COLUMBIA | SIPA
School of International and Public Affairs

Proceedings of the

Global Digital Futures Policy Forum 2016 Data Governance

Italian Academy
Columbia University, New York City
April 25, 2016

School of International and Public Affairs (SIPA), Columbia University

Proceedings of the

Global Digital Futures Policy Forum 2016
Data Governance

Italian Academy, Columbia University Campus
April 25, 2016

Table of Contents

Letter from the Dean

This document is a summary of the proceedings for the ***Global Digital Futures Policy Forum 2016***, convened by Columbia University's School of International and Public Affairs (SIPA) on April 25, 2016.

SIPA's **Global Digital Futures Policy Forum** is envisioned as a long-term intellectual initiative to reimagine our digital future, focus on the potential benefits and costs arising from global digital technology changes, and, importantly, anticipate public policy solutions to emerging problems that will shape the future of society and the economy for generations to come.

The 2016 forum considered both domestic and international dimensions of *data governance* in the context of technological change and globalization. Data flows are now central to economic activity within and across borders. This forum focused on major policy issues associated with this fundamental feature of modern life.

Over one day, a series of keynote lectures and panel discussions with leading academics, influential policy makers, entrepreneurs, legal experts, technologists, and corporate executives from around the world explored the most significant policy questions related to our digital future. Several issue briefs for each session are appended hereto.

SIPA was pleased to convene this forum as part of our **Tech & Policy @ SIPA Initiative**. This initiative includes a technology-focused curriculum for our graduate students; academic research on internet governance, cybersecurity and the digital economy; challenge grants to support applied solutions to global urban problems; high-profile events; interdisciplinary collaborations; and a start-up lab for student technology 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. Data and digital technologies are transforming all of the policy areas we study and engage at SIPA. We hope this summary will reveal the complexities and opportunities of this period.

We wish to thank Carnegie Corporation of New York, Microsoft Corporation, and the Columbia Institute for Tele-Information for their generous support for and involvement in this year's forum; and The Internet Society, for its assistance with the live streaming of this event.

Merit E. Janow

Merit E. Janow

Dean, School of International and Public Affairs

Professor of Practice in International Economic Law and International Affairs

Executive Summary

CONFERENCE OVERVIEW

On April 25, 2016, SIPA convened a major forum to examine critical issues associated with domestic and international dimensions of data governance in the context of technological change and globalization.

The goal of this event was to stimulate thought; identify key issues around digital technology and policy, with a special focus on global data governance; develop concrete recommendations and actions; and ultimately drive progress in the global public interest.

This forum occurred at a time when policymakers are facing pressing technology-related issues, including global security challenges surrounding digital intelligence and encryption; data governance; algorithmic decision-making; cyber conflict; preserving individuals' rights; the transformation of economic sectors; open data, engagement, and urban governance.

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

What follows is an executive summary of the major themes that emerged at the forum. The proceedings are arranged session-by-session with the key questions and insights from each discussion. A set of issues briefs, prepared by thought leaders, is provided, followed by the full agenda and speaker bios. Videos of session are available on the conference website: sipa.columbia.edu/experience-sipa/events/conferences/global-digital futures-policy-forum-2016.

The opening morning of the Global Digital Futures Policy Forum

CONFERENCE TOPICS

The span of topics discussed at the Global Digital Futures Policy Forum 2016 was both expansive and multidisciplinary.

Table 1. Panels and respective topics

Morning	Opening keynote discussion: How Digital Technologies & Data are Changing our World
	Panel 1: Global Security Challenges and Data: Intelligence Gathering, Encryption, and Sharing in a Time of ISIS
	Panel 2: National Data Governance in a Global Economy
Afternoon	Lunch keynote discussion: The Future of Digital Technologies for International Affairs
	Panel 3A: Potential and Pitfalls of an Algorithmic Society
	Panel 3B: Cyber Conflict: Prevention, Stability and Control
	Panel 4A: Massive Data Collection and Automation: Preserving Individuals' Rights
	Panel 4B: On Notice: The Coming Transformation of Key Economic Sectors
	Panel 5: Civic Entrepreneurs: Global Perspectives on Open Data, Engagement and Urban Governance

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

MAJOR THEMES ACROSS THE FORUM

Several unifying topics and questions emerged over the course of the discussions: the varied consequences of continuing digitalization; the need to reconfigure or update mechanisms to ensure data privacy, anonymity, reliability, and quality; the challenge of creating effective, global governance systems; strains in legal and regulatory systems' ability to respond to technological change and its consequences; and different models or approaches to update governance, legal and policy frameworks, both internationally and nationally.

The varied consequences of continuing digitalization globally

It is clear that the continued spread and adoption of digital technologies is changing our world. What is less clear, and being discovered bit-by-bit, is how these consequences manifest themselves globally and how they differ nationally.

Two broad frameworks for understanding these changes were raised during the forum. Professor Usman Ahmed characterized the changes as longitudinal and vertical. Longitudinally, the internet has impacted nearly every sector of the economy. Vertically, the smaller players, the individuals, the developers, the app developers, and the small businesses, are also benefiting tremendously from this revolution. By contrast, Professor Eli Noam characterized the changes as a kind of trickle-down Moore's Law. As the cost of computation and data storage have fallen, so too the adoption and impact of digital technologies have expanded from what might be considered the 'high-tech' sector into more traditional industries.

These changes have brought with them new industries and trade opportunities, and have cut operating costs in a number of industries. At the same time, there is evidence that the benefits from these changes may not be evenly distributed nationally or internationally. Ambassador Daniel Sepulveda felt that potentially the worst outcome that could come from the development and deployment of the information society would be if it leads to greater inequality. He suggested that there is a moral, social, foreign, economic policy, and democratic responsibility to ensure that we use the forces of the market, public policy and public private partnerships to enable widespread benefits from connectivity around the world.

New measures needed for data privacy, anonymity, reliability, and quality

A recurring message throughout the forum was that measures previously introduced to ensure data privacy, anonymity, reliability and quality are no longer as effective as they once were. More concerning, policy makers do not appear to be aware of this change and what might be done to update mechanisms for the digital age.

As explained during the opening keynote discussion, in the '70s and '80s, various techniques, partnerships, institutions and governance mechanisms were introduced to ensure reliable and quality data collection and analysis that respects the privacy and anonymity of the subjects. The challenge now with 'Big Data' comes from the sheer scale of the data available and the integral role that the private sector plays as a collector, owner and controller of datasets. It is very clear that today these techniques, partnerships, institutions and governance mechanisms need to be updated to function properly in an era of Big Data.

Since the '90s, many governments around the world have adopted policies toward open data. Computerized data analysis and release of large datasets requires effective anonymization of data. Many of these methods have become obsolete. Privacy is the major cost. Effective policy responses have not emerged to address these shortcomings.

There is increasing use of algorithms in sectors such as healthcare or for making decisions around employment. The common (mis)conception is that the use of these tools will remove human bias from decision-making and thus lead to better outcomes. However, statistical learning systems and algorithmic decision-making are not perfect. When they are wrong, they often make mistakes that no human would ever make. Not mistaking correlation for causation is a major issue. Again, there is a dearth of public policy attention in this area and thus a lack of effective policy responses implemented or in the pipeline.

The challenge of creating effective, global governance systems

The increasingly global distribution and adoption of digital technologies brings with it challenges on a similarly global scale. Yet the governance mechanisms and institutions set up to manage such global challenges are not keeping pace. Of the examples brought up throughout the forum, overall participants were sanguine as to the practicality of creating and implementing new global governance systems to respond to these challenges. The common reason for this pessimism lies in the difficulty in achieving global consensus amongst so many different parties with such divergent interests.

In one example, it was thought that a multilateral convention to govern the flow of data would be helpful to manage the emerging issues associated with cross-border data flows. However, the prospects of such an arrangement were thought to be unlikely to occur in practice. The difficulty seen in generating a global consensus on the issues related are thought to be similar to those that impede effective global internet governance.

Another example lies in the potential establishment of agreed upon norms for cyber conflict internationally. It was thought that a Congress of Vienna-like arrangement would be needed, however, the prospects of success for such an arrangement are thought to be declining. There are twenty countries that have militaries with cyber-units now. An ever-increasing number of non-state entities are either developing or gaining access to cyber capabilities. This proliferation is making it more and more difficult to engage all necessary parties, much less establish consensus.

Strains showing in national legal and regulatory systems

Strains are showing in the ability of national legal and regulatory systems to manage the consequences of various waves of technological change. These strains can be seen in a number of domains.

The legal framework for allowing intelligence agencies to assist law enforcement in digital technology-related crimes is defective, or in the case of some nations missing altogether. The international legal frameworks that govern data flows are not harmonized, and if anything, are further fragmenting. Faced with new algorithmic decision-making processes, the limits of discrimination law are being tested. Use of the concept of disparate impact is thought to be one avenue in the United States but is untested as of yet. The numerous ways in which data are analyzed or sold mean that the average user does not really know what will or might be done with the personal data they ‘consent’ to share or provide. The idea of informed consent, in such a situation, becomes hard to apply.

There is a need to revise and update national legal and regulatory systems to cope with these technological changes.

Many possible approaches to update laws, regulations and governance systems

The task of finding workable international governance frameworks and ways to update national legal and regulatory frameworks is daunting for policymakers. A variety of different models were proposed across the numerous domains covered by the panels.

In the area of intelligence agency/law enforcement access to encrypted data, it was thought that striking a balance between the diverging interests will require a satisfactory public policy solution. Optimization between public security and private security (or privacy) was not thought to be compatible in practice.

For protecting individual's data privacy, instead of thinking about having a one-size-fits-all solution, such as people giving their consent to activities many might not understand in practice, policymakers might consider a multi-pronged, more local approach that involves outreach or targeting different communities. Such an approach would allow for more customized or targeted policies depending on the relative risk that a certain community or stakeholder faces.

Ride-sharing, autonomous vehicles (or the Internet of Things) and cryptocurrencies are challenging the limits of existing regulatory and legal regimes. The commonly advocated approach, particularly by certain interest groups, has been to look to ways to create new, separate regulatory regimes to govern the activities linked to these technological changes. Panelists thought that the risk of rent seeking or regulatory capture in such proposals could be avoided by making adjustments to the existing regimes rather than establishing separate regulatory regimes.

Opening Keynote: How Digital Technology and Data are Changing our World

Moderator: Merit E. Janow, Dean, Columbia SIPA

Arati Prabhakar, Director, Defense Advanced Research Projects Agency

Kenneth Prewitt, Professor and Special Advisor to the President, Columbia University

Key questions:

How will advances linked to data creation, computationally intensive practices (e.g. artificial intelligence and automation), and the transition from a network that primarily comprises person-to-person connections to one that comprises object-to-object connections, affect highly regulated fields, where public policy mediates a variety of social, political, ethical, and economic interests, including public health, medicine (precision medicine, genomics), the automotive industry, and beyond?

- What are the major technological changes occurring as a result of data and analytics?
- What applications is DARPA driving? Where are the great opportunities?
- What are the emerging problem areas?

