the Advancement of Science and the American Academy of Arts and Sciences. He has also served as the president of the American Political Science Association. In 1990 he received the Grawemeyer Award for his book *The Meaning of the Nuclear Revolution*.

Professor Jervis earned his BA from Oberlin College in 1962. He received his PhD from the University of California, Berkeley in 1968. From 1968 to 1974 he was appointed an assistant (1968–1972) and associate (1972–1974) professor of government at Harvard University. From 1974 to 1980 he was a professor of political science at the University of California, Los Angeles.

***Herbert Lin**, Senior Research Scholar for Cyber Policy and Security, Center for International Security and Cooperation, Stanford University*

Dr. Herb Lin is senior research scholar for cyber policy and security at the Center for International Security and Cooperation and research fellow at the Hoover Institution, both at Stanford University. His research interests relate broadly to policy-related dimensions of cybersecurity and cyberspace, and he is particularly interested in and knowledgeable about the use of offensive operations in cyberspace, especially as instruments of national policy. In addition to his positions at Stanford University, he is chief scientist, emeritus, for the Computer Science and Telecommunications Board, National Research Council (NRC) of the National Academies, where he served from 1990 through 2014 as study director of major projects on public policy and information technology, and adjunct senior research scholar and senior fellow in cybersecurity (not in residence) at the Saltzman Institute for War and Peace Studies in the School of International and Public Affairs at Columbia University. Prior to his NRC service, he was a professional staff member and staff scientist for the House Armed Services Committee (1986–1990), where his portfolio included defense policy and arms control issues. He received his doctorate in physics from MIT.

***Joseph Nye**, Professor, John F. Kennedy School of Government, Harvard*

University; GCIG Commissioner

Joseph S. Nye Jr. is University Distinguished Service Professor and former dean of the Harvard Kennedy School of Government. He received his bachelor's degree summa cum laude from Princeton University, won a Rhodes Scholarship to Oxford University, and earned a PhD in political science from Harvard. He has served as assistant secretary of defense for international security affairs, chair of the National Intelligence Council, and deputy undersecretary of state for security assistance, science, and technology. His most recent books include *The Powers to Lead*, *The Future of Power*, and *Presidential Leadership and the Creation of the American Era*. He is a fellow of the American Academy of Arts and Sciences, the British Academy, and the American Academy of Diplomacy. In a recent survey of international relations scholars, he was ranked as the most influential scholar on American foreign policy, and in 2011, *Foreign Policy* named him one of the top 100 Global Thinkers. In 2014, Japan awarded him the Order of the Rising Sun.

PANEL 6B: CYBER-SECURITY AND THE INTERNET OF THINGS

***Moderator: Henning Schulzrinne**, Levi Professor of Computer Science, School of Engineering, Columbia University*

Henning Schulzrinne, Levi Professor of Computer Science at Columbia University, received his PhD from the University of Massachusetts in Amherst, Massachusetts. He was an MTS at AT&T Bell Laboratories and an associate department head at GMD-Fokus (Berlin) before joining the computer science and electrical engineering departments at Columbia University. He served as chair of the Department of Computer Science from 2004 to 2009; as engineering fellow at the U.S. Federal Communications Commission (FCC) in 2010 and 2011; and as chief technology officer at the FCC from 2012 to 2014, subsequently continuing in an advisory capacity.

Schulzrinne has published more than 250 journal and conference papers, and more than 70 Internet RFCs. Protocols codeveloped by him, such as RTP, RTSP, and SIP, are now Internet standards, used by almost all Internet telephony and multimedia applications. His research interests include Internet multimedia systems, ubiquitous computing, and mobile systems.

He has received the New York City Mayor's Award for Excellence in Science and Technology, the VON Pioneer Award, TCCC service award, IEEE Region 1 William Terry Award for Lifetime Distinguished Service to IEEE, and the UMass Computer Science Outstanding Alumni

recognition. He is a fellow of the ACM and IEEE and a member of the Internet Hall of Fame.