Keynote speakers during the opening session (from left to right): Kenneth Prewitt, Arati Prabhakar, and Merit E. Janow

Key observations:

- The tools of data, big data, and data analytics are being used in ever more numerous areas. A convergence of technologies is also occurring, e.g. machine learning and a new wave of statistical learning being utilized through artificial intelligence. As these tools are adopted and converge, there will be profound public policy consequences that we are only just grappling with.
- Statistical learning systems, while advancing rapidly, are still far from perfect. When they are wrong, they make mistakes that no human would ever make. Not mistaking correlation for causation is still a major issue.
- As the second half of the world's population gains access to the internet over the coming decade(s), questions around internet governance will be important. Will their access be like in China and Iran or like the relatively open-access that is enjoyed in the U.S.? Will it be mediated through a private provider?
- The Big Data revolution presently occurring in the social sciences is the latest in a long series of methodological and technological advances. The first major phase of change came in the 1930s with sampling theory. This phase was "theory rich but data poor." The next phase came in the 1970s or 80s, when strong partnerships were forged between the social and the physical sciences such as in human engineering, public health, or the human dimensions of sustainable development. The latest 'Big Data' phase is notable for the sheer scale of the data available but also for the integral role that the private sector plays as a collector, owner and controller of datasets.
- Various techniques, partnerships, institutions and governance mechanisms were introduced in response to previous changes to ensure reliable and quality data collection and analysis that respects the privacy and anonymity of the subjects. We are still grappling with how to update these tools in an era of Big Data.
- A challenge is seen in creating the same kind of set of arrangements that over the last 40 or 50 years were perfected between the academic sciences and the government with the new third actor: the private sector. The challenge is compounded by the private sector's incentives to maintain confidentiality, non-transparency, and intellectual property protections over data.
- The Internet of Things brings with it major security issues, particularly the potential explosion of the attack surface. These new, connected devices need to be built in a much more secure way from the bottom-up. Given that there has been systematic underinvestment in device security up until the present, public policy may have a role in providing this incentive.

Panel 1: Global Security Challenges and Data: Intelligence Gathering, Encryption, and Sharing in a World of ISIS

Moderator: Laura DeNardis, Professor, American University

Steven Bellovin, Professor, Dept. of Computer Science, School of Engineering, Columbia University

Alan Butler, Senior Counsel, Electronic Privacy Information Center

David Omand, Visiting Professor, King's College London

Key questions:

The Islamic State and other extremist groups use information and communication technologies to recruit, fundraise, and spread their messages of hate. States, and occasionally non-states, have a range of policy and technology tools to counter these online threats, but how far can policy makers push in this area without fundamentally eroding human rights and privacy, undermining democracy, or weakening these technologies to the point where they can no longer be engines of innovation and economic growth?

- How can information sharing arrangements between governments and firms, and between governments be improved to permit necessary intelligence gathering and sharing across jurisdictions? What is the role for citizen oversight/courts?

- Given differences in privacy laws within the EU—and between the US and the EU and other jurisdictions— what legal or policy mechanisms need to be created or adjusted (e.g. MLATs)?

- How should we think about content regulation and oversight in the age of terrorist attacks and online recruitment?

- How do we strike the right balance in the tensions that arise vis-à-vis human rights, commerce, security, and other important societal needs?

Panelists (from left to right): Laura DeNardis, David Omand, Alan Butler, and Steve Bellovin

Key observations:

- This discussion explored the intersection of national security, intelligence gathering, new digital technologies and massive digital data stores.
- Trust is a vital component in regard to three types of relationships: 1) Trust between consumers and the corporations that either produce devices or store personal data; 2) Trust in the ability of government authorities to uphold the law in cyber space; and 3) Trust between corporations and the government authorities that request data to aid in investigations or national security-related responsibilities.
- All panelists framed this not as a security vs. privacy situation, but rather as a security vs. security situation: “The security of people and persons and the security for our data and our personal information.”
- On the one hand, there is a need to provide security from criminals, terrorists and other malicious actors. In a situation where law enforcement is increasingly unable to access data held on devices, these law enforcement agencies have turned to intelligence agencies for assistance. What has been shown over the last few years is that the legal framework for such activity is defective or, in the case of some nations overseas, missing altogether.
- On the other hand, the threats to individual data go beyond just traditional national security threats. They include threats to the integrity and confidentiality of individual data as well as threats to individuals and governments through the use of not only physical force but also the

collection and exposure of sensitive records. There is a need to preserve individual rights, individual and national sovereignty, and the protections that are inherent in the data.

- Striking a balance between these interests will require a satisfactory public policy solution. Optimization between one or the other will not be compatible.
- The legal mechanisms to provide protection in this area include: protections of rights, protections of sovereignty and protections of data. These protections are in a state of flux as laws change or differ and court cases come to different conclusions across jurisdictions.
- The *Riley* case in the United States is a particular example of how new technologies and the vastly greater access to data that these technologies provide are challenging traditional legal frameworks.
- The legal definition and treatment of metadata is in flux. For instance, the British Parliament is currently examining this in its legislation [the Investigatory Powers Bill].

Panel 2: National Data Governance in a Global Economy

Moderator: Merit E. Janow, Dean, Columbia SIPA

Usman Ahmed, Adjunct Professor of Law, Georgetown Law

Anupam Chander, Professor, UC Davis Law School

Gordon Goldstein, Managing Director, Silverlake Partners

Mark Wu, Assistant Professor, Harvard Law School

Key questions:

The global digital economy is reliant on the exchange of data across borders. Many nations are presently asserting their sovereignty over information technologies and data. The policy decisions made now will bring with them a host of issues over the coming decade that will affect how companies operate, seen in their storage of and exchange of data, and, as a consequence, world trade and the growth of the global (digital) economy at large.

- How is the trend toward greater imposition of "data sovereignty" manifesting itself (e.g. data localization and residency, rejection of "safe harbor")?

- Is data localization another form of protectionism, industrial policy, or privacy protection? How is one to determine? What is the balance to be struck?

- How best to consider sovereignty and international trade concerns in a global economy?

Panelists (from left to right): Mark Wu, Gordon Goldstein, Merit E. Janow, Usman Ahmed, and Anupam Chander

Key observations:

- The internet has affected the economy longitudinally and vertically. Longitudinally, the internet has impacted nearly every sector of the economy. Vertically, the smaller players, the individuals, the developers, the app developers, and the small businesses are also benefiting tremendously from this revolution.
- These technological, economic and organizational changes depend upon global data flows.
- However, the international legal frameworks that govern these data flows are not harmonized. There are three different layers of legal mechanisms: the national layer, an international layer (traditional state-led national sovereign agreements and bilateral agreements), and a layer of evolving rules and standards between corporations and service providers.
- In addition to an increasingly fragmented system of regulatory oversight, there is increasingly a fragmentation of the internet itself. This fragmentation has been characterized by Professor Chander as, “different modalities of ‘data localization’ or ‘data nationalism’.”
- This process is being driven by governments’ desire to control what the information landscape within the country looks like, fears of threats or violence that governments claim they are trying to manage, concerns about foreign surveillance, and a desire to stimulate local economic development by pushing out foreign service providers.
- In terms of solutions to keep an open, global internet, speakers proposed: surveillance reform, streamlining of cross-border access to data for governments (e.g. reform of the MLAT process), and dispute resolution mechanisms so that individuals can make claims across borders and resolve issues.
- It is thought that a multilateral convention to govern the flow of data is needed but unlikely to occur in practice. The difficulty seen in generating a global consensus on the issues related to internet governance are instructive in this case.

Lunch Keynote: The Future of Digital Technologies for International Affairs

Moderator: Laura DeNardis, Professor, American University

Dian Triansyah Djani, Permanent Representative of the
Republic of Indonesia to the United Nations

Daniel Sepulveda, Deputy Assistant Secretary,
Bureau of Economic and Business Affairs, U.S. Department of State

Key questions:

The world economy and relationships between states have changed over the past decade due to the rapid adoption of digital technological changes worldwide. In turn, diplomats and foreign services have had to adapt their methods and capabilities in new and creative ways.

Additionally, changes have been triggered in other governmental organizations. At a high level, discussions around governance of the internet have engaged traditionally diplomatic organizations like the United Nations. At the same time, at a domestic level, economic development and aid communities have turned their attention to the role that digital technologies might play in continued development.

- What will be the future implications of the continued adoption and spread of digital technologies for international affairs, broadly speaking?

- What role might the United Nations and its member states play in various aspects of governance of the internet going forward?

- What will be the importance of the UN Sustainable Development Goals in steering the digital development agenda over the coming decade?

Panelists (from left to right): Laura DeNardis, Daniel Sepulveda, and Dian Triansyah Djani

Key observations:

- As we move forward, we need to ensure that the internet and the global communications platform remain and continue to act as a force for not just economic development, but for increasing opportunity in every form.

- Potentially the worst outcome that could come from the development and deployment of the information society is if it leads to greater inequality. There is a moral, social, foreign, economic policy, and democratic responsibility to ensure that we use the forces of the market and public private partnerships to enable connectivity around the world.

- There has been a changing *modus operandi* with international relations in the context of diplomacy and the internet. These changes can be thought of using Nicholson's framework in his book "Diplomacy" with diplomacy being a question of reporting, promotion and then negotiating and protecting citizens. All of these elements have been changed in some way by digital technologies.

- The key internet governance questions that require answers include: do we want to govern the internet, when we do want to govern the internet, who shall govern it, and where shall we govern it?

Panel 3A: The Potential and Pitfalls of an Algorithmic Society

Moderator: David Madigan, Executive Vice President and Dean of Faculty of Arts and Sciences, Columbia University

Solon Boracas, Postdoctoral Research Associate, Center for Information Technology Policy, Princeton University

Roxana Geambasu, Assistant Professor, Dept. of Computer Science, School of Engineering and Data Sciences Institute, Columbia University

Bernard Harcourt, Professor, Columbia Law School

Frank Pasquale, Professor, University of Maryland

Key questions:

Public and private sector organizations, including content intermediaries, are increasingly using algorithms and automation in decision making. Insurance, trading, medicine, policing, and marketing are all undergoing changes due to the adoption of these practices. Increasing automation may have the counterintuitive effect of reducing human autonomy, though, as decisions are made in ways that are beyond the control or understanding of many individuals. The evidence base on which to make policy decisions surrounding these practices and their consequences remains limited.

- What are the consequences and subsequent public policy challenges associated with uses of algorithmic and automated decision making in the public and private sectors?

- In the absence of a robust evidence base, how can policy makers ensure the use of algorithms adheres to societal norms? How might this evidence base be put together?

- How should we consider liability issues and who is responsible for accountability over algorithmically determined or automated decisions?

Panelists (from left to right): Roxana Geambasu, Solon Barocas, Frank Pasquale, Bernard Harcourt, and David Madigan

Key observations:

- There is increasing use of algorithms in sectors (e.g. healthcare) and for making decisions (e.g. employment). The common (mis)conception is that the use of these tools will remove human bias from decision making and thus lead to 'better' outcomes.

- It is important to understand that there are potentially different epistemologies for (algorithmic) decision making. There is the traditional, scientific, peer-reviewed epistemology, which can be contrasted with a different kind of approach to commercially motivated use of data analytics and algorithms modeled on the Amazon and Google methods.

- A divide in the community has arisen. On one side are those who handle big data (e.g. statisticians, epidemiologists) who are pushing for more clear, standardized guidelines or standards of care nationally and internationally. On the other side are professionals who push back and say, "We need judgment."

- The validity of the training data when using machine learning techniques is important to establish in order to avoid potential discrimination from algorithmic decision making. In the area of employment, historical patterns and large data sets are used to train machine learning methods so as to guide decision making. While someone is not actually hand-coding in their particular preference for men over women, the datasets used can embody historically biased notions of which candidates are better than others. Data do not always represent an objective fact of the world but rather the imprint of historical discrimination in the records we use to train.

- Discrimination law might have some avenues to counteract potential discrimination. Disparate impact might offer the best hope. The plaintiff would have to show that there was an alternative way of achieving the same outcome that had a less severe disparity. In other words, could the employer try to find the best candidates for the job with a different method that results in a different allocation of those opportunities to people that belong to certain groups. If it can be shown that such an alternative exists, then there may be the obligation for the employer to adopt that method. In fact, they may bear some legal liability.

- Some additional policy solutions include imposing a fiduciary duty on organizations that use certain algorithmic decision making processes in a way that is deemed to be in contravention of discrimination law, or a kind of bill to mandate open access over the algorithms where everybody gets to see how or why the algorithm is proposing which course of action (“opening the black box”).

- Technical tools are being developed to understand the implications of using personal information and algorithms. External tools can reveal, from the outside, how personal data is being used and for what purposes. In addition, internal tools can reveal to programmers the implications of the use of a user's personal information on the user population.

Panel 3B: Cyber Conflict: Prevention, Stability and Control

Moderator: Jay Healey, Senior Research Scholar, Columbia SIPA

Fred Kaplan, Columnist, Slate

Angela McKay, Director of Cyber Security Strategy, Microsoft

Key questions:

Global cyber conflict continues to worsen year after year, even as the world is becoming incredibly and irreversibly reliant on digital systems and data. Yet in 2015 the major cyber powers agreed on a number of measures to reduce the risk of cyber conflict, most notably on agreements on norms about cyber espionage and targeting in warfare. The future is filled with uncertainty in this area: cyber conflict may continue to escalate and, with it, undermine the benefits that the digital revolution might bring. Or nations might find ways to resolve their competing interests at an international level and develop new instruments for managing conflict.

- What progress has been made in norms, confidence-building measures, and crisis management (e.g. treaties, norms, domestic and international sanctions)? What are the emerging norms in light of US-China, China–UK, G20, and other developments?

- What are the critical gaps that have to be addressed (either between private enterprises and government or between governments) to minimize the risks of cyber conflict? What might public policy do to fill these gaps?

- What role is there for non-state actors to contribute to crisis stability and control dangerous escalation?

Panelists (from left to right): Angela McKay, Jason Healey, and Fred Kaplan

Key observations:

- The security problems with the internet are not new. After three decades, whole systems and networks have grown up with few provisions for security. What is new is the level of conflict escalation between countries as the adoption of these insecure technologies has increased globally. There is a general escalation of cyber attacks worldwide, moving primarily from financially motivated into greater nation/state activity.

- An issue with norms in cyber conflict is that there is no clear point at which it is agreed that a state or entity has 'crossed the line'. The conundrum lies in the need to disclose capabilities so as to use them as a deterrent (thereby establishing what indeed is stepping over the line). Even the extent to which cyber capabilities should be disclosed is an area of debate. Only very recently have the United States and other nations decided to reveal these capabilities. Norms in this area are thus in a state of flux.

- As escalation has occurred, there has been a concomitant need to both improve defenses and limit conflict and to help policymakers understand not only the immediate consequences, but also the implicit consequences seen in eroded trust, internet fragmentation, data sovereignty, and other areas.

- The ability to establish agreed upon norms internationally is thought to be declining. There are twenty countries that have militaries with cyber units now. An ever-increasing number of non-state entities are either developing or gaining access to cyber capabilities. This proliferation is making it more difficult to engage all necessary parties, much less establish consensus.

- There are disincentives for countries to agree on norms. The process of establishing norms will require countries to compromise on capabilities that they do not necessary wish to give up. Each country will have a different set of capabilities that they wish to retain, leaving little ground for broad-based consensus. This doesn’t mean that a process on establishing norms shouldn’t start, as for example has been the case over the past year with various agreements to curtail economic espionage. It is just that our expectations shouldn’t be too high in terms of the scope of norms that can be established.

- A combination of measures will ultimately need to be taken in the ecosystem: Technical measures like reducing the number and severity of vulnerabilities. Operational measures to clean the environment. Strategic measures like some regulation of cyber security in some markets that don't have natural market drivers to improve security to the level of the attacks that they are facing. At some point, policy measures, like norms, will also be needed, though norms alone will not act as a panacea.

- If norms are going to be effective, they would have to be like a Congress of Vienna, where the big powers discuss what can and can’t be done. An issue that then arises is what happens if a country breaks the rules? Who will administer the punishment and what should the punishment be? Answers to these questions are not yet clear.

Panel 4A: Massive Data Collection and Automation: Preserving Individuals' Rights

Moderator: Anya Schiffrin, Lecturer, Columbia SIPA
Joseph Cannataci, UN Special Rapporteur for Privacy
Ashkan Soltani, former Chief Technologist, Federal Trade Commission
Alexis Wichowski, Adjunct Professor, Columbia SIPA

Key questions:

The collection, aggregation, and sharing of data are at the heart of intelligence gathering practices, online advertising, and the distributed Internet of Things networks of sensors. Cultural practices are changing, and new concerns are emerging due to this ubiquitous capture and sharing of everyday information.

Public policy will be called on to protect or preserve previously established individuals' rights in a context where the sheer quantity of personal and behavioral data and the uses of these data exceed most people's comprehension.

- How can public policy best protect individual civil liberties while also enabling digital data collection and analysis, and the benefits that it brings at a national and global level?

- Is there a possibility for people to assert their ownership rights over their data within this context? Is this desirable? Are there "standards" that can be introduced, and, if so, by what type of entities?

- Can corporations design private voluntary mechanisms and can such mechanisms contribute positively?

Panelists (from left to right): Alexis Wichowski, Anya Schiffrin, Joseph Cannataci, and Ashkan Soltani

Key observations:

- In the 1970s and 1980s, computerized data analysis of large datasets brought with it discussions about anonymization of data. Since the 90s, many governments around the world have adopted policies toward open data. When Big Data and open data are brought together, a lot of the old anonymization techniques no longer work. Privacy is the major cost. A rethink is required, if not about Big Data, certainly about open data, because the benefits from open data have to be weighed against the losses to privacy.

- Most of the policy with regards to the governance of information, particularly sensitive private information, in the U.S. at least, is based on a consent model where consumers can opt-in or choose to share particular types of information, or they can choose to opt-out. This model does not seem to be as applicable now as it might have been in the past. The sheer amount of data being collected, and the numerous ways in which data are analyzed or sold, mean that the average user does not really know what will or might be done with the personal data they ‘consent’ to share or provide.

- This is the challenge with privacy harms in general. They are low probability events with potentially high impact. Most people are not able to gauge the probabilities and potential impacts, especially when the negative impacts accrue in the long-term.

- Instead of thinking about having a one-size-fits-all solution for people to have their data protected (e.g. people give their consent but don't understand what it is they are consenting to) policymakers might consider an approach that involves targeted outreach to specific communities at relatively higher risk.

- Another way for governments to intervene may be through education. Awareness campaigns and education might help people understand what the risks are. Educating policymakers on the trade-offs, the tools, and the opportunities around technology policy is also important.

- Finding ways to incentivize companies to protect consumer data and privacy, (e.g. fiduciary duty with regards to consumer data or with regards to data in general), is another avenue to consider. As a consequence, companies may begin differentiating themselves on security or privacy. This would, in turn, permit informed/educated consumers to make a choice about what attributes they wish to have in the technology purchases that they make.

Panel 4B: On Notice: The Coming Transformation of Key Economic Sectors

Moderator: Vikram Pandit, Founding Principal, The Orogen Group, and Trustee, Columbia University

Daniel Gallancy, CEO, SolidX Partners

Eli Noam, Professor, Columbia Business School

Andrew Saltzberg, Global Mobility Policy Lead, Uber

Joah Sapphire, Adjunct Professor, Columbia SIPA

Key questions:

This panel discussed several key sectors that are currently undergoing significant disruption as a result of the development and commercialization of data and digital technologies over the past decade: finance, urban transportation, telecommunications and logistics. For instance, the rise of Bitcoin and other cryptocurrencies over the past five years has prompted the financial sector to quickly adopt the underlying blockchain technology to gain efficiencies in their own operations. Utilities and agriculture are rapidly adopting sensors and data-driven operations. The 'uberization' of several markets over the past decade (e.g. hotels, taxis) is now moving into logistics.

- What changes are occurring in key economic sectors due to new waves of technology and how are these changes manifesting themselves?

- What are the public policy consequences of these changes? How might these consequences differ globally?

- Are there comparative policy models emerging to deal with these changes internationally? What characterizes these differing models?

- How might the public and private sectors effectively engage one another in promoting the adoption of or dealing with the consequences of these technologies globally?

Panelists (from left to right): Andrew Saltzberg, Eli Noam, Daniel Gallancy, Joah Sapphire, and Vikram Pandit

Key observations:

- A kind of trickle-down Moore's law is occurring in virtually every aspect of society. A challenge lies in the way that the societal processes of government are slowing down. This is occurring because there are “too many cooks in the kitchen.”

- These technology-driven changes are very new. Uber is only five years old. Bitcoin is seven years old. The shared ride products are less than two years old. We don’t yet know what the long-term consequences of all these things are.

- Ride sharing presents challenges to legal and regulatory systems set up to deal with different configurations in the past. In terms of transport, there was mass transit, which was essentially entirely publicly operated, and private transport, someone driving their own car. Now there is ride sharing arrangements that sit somewhere in the middle.

- Uber is also part of the transition from a W-2 type of economy possibly to a 1099 type of economy. This is one in which everybody is an independent contractor. It is also one in which work-related benefits and retirement and additional issues are not provided for anymore. The question to be answered as a society is whether we develop arrangements to deal with these changes?

- Blockchains are, in essence, a new database technology. The underlying asset, a crypto-currency like Bitcoin, for example, powers that database technology. It is the asset that makes that database technology secure and stable.

- Blockchains are presenting policy challenges because they supposedly possess attributes of many types of things. It has attributes of currencies, commodities, and at times may have attributes of securities. An open question is whether it really needs its own classification from a regulatory perspective?

- Ride-sharing, autonomous vehicles (or the Internet of Things) and cryptocurrencies are challenging the limits of existing regulatory and legal regimes. The commonly advocated approach, particularly by certain interest groups, has been to look to ways to create new, separate regulatory regimes to govern the activities linked to these technological changes. The risk of rent-seeking or regulatory capture in such proposals could be avoided by making adjustments to the existing regimes rather than establishing separate regulatory regimes.

Panel 5: Civic Entrepreneurs: Global Perspectives on Open Data, Engagement and Urban Governance

Moderator: Hollie Russon Gilman, Post-Doctoral Fellow for Technology and Public Policy, Columbia SIPA

Ania Calderón, General Director, Open Data, Office of the President, Republic of Mexico

Michael Mattmiller, CTO, City of Seattle

Cathy Wissink, Senior Director, Technology and Civic Engagement, Microsoft

Key questions:

Around the globe technologists, government innovators, and civil society are leveraging digital tools and open data to make governance more responsive to citizens, strengthen the relationship between citizens and their government, provide new ways for citizens to participate in decision making in their communities, and make governments more accountable. Yet if the past decade is anything to go by, none of these outcomes are guaranteed.

- What are the most promising global examples of data and technology being used to hold government to account, better govern urban areas, or increase civic engagement?
- What might be the subsequent outcomes—both positive and negative—in areas such as governance, health care, and sustainable or local development?
- What kind of evidence base is required so as to generate robust and meaningful evaluations of the outcomes and success various open data initiatives?

Panelists (from left to right): Ania Calderón, Hollie Russon Gilman, Michael Mattmiller, and Cathy Wissink

Key observations:

- ‘Civic innovation’ is occurring in a number of ways. Government is opening up to a diverse group of stakeholders that weren't part of the public debate before. There is more collaboration between government and new startups that have a civic entrepreneurship role. More community and cross-sector interactions means more partnerships among government, the private sector and the civic tech community.

- City-based initiatives tend to fall between two ends of a spectrum. There are well-intentioned community members who envision a solution and make it their mission to see it through. On the flip side, government can be more intentional about saying, "Here is our problem, help us solve it," then actively reaching out to community members.

- Technology sustainability and maintenance is an emerging issue. Everyone wants to create a 1.0 version of a technology. Yet no one wants to support or maintain a technology. Over time, problems emerge, e.g. the data source fails or there is a security breach.