***James Kaplan**, Partner, McKinsey and Company*

James M. Kaplan is a partner at McKinsey and Company in New York. He convenes McKinsey's global practices in IT infrastructure and cyber security. He has assisted leading institutions in implementing cyber-security strategies, conducting cyber-war games, optimizing enterprise infrastructure environments, and exploiting cloud technologies. James led McKinsey's collaboration with the World Economic Forum on "Risk and Responsibility in a Hyper-Connected World," which was presented at the Forum's recent Annual Meeting in Davos. He has published on a variety of technology topics in the *McKinsey Quarterly*, the *Financial Times*, the *Wall Street Journal*, and the *Harvard Business Review Blog Network*.

***Rima Qureshi**, Senior VP, Chief Strategy Officer and Head of Mergers and Acquisitions, Ericsson*

As Chief Strategy Officer, Rima Qureshi is based in Canada and Sweden. She is responsible for the company's overall strategy, for driving the Mergers and Acquisitions strategy and activities, as well as serving as chairman of Business Unit Modems.

Qureshi joined Ericsson in 1993, and her experience spans leadership roles in R&D, sales, and services. She has led improvement programs for a major customer in North America and managed Global Service Delivery Centers in Montréal, Canada; Dallas, San Diego and New York City in the U.S.; and Mexico City in Mexico; and São Paolo in Brazil. During 2013, Qureshi led strategic projects for Ericsson globally.

Along with all other members of the executive leadership team, Qureshi reports to president and CEO Hans Vestberg. In her previous role, Qureshi and her leadership team have successfully completed the integration of the CDMA and LTE assets of the former Nortel Networks Corporation in North America and of other subsequent acquisitions.

Qureshi was appointed to the Board of Directors of MasterCard Worldwide in April 2011, based on her broad international experience and business acumen. In April 2014, she was appointed a new member of Wolters Kluwer Supervisory Board, a global leader in professional information services.

Supporting the belief that mobile broadband can bridge economic divides and help those in need, Qureshi also heads up the Ericsson Response program. Ericsson Response is an employee volunteer organization that provides technological and consulting expertise to humanitarian relief efforts, working with partners including various UN agencies.

Qureshi holds a bachelor's degree in Information Systems and an MBA, both from McGill University in Montréal, Canada.

***Tobby Simon**, Founder and President, Synergia Foundation; GCIG Commissioner*

Tobby Simon is the founder and president of Synergia Foundation, a strategic think tank that works closely with academia and industry to develop cutting-edge practices and solutions through applied research in the domains of geopolitics and geosecurity. He is also the president and founder of the Synergia Group, a business advisory and incubation company that works in the area of translational research.

Tobby has over 30 years of multidisciplinary expertise in healthcare, cyber security, aerospace, energy, supply chain risk management, and strategic consulting. His success in the industry won him accolades, including the National Certificate of Merit for Exports from the Government of India in 1992. At the young age of 29, Tobby became the president of a French pharmaceutical conglomerate, CSP, heading its operation in Asia. Over the next eight years, Tobby worked pro bono for Nobel Prize winner Médecins Sans Frontières (MSF) and the WHO to build end-to-end supply chains for antiretroviral, anti tuberculosis, and antimalarial drugs from India. This project is currently helping millions of afflicted patients all over the world. He was closely involved with several humanitarian missions in Peru, South Africa, Afghanistan, Sri Lanka, CIS, and India. He has also been an advisor to EU-AEDES, The Croix Rouge, Pharmaciens Sans Frontières and the World Congress on Information and Communication Technology. While rendering pro bono work for humanitarian organizations, he advised and helped a number of global companies in telecommunication, power, pharmaceuticals, aerospace, etc., successfully establish their business in South Asia.

Tobby has been instrumental in building research collaborations with some of the finest academic institutes including Harvard-MIT Division of Health Sciences and Technology, Cambridge University, The Indian Institute of Management Bangalore, and the Indian Institute of Technology Kanpur.

Tobby is very active on a number of international bodies. He was recently nominated as commissioner to the Global Commission on Internet Governance headed by the Swedish Foreign Minister Carl Bildt. Tobby serves on the advisory board of the Center for a New American Security (CNAS), a bipartisan think tank that works closely with key policy makers in the United States. He was also a member of the International Council of the Belfer Center for Science and International Affairs (BCSIA).