- Two major challenges are arising from technology and data driven innovation at a local level. The open data approach brings potential privacy harms. Also, only certain people on the ‘right side’ of the digital divide are able to benefit from these initiatives.

- Interagency trust is a common challenge that impedes effective information and data sharing. The solution lies in creating a situation where agencies are able to share the credit for projects that are done well but are not hung out to dry alone if problems arise. This de-risks the proposition of doing things differently, versus sticking with the status quo.

- Another helpful way in which to introduce change within government institutions is the ability to hire or bring new and different people in – particularly people who can help government agencies think about what the commercial sector is doing.

- Important questions lie around whether investment is occurring in initiatives that can scale-up. When public funds are going towards initiatives, there is a need to prove that they are going to have some sort of meaningful impact at scale.

- Open data standards are an issue both within and between countries. If the inputs and outputs of programs cannot be compared, or if data sets cannot be linked across each other, it is hard to come up with new insights. Peer networks to share best practices and drive toward commonly agreed upon standards are important in this respect.

Issues Briefs

Panel 1: Global Security Challenges and Data

By David Omand

We are living through the beginnings of a revolution in human affairs enabled by the digitization of information and means of communication through the Internet, web and mobile devices (with the Internet of Things to come). We are now dependent on this technology for our economic and social progress, to deliver international economic development and for our national security and public safety. As set out below, trust has to be built in the open Internet as a safe place to innovate, to do business, to shop and to interact socially, and in the ability of the authorities to be able to uphold the law in cyberspace. That trust cannot be taken for granted.

Conflicting priorities arise at three levels:

- Surveys record increasing *concerns by individuals* for their right to privacy, for protection of their personal information from hackers, from carelessness on the part of corporations, from unrestrained government surveillance, from new techniques such as predictive analytics, and from the very business model of the Internet that rests on the monetization of personal data. One result is the demand for end-to-end encryption, anonymization software, for secure apps and mobile devices and for stronger data protection law. Another is the risk of fragmentation of the Internet as some governments seek to restrict where their citizens' data may be processed or stored.
- At the same time, *law enforcement* expresses growing concern over the way that serious criminals are able to exploit the vulnerabilities of digital technology (and human behavior when using it) to conduct their crimes at scale. Daesh terrorists have been able to use the web to publicize their atrocities and recruit new followers whilst being able to hide their communications from the authorities. Criminal activity using the Internet (including the Dark Net) includes terrorist facilitation, sale of cyber attack exploits, global fraud and money laundering, narcotics trafficking, proliferation of weapons of mass destruction, human trafficking, child sexual abuse and intellectual property theft. Law enforcement is finding it increasingly difficult to counter these threats, to establish the identities of those responsible and to secure the evidence they might have in the past to bring the criminals to justice, especially when they are hiding overseas, or the evidence is in corporate databases in another jurisdiction.
- Meanwhile, *national intelligence agencies* have been able to exploit digital technology to gather information for the protection of national security (the

> fundamental duty of government) including generating intelligence for military operations and force protection around the world, to support diplomacy and national security policy making and to protect the critical national infrastructure from destructive cyber attacks. At the same time, intelligence agencies have been trying to use their advanced capabilities to assist law enforcement in their mission to keep the public safe, uncovering global criminal networks, and especially tracking terrorists across frontiers. The legal framework for such activity has been shown to be defective or missing altogether in many nations. The exposure of many of these capabilities has heightened the concerns over privacy described above.

As with all hard public policy issues there is no easy way of reconciling competing demands. Place security of personal data and anonymity on the Internet above all else and law enforcement is shut out, the rule of law is undermined, crime, terrorism and cyber attacks will flourish. Prioritize access for law enforcement and intelligence agencies, for example through weakening encryption standards, and confidence in the Internet as a secure medium will be lost and fragmentation of the Internet will spread.

A set of satisficing measures is needed sufficient to ensure respect for *all* our fundamental rights - to the rule of law, to life, to freedom of speech and assembly, to enjoyment of property, to privacy for personal and family life - without lurching to any extreme. In particular, security and privacy should not be traded off one for the other: a sufficiency of both is necessary in a civilized society.

What makes these issues even harder is that solutions have to be found not just nationally but internationally, and in the context of a global struggle over the governance of the Internet itself. Measures are needed that reinforce the nature of the Internet as a secure, open and safe medium, that are technically sound and that make business sense as well as encouraging the ‘permissionless’ innovation that is the hallmark of the Internet. Government policies might therefore:

- Insist upon continuing multi-stakeholder Internet governance engaging governments, the Internet companies, the tech community and civil society.
- Oppose mandatory data localization and the fragmentation of the Internet into national blocks.
- Maintain the open nature of the Internet where data flows are based upon efficient routing principles and protocols and on open standards openly arrived at.

A promising approach is to encourage in forums such as the OECD, the UN Governmental Group of Experts, the Internet Governance Forum, NETmundial, G20 and the World Summit on the Information Society the development of norms of responsible conduct in cyberspace for like-minded States (accepting that although not all States will initially comply, the reputational cost of bad behavior will be raised). Governments, civil society and the tech community should:

- Insist upon the application of International Humanitarian Law to constrain offensive activity in cyberspace as much as in the everyday physical world.
- Insist upon Governments not weakening or compromising encryption or other standards on which the integrity of the Internet depends. The core infrastructure of the Internet must remain stable and secure.
- Ensure the development of the Internet of Things includes security, and is not based on closed, proprietary systems.
- Enable cyber security partnerships between government agencies, the private sector operators of the critical national infrastructure and the tech community.
- Encourage the development of the cyber insurance industry.
- Insist that any restrictions on Internet content are solely for the purposes of public safety and security and as provided by law and oppose governments trying to shift to the private sector responsibility for policing the content of Internet traffic.
- Encourage the development of new trust architectures, such as may come from blockchain innovation

Governments should, in particular:

- Work to develop common standards of data protection across borders to build confidence in data hosting and processing where most efficient.
- Build effective international information and evidence arrangements to tackle current issues of terrorism, organized global criminality and cyber security. Starting with discussions between the US and the EU seek to reform Mutual Legal Assistance Treaty MLAT processes and develop cyber-MLATs and cross-border arrest warrants for cyber crimes.

To reinforce both security and privacy, governments, civil society and the tech community should:

- Accept the necessity for digital intelligence activity (including, when necessary, access to the Internet in bulk as a legitimate means of gathering foreign intelligence and managing the risks of hostile cyber attacks) but insist all such activity must be covered by the rule of law. Statutory safeguards should involve:
- Regulation of intelligence and law enforcement agencies stipulating the purposes for which they may acquire secret intelligence and the safeguards for privacy and other human rights that must be applied when intrusive methods are used.

- Authorization procedures that cover all the ways of accessing digital intelligence: from communications data, the content of communications, interference with equipment (including hacking into adversaries' systems) and the holding and exploitation of databases containing personal information about individuals.
- Independent judicial and legislative oversight of intrusive intelligence activity.
- Independent judicial investigation of allegations of abuse and right of redress if proven.
- Apply the principles of the Universal Declaration of Human Rights, accepting that the right to privacy in cyberspace is not absolute where there are legitimate, necessary and proportionate reasons for the authorities to intrude (including 'reasonable searches and seizures' as provided for in the U.S. Constitution's 4th Amendment).
- Accept that law enforcement has the right to seek, with proper authority, evidence relevant to investigations that is held by Internet companies, and that companies have a duty to respond cooperatively where there is no conflict of laws, where the request is legally sound and reasonable in the circumstances, and where to comply with the request would not place at risk unreasonably the security of other users of cyberspace.
- Accept that privacy rights are engaged when the authorities seek bulk access to personal information (in motion or stored). The extent of privacy intrusion, and thus whether it is compatible with privacy rights, depends then upon whether computerized search algorithms to filter, target and select material for analyst examination comply with the principles of lawfulness, necessity and proportionality. Mass surveillance, on the other hand, should be considered unlawful.
- Provide for added protection where legal professional privilege, journalistic material, ministers of religion and legislators are concerned.
- Accept that there are legitimate reasons for enabling anonymity on the Internet, including for use by dissidents in repressive regimes and by journalists to protect their sources but that, as with privacy, it is not an absolute right. In particular, there is no right to anonymity for operation of websites on the dark net.
- Redefine legal thresholds for so that the most revealing forms of meta data such as the complete browsing history of an individual are treated in the same way as content of communications, whilst allowing basic communication data – who called, when, where, for how long, by what means – to remain a basic tool of policing.

Panel 2: National Data Governance in a Global Economy

By Anupam Chander

Introduction

Global data flows are the lifeblood of the global economy today and of the technologies of the future. Yet, the regulation of how data is to be handled remains largely the province of national laws. How we resolve the dilemmas of global flows within a nation-state structure will impact the digital economy, free expression, privacy, security, consumer protection, and taxation. Just as we once built an architecture for cross-border flow of goods, we need to build an architecture for cross-border flow of information.

Problem Statement

In the absence of, at minimum, a *modus vivendi* for global data flows, the World Wide Web may increasingly tear apart, and the global Internet may disintegrate into national or regional 'Splinternets.'

Issues

Global Data Flows Are Crucial to Innovation

Many of the most promising technologies and economic innovations rely on global data flows. Consider the following ten recent developments:

1. **The Internet of Things.** Devices like an Apple Watch or a Samsung Smart TV — or even a John Deere or Komatsu heavy machine — depend on the flow of information across national borders to gather and process data.
2. **App Economy.** Individuals and small companies can now build applications and leverage global marketing, distribution, and payments networks to sell their products and services to the nearly 2 billion smartphone users across the world.
3. **Outsourcing of Services.** The ability to outsource business processes and information technology services depends on the cross-border flow of information.
4. **E-commerce.** Companies like Alibaba and eBay depend on global information flows to enable people to sell to, and buy from, global markets.
5. **Cloud computing.** Cloud computing depends on the transfer of large volumes of information, often across borders, to server farms typically located based on network efficiencies, security, and costs. Robots, for example, increasingly depend on cloud-based information storage and processing.
6. **Big data.** Data sets can be larger if they include people across borders; analytics are often performed using tools and companies located in foreign jurisdictions.
7. **Digital products and streaming services.** Digital music and video services, from Apple, Netflix, Spotify, and others, increasingly allow customers across the world to download or stream audiovisual content.

8. **Social media and websites generally.** Social media, and the Web generally, implicate significant information sharing across borders.
9. **The sharing economy**. AirBnB, Uber, and the like allow one to share one's resources, often for a price, with people from anywhere in the world.
10. **Crowdfunding**. People planning new projects can now raise funding from supporters across the world.

Rules that make it difficult to move data across borders will complicate and even at times make impossible efforts to offer such innovations. For example, if companies rolling out Internet-enabled devices have to create or purchase separate data infrastructures for each country in which they operate, the costs of providing many such devices may prove prohibitive. Companies like AirBnB, Uber and Upwork depend on individuals across the world sharing information across national borders. Finally, rules that prevent information from leaving home except in difficult to obtain circumstances can effectively bar foreign service providers offering back office outsourcing from processing information (a result that trade protectionists favor).

The Rise of Internet Border Controls: From Censorship to Data Localization

Efforts by national governments to assert control over global data flows trace back at least to the turn of the Millennium. A French court ordered Yahoo! to prevent Nazi material from being made available within France. Yahoo! protested that they should be governed by the liberal free speech codes of their American home, but the French court was unpersuaded, and Yahoo! voluntarily complied by removing the material from its services everywhere. A more notorious application of governmental efforts to control information can be found in the so-called Great Firewall of China, which enlists Internet companies in censoring material within the country. Recently, France's privacy regulator has penalized Google for failing to remove search results subject to the "right to be forgotten" from sites outside France, not just from results accessible in France as Google was prepared to do.

The French Yahoo! decision and the Great Firewall of China represent what we might describe as the first generation of Internet border controls, that is, efforts to control information coming *into* a country. "**Data localization**" is the name for a less familiar but increasingly popular new kind of Internet border control. This second generation of Internet border controls seeks to keep information from going *out* of a country. Governments seek data localization on a variety of grounds, from data protection to outright protectionism.

Many governments have increasingly sought "**data sovereignty**," often seeking both to control data within their countries and to limit the flows of data outside their countries. The globalization of data raises issues that the globalization of goods did not, because data often contains very personal information, for example about our searches, our likes, our friends, our finances, and our health. It is easy to use the sensitivity of data to bar foreign service providers by requiring that data be stored or processed by local providers. Assertions of data sovereignty often coincide with a general industrial plan to grow a local set of Internet services to displace the largely American leaders (including Google, Apple, Facebook, and Amazon, or “GAFA” as they are sometimes labeled in Europe). Experience with trade in goods, however, tells us that it is possible to meet varying national safety standards even when importing goods from abroad.

Figure 1. Internet Border Controls

	First Generation	**Second Generation**
Type of control	Censorship	Data Localization
Stated Goals	Prevent unwanted information from entering country for social or political purposes	Prevent information from leaving country to (1) protect privacy (though privacy can be protected even when information is processed abroad); (2) assist local law enforcement, surveillance & control; (3) promote local enterprise
Examples	Great Firewall of China	Russian data localization

Protecting Privacy and Avoiding Foreign Surveillance

Last year, the European Court of Justice took up an Austrian law student’s challenge to Facebook’s processing of his personal information. In *Schrems v. Irish Data Protection Commissioner*, the court concluded that United States surveillance practices meant that European data could no longer be processed in the United States under an existing Safe Harbor agreement. In response the United States has agreed to added protections against mass surveillance for Europeans under a “Privacy Shield” arrangement, including a right under a new United States Judicial Redress Act to sue the U.S. government for mishandling their data. Some in Europe have criticized the new arrangement as containing inadequate guarantees.

The case against Facebook recalls two other cases in which American companies have been asked to assist U.S. law enforcement. In 2013, a US. judge directed Microsoft to turn over user information stored on its Irish servers, but Microsoft has challenged the order, earning the support of the Irish government. Most prominently, in a domestic case with international implications, Apple fought the U.S. government's initial efforts to compel it to assist in defeating a security feature on its iPhone, in part because complying would empower other governments to demand Apple's assistance as well.

Because both Europe and the United States recognize the importance of cross-Atlantic data flows to the economies of both regions, a new arrangement permitting transfer must be found to allow information to flow across the Atlantic. As it stands now, companies and individuals continue to transfer information because of necessity, but lack any assurance that such transfers will not subject them to liability. As the European Union (EU) implements the new General Data Protection Regulation (replacing the 1995 Data Protection Directive), liability under EU law becomes ever more alarming, potentially subjecting a company to fines up to four percent of the company's annual global turnover.

Conclusion: Charting a Path Forward in Cyberspace

If we are to gain the enormous benefits from information exchange made possible by the Internet, we will need to engage in a series of reforms. These may include:

- *Surveillance Reform*. Need for respecting dignity of foreigners abroad; recognize that International Covenant on Civil and Political Rights (ICCPR) obligations apply to a government's actions not just at home, but also with respect to foreigners abroad. The US EU Privacy Shield provides some assurance that Europeans will not be subject to mass surveillance by U.S. authorities, including actionable guarantees of freedom from mass surveillance under the Judicial Redress Act. Thus far, it is unclear whether citizens of foreign countries outside Europe might benefit from similar guarantees of freedom from mass surveillance.
- *Privacy protections*. Governments need to ensure data protection, so that privacy and security are upheld regardless of where data flows. Here there a number of competing models, including the European Union's General Data Protection Regulation (an omnibus consent based approach to all processing of personal information regardless of entity) or the United States sectoral privacy law (focused on certain categories of sensitive information held by industry professionals) coupled with privacy promises enforced by the Federal Trade Commission and class action lawyers.
- *Free Trade Commitments*. Commit governments to permit data to flow across the world and services to be performed from abroad, unless legitimate interests such as privacy require otherwise. If it is ratified, the Trans-Pacific Partnership agreement between a dozen Pacific rim nations would require governments to permit cross-border data flows unless justified by a "legitimate public policy objective." It is unclear whether the Transatlantic Trade and Investment Partnership (TTIP) being negotiated between the United States and Europe will subject European crossborder

data flow restrictions to any trade disciplines. Finally, the Trade in Services Agreement (TiSA) being negotiated now between a large number of developing and developed nations, including the United States and nations of Europe, seems likely to include provisions favoring crossborder data flows.

- *Crossborder Government Access to Data*. Reform of the cumbersome Mutual Legal Assistance Treaty process is needed, but any reform must respect human rights limits on government access. The current process is flawed in multiple respects. As a map by Access Now makes clear (see https://mlat.info/), not every country has a law enforcement information sharing agreement with every other country. A United States statute from 1986, the Stored Communications Act, prohibits Internet companies subject to the law from sharing information with foreign governments, permitting sharing only with "governmental entities" (defined as "a department or agency of the United States or any State or political subdivision thereof"). Finally, even when a law enforcement agency seeks information through the MLAT process, compliance is painfully slow. Governments will need to work in multiple forums to improve human rights-protective systems of government access to information stored across borders. Because security information held abroad will often be held by corporations, corporations too must pay increasing attention to what rules they follow in providing access to foreign service providers.
- *Dispute Resolution*. Encourage the development of Internet-based crossborder dispute resolution systems. Existing trade agreements and even the "twenty-first century" agreements being negotiated now lack low cost mechanisms accessible to consumers and businesses to resolve disputes. Companies like eBay and PayPal have created their own global dispute resolution systems, and it seems likely that more private efforts to create such Internet based mechanisms will emerge.

Panel 3B: Cyber Conflict: Prevention, Stability and Control

By Jason Healey[1] and Tim Maurer[2]

'Removing the Heat from Cyber Competition and Conflict'

Only a few years ago, there were almost no norms globally accepted by governments on cybersecurity or cyber conflict. Even the United States, which had long pushed such norms, had publicly announced very few. The United States and a few other allies confirmed that laws of armed conflict (otherwise known as International Humanitarian Law or the "Geneva Convention") applied to cyberspace.

This has changed with tremendous progress recently, so much so that 2015 could be called was the Year of Global Cyber Norms.

Norms and Cyber Norms

In the academic literature, norms have been famously defined by Peter Katzenstein as "collective expectations for the proper behavior of actors with a given identity."[3] Norms generally can range from the global level to the nucleus of the family and they can be implicit or explicit. For example, laws can but do not always represent a norm. A law to which people adhere can represent "a collective expectation for the proper behavior of actors with a given identity." On the other hand, a law that's in the books but that nobody adheres is not reflective of an actual norm and collective expectation for the proper behavior.

In the international cybersecurity discussion, "norms" have taken on a slightly different meaning. The 2015 report of the UN Group of Governmental Experts states that "Voluntary, non-binding norms of responsible State behavior can reduce risks to international peace, security and stability. Accordingly, norms do not seek to limit or prohibit action that is otherwise consistent with international law."[4] Cyber "norms" in this sense could be seen as "potentially a precursor to eventual customary international law (through practice) that might eventually (after years) be codified."[5]

The narrative about norms for cyberspace (or alternately, ICTs for Information and Communication Technologies) is rooted in politics, as with most norms. The process started with a Russian proposal in the late 1990s for a legally binding

[1] Jason Healey is Senior Research Scholar at Columbia University's School of International and Public Affairs and Senior Fellow at the Atlantic Council.

[2] Tim Maurer co-leads the Cyber Policy Initiative at the Carnegie Endowment for International Peace and serves as a member of the Research Advisory Network of the Global Commission on Internet Governance.

[3] Peter Katzenstein. *The Culture of National Security: Norms and Identity in World Politics* (New York: Columbia University Press: 1996) 5

[4] United Nations, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (22 July 2015) UN Doc A/70/174

[5] Michele Markoff, Department of State, in email conversation with authors, 7 April 2016.

cybersecurity treaty.[6] According to Sergey Ivanov, Russia's Minister of Defense from 2001 to 2007, "Russia wants to develop international law regimes for preventing the use of information technologies for purposes incompatible with missions of ensuring international stability and security."[7] However, the Russian government's proposal was met with skepticism not just by the U.S. government. As Ronald Deibert, professor of political science, explains

> Russia has been pushing for arms control in cyberspace, or information-weapons control. Most people dismiss this as disingenuous, and I tend to agree. Most observers see it as Russia‘s attempt to constrain U.S. superiority in the cyber domain. Russia is more concerned about color revolutions and mobilization on the Internet by dissident and human rights groups – and trying to eliminate the United States' ability to support that type of social mobilization – than it is about protecting the Internet.[8]

These concerns are complemented by skepticism regarding the enforceability and verifiability of a treaty relating to cybersecurity. The United States pushed its own process, leading to five unanimous UNGA resolutions on "Creating a Culture of Cybersecurity, because "challenges to cybersecurity was better answered by a good defense than by constraining offense (technology), providing a juxtaposition to the Russian argument that security could only be accomplished through arms control."[9]

The norms agenda really started to pick up speed when the Obama administration took office with a marked shift toward more international engagement. This shift included greater engagement in discussions about cybersecurity, with the US starting to actively promote the idea of international norms for cybersecurity after it largely ignored the resolution in the UN General Assembly's First Committee for the first decade.[10]

Over time, the norms agenda evolved, as it was adopted and expanded by other countries and became a concerted effort of the international community. The overarching goal of the diplomatic efforts to date has been to agree to norms guiding behavior in cyberspace. From an academic perspective, these

[6] Tim Maurer, "Cyber Norm Emergence at the United Nations – An Analysis of the UN‘s Activities Regarding
Cyber-security?", Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011

[7] Christopher A. Ford, "The Trouble with Cyber Arms Control," The New Atlantis – A Journal of Technology & Society, Fall 2010, http://www.thenewatlantis.com/publications/the-trouble-with-cyber-arms-control.

[8] Ronald Deibert, "Tracking the emerging arms race in cyberspace," Bulletin of the Atomic Scientists 67.1, January/February 2011, http://thebulletin.org/2011/januaryfebruary/ronald-deibert-tracking-emerging-arms-race-cyberspace.

[9] Michele Markoff, Department of State, in email conversation with authors, 7 April 2016

[10] White House. "U.S. International Strategy for Cyberspace". 16 May 2011;
U.S. Department of State, International Security Advisory Board. "Report on A Framework for International Cyber Stability". 2 July 2014

discussions can be broken down into four components: contestation, translation, emergence, and internationalization.[11]

Cyber Norms: Contestation, Translation, and Emergence

Norm contestation: At first, there was disagreement in the international community whether existing international law and norms already apply to cyberspace or if the international community should develop new laws specific to cyberspace. A few countries, China, in particular, contested the idea that existing norms apply and were a proponent and promoter of the latter approach. Conversely, the United States and United Kingdom announced a set of norm-like policy goals or "rules of the road" (in the words of then UK Foreign Minister William Hague), as did Dr. Hamadoun Touré, the Secretary General of the International Telecommunications Union.[12]

However, in 2013, the UN Group of Governmental Experts (with representatives from 15 countries including China, Russia and the United States), published a consensus report affirming that "international law and in particular the United Nations Charter, is applicable." This report and the year 2013 can therefore be seen as the end of the norm contestation period, especially regarding the application of international humanitarian law. Though pushback flares up occasionally, the idea of norms in this space has been largely put to rest.

Norm translation: In parallel to these political negotiations, other experts had been investigating how existing norms and laws could be translated to cyberspace. The United States, United Kingdom, Australia and other states had already announced that they believed the laws of armed conflict applied to military cyber operations. However, there was little work describing precisely *how* they applied.

Accordingly, the most important effort of norm translation has been the *Tallinn Manual on the International Law Applicable to Cyber Warfare* developed by a group of international (but all Western) lawyers under the auspices of NATO's Cooperative Cyber Defense Center for Excellence published in 2013.[13] It examines in significant detail how existing international law governing activity above the threshold of use of force and armed attack could apply to cyberspace. This area has moved to the center of the cyber-security community's attention. The Tallinn Manual 2.0 expected in 2016 is only one example of an increasing flurry of activity focusing on this issue.

[11] This section is based in part on Maurer, Tim. "Cybersecurity and Asia" (September 2015) https://static.newamerica.org/attachments/9847-cybersecurity-and-asia/Cyber-security%20and%20Asia.b7302cdb44324fc38d6c49455429b59e.pdf.

[12] Jason Healey, "Comparing Norms for National Conduct in Cyberspace," Atlantic Council, 20 June 2011, http://www.atlanticcouncil.org/blogs/new-atlanticist/comparing-norms-for-national-conduct-in-cyberspace.

[13] Cooperative Cyber Defense Center of Excellence, "Tallinn Manual," https://ccdcoe.org/tallinn-manual.html.

Norm emergence: Just as the year 2013 saw the end of the phase of global discussions on norm contestation, so was 2015 the year of norm emergence and internationalization.

The process started with a speech in May 2015 in Seoul, wherein Secretary of State John Kerry laid out two sets of norms important to the United States; the first set already rooted in international law, the second are proposed norms to create better rules of the road on cyber offense and defense:

> [T]he basic rules of international law apply in cyberspace. Acts of aggression are not permissible. And countries that are hurt by an attack have a right to respond in ways that are appropriate, proportional, and that minimize harm to innocent parties.
>
> We also support a set of additional principles that, if observed, can contribute substantially to conflict prevention and stability in time of peace...
>
> First, no country should conduct or knowingly support online activity that intentionally damages or impedes the use of another country's critical infrastructure.
>
> Second, no country should seek either to prevent emergency teams from responding to a cybersecurity incident, or allow its own teams to cause harm.
>
> Third, no country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain.
>
> Fourth, every country should mitigate malicious cyber activity emanating from its soil, and they should do so in a transparent, accountable and cooperative way.
>
> And fifth, every country should do what it can to help states that are victimized by a cyberattack. [14]

These norms were treated with a bit of caution by many experts. As expressed by General Michael Hayden, former head of the Central Intelligence Agency and National Security Agency, "We only steal stuff to keep you free and to keep you safe. We do not steal stuff to make you rich. I know of four other countries that can say those last two sentences. Everyone else steals for commercial advantage." This complicates the U.S. government's push that national intelligence agencies should not steal commercial secrets for the benefit of local companies, Kerry's third norm.

[14] Secretary John Kerry, "An Open and Secure Internet: We Must Have Both," remarks in South Korea, 18 May 2015, http://www.state.gov/secretary/remarks/2015/05/242553.htm.

Yet it turns out, these norms were in fact the beginning of a new era. With the growing number of bilateral and multilateral agreements, norm internationalization is now also starting to take center stage.[15]

Cyber Norms: 2015, the Year of Internationalization

Just a few months after Secretary Kerry laid out the U.S. perspective on norms, in July 2015, another UN Group of Governmental Experts, this time comprised of representatives from 20 countries, agreed to a new consensus report including the following cyber norms in addition to several others focusing on supply chain integrity and responsible vulnerability disclosure:

- States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
- States, in ensuring the secure use of ICTs, should respect … the promotion, protection and enjoyment of human rights on the Internet, as well as … the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;
- A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;
- States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts.
- States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;
- States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams … of another State. A State should not use authorized emergency response teams to engage in malicious international activity. [16]

This was a far richer set of norms than most outside experts had expected the UN GGE to be able to agree on; after all, the level of tension between the United States, China and Russia on a range of issues, not just cyber, was already high. The Snowden revelations of US cyber espionage seemed likely to torpedo any significant agreement, yet there was more concordance to come.

During his September 2015 visit to the United States, President Xi Jinping of China and President Barrack Obama welcomed the UN GGE report and agreed to “establish a high-level joint dialogue mechanism on fighting cybercrime and related issues” as well as important norms:

[15] *See* Tim Maurer, "The new norms." *Jane’s Intelligence Review* (March 2016): 52-53

[16] United Nations General Assembly, “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,” UNGA A/70/174, 22 July 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

> The United States and China agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities.
>
> The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.[17]

A month later, when Xi visited London, he struck a similar agreement on theft of trade secrets with Prime Minister Cameron:

> UK and China agree not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of providing competitive advantage.[18]

According to press, when Premier Angela Merkel of Germany was in Beijing, she was able to secure the same promise, so that "China and Germany agreed to work on stopping economic cyber spying between the two nations," however, unlike the US and UK agreements, this has yet to appear in a formal, concluding statement by the leaders.[19] Even so, there was still more norm internationalization to come.

At the Ankara Summit, in November 2015, the leaders of the G20 nations – including from true cyber powers such as Russia, China and the United States but also from Brazil, India and Indonesia – gave their approval to this latest UN GGE report and called out several specific norms:

> We affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.
>
> All states in ensuring the secure use of ICTs, should respect and protect the principles of freedom from unlawful and arbitrary interference of privacy, including in the context of digital communications.
>
> We also … affirm that international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the

[17] The White House, "FACT SHEET: President Xi Jinping's State Visit to the United States," 25 September 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[18] UK Government, "UK-China Joint Statement 2015," 22 October 2015, https://www.gov.uk/government/news/uk-china-joint-statement-2015.

[19] Stefan Nicola, "China Working to Halt Commercial Cyberwar in Deal With Germany," Bloomberg Technology, 29 October 2015, http://www.bloomberg.com/news/articles/2015-10-29/china-working-to-halt-commercial-cyberwar-in-deal-with-germany.

> view that all states should abide by norms of responsible state behaviour in the use of ICTs.[20]

Secretary Kerry's speech in Seoul had just been in May 2015 and by November of that same year, just six months later, norms went from proposal to agreement at the top levels of global governance.

Private-Sector Norms

In addition to states proposing international cybersecurity norms, non-state actors have also been actively participating in this discussion. In one sense, the Internet was built on norm-like international behavior, from technologists building the network based on "rough consensus" to cooperating across boundaries to limit disruptions to the network. In late 2014, Microsoft took these norms one step further, launching a report proposing six specific norms overlapping with certain norms proposed by states:

1. States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.
2. States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.
3. States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.
4. States should commit to nonproliferation activities related to cyber weapons.
5. States should limit their engagement in cyber offensive operations to avoid creating a mass event.
6. States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.[21]

Complementing its substantive proposals, Microsoft also issued a procedural recommendation proposing a G20 + ICT20, the G20 member states meeting with twenty leading ICT providers, to develop an "agreed-upon norms document" which would "allow the 20 most developed economies to hold themselves and others accountable to the agreed-upon behaviors in cyberspace."

[20] G20, "G20 Leaders' Communiqué Antalya Summit, 15-16 November 2015," http://www.consilium.europa.eu/en/meetings/international-summit/2015/11/G20-Antalya-Leaders-Summit-Communique-_pdf/.

[21] Angela McKay, Jan Neutze, Paul Nicholas, and Kevin Sullivan, "International Cybersecurity Norms," Microsoft, December 2014, http://aka.ms/cybernorms.

Why Was 2015 the Year of Cyber Norms?

While these norms include certain caveats, for example, what is considered "unlawful" will depend on each country's domestic laws, it appears the remarks by Secretary Kerry lit a spark which took norms from an area of contention toward much greater international appeal, including G20 backing and statements by heads of state. The two most repeated norms include one of the least controversial (that "the basic rules of international law apply in cyberspace" which had been previously agreed to in the 2013 UN GGE report) up to certainly the most controversial (that "no country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain").

There are at least six likely, overlapping reasons why 2015 was a year when so much progress was made on articulating cyber norms.

Rising cyber tensions. Certainly within the United States, but assumedly in other nations as well, government officials and experts were seeking means to counter the rising frequency and violence of cyber attacks. From cyber espionage, to disruptive attacks like Stuxnet or against Sony, each nation seems to feel strategic vulnerability to others in cyberspace. Norms, in part, gained appeal because key states saw stability as being in their national security interest.

Leadership's personal attention. Within the United States, this concern was driven by the personal attention of President Barrack Obama who raised the issue with President Xi Jinping in the Sunnylands summit, mentioning the "deep concerns we have as a government around theft of intellectual property."[22] In China, President Xi named himself chair of an Internet security working group.[23]

Diplomacy and summit politics. Diplomats sometimes need a win for national (or even personal reasons) and may be willing to make tradeoffs they'd otherwise refuse. Likewise, leaders want to have successful summits. China came ready to the United States and the United Kingdom to make deals and ensure the summits would be a success. According to discussion with participants in the earlier 2013 UN GGE report, similar to President Xi having his first summit with President Obama at Sunnylands, the Chinese delegation was willing to compromise at the 2015 UN GGE.

Universality. When the governments selected norms at least some of them were meant to be relatively easy for most states to agree to, as it would be in their long-term interest. Therefore, key criteria were universal appeal and utility to be good for all states' national security.

[22] The White House, "Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting," 8 June 2013, https://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-.

[23] Shannon Tiezzi, "Xi Jinping Leads China's New Internet Security Group," The Diplomat, 28 February 2014, http://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/

Hard diplomacy. Diplomats, especially but not only from the US State Department, put in long hours negotiating and dealing with their counterparts to make progress over the course of 2015. Key international conferences, such as the Global Conference on Cyberspace in The Hague in April 2015, kept this momentum thanks to hard work by the Dutch government.

Low cost to commit to norms. It is also possible nations were willing to commit to norms because they give modest gain at relatively low cost. After all, if attribution continues to afford plausible deniability, then it could be hard for other states to prove that a nation is violating the norms. Many pessimistic experts felt there is little-to-no chance countries would forego cyber espionage. Likewise, other experts doubt states will live to up to the norm that “States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products.”

Looking Forward

This last possible reason - a perceived low cost for committing to norms - points to the key factor in whether these new international norms will be effective.

The new, most pressing question will be whether and how states will implement and internalize the norms to which they agreed. According to the lead US diplomat negotiating these norms,

> most states are not in a position to accept new binding concepts in cyberspace. This allows them to initially sign on with no real penalty - that is, until the international community makes it common practice. Then deviations in behavior may be punished by the international community whether the norms are codified or not.24

Since the Obama-Xi agreement to limit stealing intellectual property for commercial gain, there has been intense debate within the US cyber community on whether China is living to the letter (or even the spirit) of the norm. But even if it leads to a reduction, but not an elimination, of such cyber espionage, it should still be considered a success. After all, diplomacy isn't binary. It's analog and if the norm leads to "less but not zero" – it is still a win for the United States and other nations facing such thefts.

If norms are in fact “collective expectations for the proper behavior of actors” then actors that fail to live up to those expectations will suffer at least reputational costs, especially if heads of state personally and publicly committed to them. In fact, this can be a central goal of diplomacy, to unveil the hypocrisy of other actors. So if a given norm is not enacted, national leaders who received a face-to-face agreement from President Xi will be in a much stronger position to respond to Beijing over its commercial espionage. The same holds true for other nations who may feel their critical infrastructure has been targeted or attacked by

[24] Michele Markoff, Department of State, in email conversation with authors, 7 April 2016.

the Russian or the US military or intelligence community, despite the explicit commitments by those governments.

Even though the progress on cyber norms over 2015 was sudden, that success had in fact been built on the years of hard work by diplomats, cyber experts, and many others. It is now time for more hard work, to help nations live up to these norms to ensure a more peaceful cyberspace in future.

Panel 4B: The Coming Transformation of Key Economic Sectors

By Joah Sapphire

Introduction

Several vital economic sectors are currently undergoing significant disruption as a result of the advancement of digital technologies over the past decade. The emergence of digital technologies coincides with the convergence of smaller and faster chips embedded with sensors and actuators that are underpinning a multitude of devices. These devices are sending and receiving huge amounts of data over the high speed, global Internet. The storage and analytics of that data support limitless solutions and applications. Taken together this convergence is often referred to 'the Internet of Things (IoT)' and provides the backdrop for the next industrial revolution.

The financial sector faces the growth of Bitcoin and other cryptocurrencies and is now exploring adopting the underlying blockchains technology to gain efficiencies in their own operations. Automotives are rapidly incorporating sensors, artificial intelligence and data-driven operations in an attempt to develop autonomous vehicle solutions. The recent 'uberization' of several markets (e.g. hotels, taxis) is now moving into logistics.

Just as with the first industrial revolution, when governments were slow to react in understanding how to regulate international commerce driven by new technology, today the digitization of our economy is presenting a new set of policy challenges that may be the most complex we have ever faced. While it is impossible to capture the multitude of issues surrounding this change, an examination of the impending policy needs presented by cryptocurrencies, blockchains, autonomous vehicles and urban transportation can serve to offer some important insights for the coming transformation of key economic sectors.

Problem Statement

The digitization of cryptography has given rise to the advent of cryptocurrencies and blockchains. The ability to transact on the internet in a simple and anonymous manner is creating new difficulties for policy makers and regulators that were never before imagined. With smart phones gaining prevalence across every corner of the globe, how should governments balance allowing individuals to benefit from this technology through new ways to transact with one another while maintaining a consistent rule of law to control fraud and abuse? The stability of blockchains offers new ways to organize transactions and relationships but what mechanisms are in place to ensure the proper accounting of this new platform? All of these issues are important discussion points as connected devices become the common platforms for transacting in the global economy.

The development of autonomous vehicles has attracted huge investment from global automotive companies, auto parts suppliers and diverse technology companies that are new entrants in the automotive sector. While autonomous vehicles offer a tremendous profit opportunity, they present a multitude of policy challenges, with perhaps the greatest being how to regulate safety when the driver is now the vehicle. Governments have a responsibility to maintain the safety of the public especially on the roadways. In the case of autonomous vehicles and other emerging robotic devices how can the safety of the owner, user and general public be preserved when there is no human in the loop? Autonomous vehicles represent an immediate challenge to our current safety regulatory regime and that offers the opportunity for a demanding discussion of current international governmental approaches.

Finally, so-called sharing economy companies are very visibly disrupting numerous industries from hospitality to mobility. Urban transportation has experienced one of the fastest transformations and governments at all levels are facing new challenges as Uber, Lyft and others gain a greater share of markets. Ride sharing is quickly evolving into new logistics solutions, and policy challenges around labor relations and liability among others are now front and center, requiring governments to adapt to keep pace.

Cryptocurrencies and Blockchains

Since the public release of Bitcoin in 2009, governments have worked vigorously to develop rules and regulations to govern this new way to transact. However, there is still great divergence between how different governmental organizations and agencies define and consider cryptocurrencies and blockchains.

The initial efforts aimed at users of cryptocurrencies highlight four distinct policy issues, relating to the definition of a cryptocurrency, that have broad and substantial fiscal, monetary and economic implications (for more detailed explanation of the definitions below, see Appendix 1):

- From the users' perspective, the Financial Action Task Force (FATF) defines crytocurrencies as a currency, so for tax purposes, should profits from sales be taxed as ordinary income? 25
- Or is it a capital asset, following the Internal Revenue Service (IRS) definition, and thus gains and losses should be subject to capital gains tax rates and losses should be used to offset other gains?26
- Could certain cryptocurrencies meet the 'Howey' test and thus be treated as a security, implying treatment under federal securities laws and

[25] FATF (2014), "Virtual Currencies Key Definitions and Potential AML/CFT Risks", available from: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf, (accessed 4/12/16)

[26] IRS (2014), "IRS Virtual Currency Guidance:", available from: https://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance, (accessed 4/12/16)

oversight by the Securities and Exchange Commission (SEC) in the U.S.?27

- Finally, do cryptocurrencies meet the U.S. Commodity Exchange Act's definition of a commodity, implying that that mining Bitcoin should be taxed in another form such as royalties on mineral rights?28

Without proper policies in place the ambiguity of the treatment of cryptocurrencies impacts all of the actors in this sector from exchangers to miners of virtual currency. This lack of clarity limits that broad international adoption of cryptocurrencies.

At the same time, this also enables the potential for use of cryptocurrencies to support crime and tax evasion. Anti-money laundering and know your customer rules must now be applied to virtual currency. From a global policy perspective, are there sufficient regulatory bodies in place to ensure that cryptocurrencies are not being used to finance terrorism? Should these entities be satisfied with self-regulation by the financial industry or do governments need to step in to ensure that this new ability to transact is not exploiting weaknesses in the global payment system?

Cryptocurrencies provide the ability to transact. This differs from the underlying blockchains, which supports the shared ledger. The Australian Stock Exchange (ASX) in January of 2016 announced it was implementing a blockchain solution for equity trade processing. The new distributed ledger could reduce administrative costs and increase the efficiency of ASX's trading system. This is one of the first commercial applications of blockchains and many other finance entities are exploring the adoption of this new technology. Listed equity stock trading is a highly regulated market. Trading must be harmonized across the entire globe to ensure stable pricing and execution. Has there been enough testing of blockchains to ensure it is ready to go live? Who would be liable in the event of an incident and according to what standards? Numerous questions must be quickly studied and addressed.

Autonomous Vehicles

The United States Department of Transportation (USDOT) National Highway Traffic Safety Administration (NHTSA) defines vehicle automation as having five levels.29 While each level of vehicle automation has numerous policy issues, this discussion will involve Level 4 or Full Self-Driving Automation. A Level 4 vehicle is designed to perform all safety critical driving functions and monitor

[27] U.S. Supreme Court, SEC v. Howey Co., 328 U.S. 293 (1946), available from: https://supreme.justia.com/cases/federal/us/328/293/case.html, (accessed 4/12/16)

[28] Commodity Futures Trading Commission (CFTC) (2015), Docket No. 15-29, Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, available from: https://supreme.justia.com/cases/federal/us/328/293/case.html, (accessed 4/12/16)

[29] No Automation (Level 0), Function Specific Automation (Level 1), Combined Function Automation (Level 2), Limited Self-Driving Automation (Level 3), and Full Self-Driving Automation (Level 4). For full definitions of each level of automation please see Appendix 2.

roadway conditions for an entire trip. Such a design anticipates that the driver will provide destination or navigation input, but is not expected to be available for control at any time during the trip.30 Governments have very recently ramped up discussions of how to approach this innovation.

In February of 2015, the United Nations Economic Commission for Europe (UNECE) was the first international body to discuss international regulatory steps concerning autonomous vehicles. Under the auspices of the World Forum for harmonization of vehicle regulations, the UNECE Working Party on Brakes and Running Gear reviewed proposals covering semi-automated driving functions to pave the way for more highly-automated vehicles.31

The United States (US), United Kingdom (UK) and Japan among others have held hearings to discuss Level 4 vehicles but thus far have not enacted any new policies specifically governing autonomous vehicles. Within the US, at the state level, California, Michigan, Florida, Nevada, Tennessee and Washington D.C. have enacted legislation allowing limited driverless vehicle testing on public roadways.32

It is clear that policy makers are struggling with the best approach to address this new technology. The only approach that has been tried thus far is offering testing in controlled environments. Many technology companies feel this is insufficient because autonomous vehicles need to learn from real world environments. In the US, major autonomous vehicle players are increasingly growing frustrated with inaction at the federal level and complaining that US states are enacting a patchwork of laws that are not supportive of the commercialization of Level 4 vehicles.

In general, national or central governments need to update, establish and enforce policies and regulations around safety, privacy, data sharing, cybersecurity, manufacturing, vehicle design, infrastructure and data communications related to autonomous vehicles to enable state or provincial governments to then further tailor rules that meet distinct local needs.

- At the national level policy challenges include revising vehicle equipment requirements such as steering systems, braking systems, visual aids (side and rearview mirrors), seatbelts, and airbags, just to name a few. All of

[30] NHTSA (2013), “Preliminary Statement of Policy Concerning Automated Vehicles Available”, available from: http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf, (accessed 4/12/16)

[31] UNECE (2015), “UNECE to discuss first international regulatory steps concerning automated-driving”, available from: http://www.unece.org/info/media/presscurrent-press-h/transport/2015/unece-to-discuss-first-international-regulatory-steps-concerning-automated-driving/unece-to-discuss-first-international-regulatory-steps-concerning-automated-driving.html, (accessed 4/12/16)

[32] Gabriel Weiner and Bryant Walker Smith, “Automated Driving: Legislative and Regulatory Action”, available from http://cyberlaw.stanford.edu/wiki/index.php/Automated_Driving:_Legislative_and_Regulatory_Action, (accessed 4/12/16)

these current equipment specifications will have to be modified for Level 4 vehicles that use GPS, LiDAR[33] and radar for situational awareness.

- Roadway infrastructure requirements need to be revised in terms of signage and road striping for autonomous perception.
- In terms of liability does a human need to be in the loop? Should there be a human driver at all times or is there a need to require a human be available to override an autonomous vehicle system. If a human is not in the loop where does liability reside? With the vehicle owner? With the manufacturer? What standards or instructions should be required of the decision making of a Level 4 vehicle on the public roadways to ensure safety of the public?

At the state, provincial or local level policy challenges include vehicle permitting, infractions and infrastructure. With Level 4 vehicles, human error should be drastically reduced. This changes the paradigm for speeding tickets, traffic infractions and drunk driving laws, which are all administered at the state or local level. Other considerations include parking tickets, incentives for high occupancy vehicles and support for public transportation. All of these policy regimes will need to be revisited and competitiveness of a nation may depend on ensuring that these emerging rules and regulations are consistent across jurisdictions.

The race is on globally. Despite President Obama proposing $4 billion over ten years for autonomous vehicle research and testing, Google has indicated it may look to the UK as its first deployment market. The UK has advanced limited regulation for autonomous vehicles and instead is supporting new private insurance for autonomous vehicles to enable deployment in the real world, creating real global competition in this exciting new sector.[34] Dramatic cooperative action between nations is quickly taking shape as exemplified by transport ministers of all 28 European Union member states signing on April 14, 2016 the ‘Amsterdam Declaration’ that details steps necessary to establish rules and regulations to allow autonomous vehicles on the public roadways.[35]

Urban Transportation

After the launch of Uber in 2009 and Lyft in 2012, the growth of ride sharing applications has proliferated across the globe. There are numerous ways in which entrepreneurs are designing applications to support the tremendous need for mobility solutions in urban areas.

[33] An acronym of Light Detection And Ranging, LiDAR is a surveying technology that measures distance by illuminating a target with a laser light.

[34] James Titcomb (2015), “Google's meetings with UK Government over driverless cars revealed”, The Telegraph, available from: http://www.telegraph.co.uk/technology/2016/01/21/googles-meetings-with-uk-government-over-driverless-cars-reveale/, (accessed 4/14/16)

[35] Government of Netherlands (2016), “Europe wants to pick up the pace towards market introduction of self-driving vehicles”, available from: https://www.government.nl/latest/news/2016/04/14/europe-wants-to-pick-up-the-pace-towards-market-introduction-of-self-driving-vehicles, (accessed 4/18/16)

Historically, most governments regulated commercial vehicle for hire services at the local level. The primary policy goals often included transparent and standardized fares, licensed and safe drivers, and licensed and safe vehicles. More recently policies and regulations to ensure equitable services for the disabled, initiatives to reduce greenhouse gas emissions, and congestion pricing have been introduced in various jurisdictions. Overall, with hundreds of thousands of localities on every continent, there is currently a patchwork of fragmented policies and procedures regulating vehicle for hire services.

In spite of this fragmentation, Uber, Lyft and others have been able to grow rapidly and generate substantial revenue in developed and developing nations alike. As these new services have grown they are facing increasing opposition from existing local providers. In reaction to this opposition, some localities have banned these app-based services entirely and others are requiring onerous and inconsistent registration requirements. Beyond, the registration and licensing issues, individual safety for riders and drivers is an emerging issue. The unfortunate murder of six people by an Uber driver in Kalamazoo, Michigan, in February 2016 illustrates that there may be the need for federal or national legislation to ensure the safety of all participants in app based services.

As the ride share market becomes saturated in developed nations, large technology companies are seeking to leverage connected devices to transform logistics services especially in urban areas. From an environmental perspective fossil fueled ground transportation vehicles contributed approximately one-quarter of energy-related global greenhouse gas emissions (GHGs) and were responsible for about one-fifth of energy use.36 New technologies to better optimize last mile freight delivery in urban areas offers a unique opportunity to reduce GHGs and tap a very lucrative logistics market. New solutions for logistics may include autonomous air and ground vehicles teaming together to deliver goods in an environmentally sound, cost effective manner. As firms look at these solutions, how can government provide the proper support to enable improvements of urban areas? What standards must be put in place, what regulations need to be changed, and what agencies need to take the lead to enforce the proper rules when the convergence of new technology transforms vast sectors of the economy?

Conclusion

There are myriad policy issues related to cryptocurrencies, blockchains, autonomous vehicles, and urban transportation. Cryptocurrencies face questions around their status as a currency, asset, security or resource. This can be viewed as a national or central government issue with important international considerations in terms of harmonizing with the global financial system. Whereas automotive vehicle regulation is a federal/central, state/provincial and

[36] International Association of Public Transport (2014), Action Plan for 2014 UB Climate Change Summit, available from: http://www.un.org/climatechange/summit/wp-content/uploads/sites/2/2014/07/TRANSPORT-Action-Plan-UITC_revised.pdf, (accessed 4/18/16)

local government issue where brand new policies and procedures must be developed and implemented as the vehicle as the driver becomes a reality. Urban transportation app-based services on the other hand can be considered a local issue with logistics and vehicle for hire regulations needing to be tailored to the local community. And yet as new technology continues to converge, any rule at the local level must be suitable to offer the interoperability required of the digital economy that knows no bounds.

As governments grapple with these new innovations many are beginning to recognize the dramatic ways in which applications and solutions related to digital technologies are transforming our global economy. It will be a requirement of policy makers at all levels of government to carefully balance the competing needs of various actors to ensure that the complexities of the 21st century are properly weighted and evaluated in order to support the increasing prosperity and quality of life that these new technologies have the potential to deliver.

Appendix 1

At an international level, through the Financial Action Task Force (FATF), general definitions of cryptocurrencies and blockchains have emerged to support regulation of this new innovation. The FATF defined cryptocurrency as “a math-based, decentralised convertible virtual currency that is protected by cryptography…Hundreds of cryptocurrency specifications have been defined, mostly derived from Bitcoin, which uses a proof of work system to validate transactions and maintain the block chain.”37

As a decentralized virtual currency, cryptocurrencies are distinct from FinCEN's definition of real currency as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance.” Thus, in contrast to real currency, "virtual currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction.”38

In the United States, in March of 2014, the Internal Revenue Service (IRS) detailed “that virtual currency is treated as property for U.S. federal tax purposes.”39 General tax principles that apply to property transactions apply to transactions using virtual currency, with tax consequences on wages or capital gains or losses derived in cryptocurrencies. A payment made using virtual currency is subject to information reporting to the same extent as any other payment made in property.

[37] FATF (2014), op cit.

[38] FINCEN (2013), Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, available from: https://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html, accessed (4/14/16)

[39] IRS (2014), op cit.

The Security and Exchange Commission may consider certain activities related cryptocurrencies as the exchange of securities, which would thus fall under federal securities laws. Such activities would have to pass the 'Howey' test, which defines a security as a, "contract, transaction or scheme whereby a person [1] invests his money [2] in a common enterprise and [3] is led to expect profits [4] solely from the efforts of the promoter or a third party."40 This may be applicable to certain instances where new cryptocurrencies are created or bought/sold on online marketplaces.

Finally, the Commodity Futures Trading Commission has labeled Bitcoin, one of many cryptocurrencies, as a commodity41. This decision was based on the potential for cryptocurrencies, like Bitcoin, to fall under the broad definition of a commodity in the Commodity Exchange Act as, "all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in".

Appendix 2

The United States Department of Transportation (USDOT) National Highway Traffic Safety Administration (NHTSA) defines vehicle automation as having five levels: No-Automation (Level 0): The driver is in complete and sole control of the primary vehicle controls at all times. Function-specific Automation (Level 1): Automation at this level involves one or more specific control functions. Examples include electronic stability control or pre-charged brakes. Combined Function Automation (Level 2): This level involves automation of at least two primary control functions designed to work in unison to relieve the driver of control of those functions. An example of combined functions enabling a Level 2 system is adaptive cruise control in combination with lane centering. Limited Self-Driving Automation (Level 3): Vehicles at this level of automation enable the driver to cede full control of all safety-critical functions under certain traffic or environmental conditions and in those conditions to rely heavily on the vehicle to monitor for changes in those conditions requiring transition back to driver control. The driver is expected to be available for occasional control, but with sufficiently comfortable transition time. The Google car is an example of limited self-driving automation. Full Self-Driving Automation (Level 4): The vehicle is designed to perform all safety-critical driving functions and monitor roadway conditions for an entire trip. Such a design anticipates that the driver will provide destination or navigation input, but is not expected to be available for control at any time during the trip. This includes both occupied and unoccupied vehicles.42

[40] U.S. Supreme Court (1946), op cit.

[41] CFTC (2015), op cit.

[42] NHTSA (2013), op cit.

Panel 5: Global perspectives on open data, engagement and urban governance

By Hollie Russon Gilman

It is common nowadays to bemoan the state of our democracy: from growing citizen disaffection, to the growing influence of money in politics. The 2015 Edelman Trust Barometer shows a global decline of trust in government with numbers reaching historic lows.[43] In surveys, government dysfunction continues to surpass the economy as the problem Americans are most likely to list as the country's most serious. A recent Pew survey found that trust in government remains at historic lows. [44] Only 19% of Americans say they can trust the government always or most of the time. The majority of Americans (60%) think their government needs "major reform," in contrast to the late 1990s when less than 40 percent of those surveyed thought so. Only 20% would describe government programs as being well run and 55% of the public says that "ordinary Americans" would do a better job of solving national problems then elected officials.[45]

However, partly in response to citizens' growing disaffection, a wave of participatory policy reform has emerged in America's largest cities, capitalizing on new technology, open data and democratic experiments that aim to improve democracy.[46] Around the globe technologists, government innovators, and civil society are leveraging digital tools and open data to make governance more responsive to citizens, strengthen the relationship between citizens and their government, provide new ways for citizens to participate in decision-making in their communities, and make governments more accountable.

Civic Tech

There are many conversations concerning "civic technology," or "civic tech" and the opportunities for leveraging digital tools to benefit the public. The $6 billion civic technology is just a piece of the $25.5 billion that government spends on external information technology (IT). Government investments in civic technology can spur powerful partnerships that foster public sector innovation.[47]

There is debate about its precise definition including who is even involved in civic tech. For instance, does it include governments seeking to modernize their

[43] Edelman Trust Barometer 2015

[44] Pew Research Center, November, 2015, "Beyond Distrust: How Americans View Their Government.

[45] Ibid.

[46] See also Beth Simone Noveck (2015). *Smart citizens, smarter state: The technologies of expertise and the future of governing.* Cambridge, MA: Harvard University Press

[47] See also Hollie Russon Gilman, "The Future of Civic Technology" April 20, 15 *Brookings Institute* http://www.brookings.edu/blogs/techtank/posts/2015/04/20-civic-technology

systems or people sharing resources better? Is it about efficacy or effectiveness? Should the emphasis be on people or politics? Perhaps a definition can be expansive enough to include a variety of actors and activities.

Further, we need more examples of data and technology being used to hold government to account, better govern urban areas or increase civic engagement. This can help spur research of the subsequent outcomes – both positive and negative - in areas such as governance, healthcare and sustainable or local development? Evidence is required to generate robust and meaningful evaluations of the outcomes and success of various open data initiatives. This paper outlines four examples of data and innovation to strengthen urban governance and concludes with three key takeaways for researchers, policymakers, and practitioners.

Chicago OpenGrid

Chicago has created OpenGrid to provide an open source, situational awareness system to enable an easily accessible and centralized open source repository of public information.[48] OpenGrid reflects one of the most advanced deployments to use government data to empower citizens.[49] It reflects the latest installation in Chicago to build open source data efficiency that is scalable.[50] Their WindyCity platform integrated seven million pieces of data from city departments every day and paired it with a powerful analytics tool to create data visualization to equip managers with new insights on city operations in real time.[51] It won one million dollars from Bloomberg Philanthropies Mayor's Challenge.[52] OpenGrid reflects the latest version of open data being released to spur civic education, agency, and industry. In contrast to processes that simply release data without an engagement strategy, OpenGrid is designed for participation, collaboration, and replicability.

Participatory Budgeting

Participatory budgeting (PB) started in 1989 in Porto Alegre, Brazil, by the leftist Partido dos Trabalhadores (Workers' Party). PB gives citizens the opportunity to learn about government practices and to come together to deliberate, discuss, and substantively affect budget allocations (Shah 2007). In its original campaign

[48] See also "Chicago Tech Plan," City of Chicago http://techplan.cityofchicago.org/

[49] See Sean Thornton "Chicago Launches OpenGrid to Democratize Open Data" *Harvard Data-Smart City* Solutions, January 20, 2016 http://datasmart.ash.harvard.edu/news/article/chicago-launches-opengrid-to-democratize-open-data-778?utm_content=buffere195b&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

[50] Jason Sheuh "3 Reason's Chicago's Analytics Could be Coming to Your city" *Government Technology*, April 1, 2014 http://www.govtech.com/data/3-Reasons-Chicagos-Analytics-Could-be-Coming-to-Your-City.html

[51] "Chicago Uses MongoDB To Create A Smart and Safer City" https://www.mongodb.com/customers/city-of-chicago.

[52] Amina Elahi "Bloomberg Awards Chicago $1 M for Real-Time Analytics Platform" *Built in Chicago* March 13th, 2013. http://www.builtinchicago.org/blog/bloomberg-awards-chicago-1m-real-time-analytics-platform.

for participatory budgeting, the PT outlined four basic principles guiding PB: (1) direct citizen participation in government decision-making processes and oversight; (2) administrative and fiscal transparency as a deterrent for corruption; (3) improvements in urban infrastructure and services, especially aiding the indigent; and (4) a renewed political culture in which citizens would serve as democratic agents. Recent research convincingly demonstrates that in the last twenty years PB has enhanced the quality of democracy in Brazil and other positive outcomes linked to specific uses of PB in Brazil include increased municipal spending on sanitation and health, increased numbers of CSOs, and decreased rates of infant mortality.[53] Digital tools, including SMS, have been used for various aspects of the process including ideation, dissemination of ideas, and voting. In 2016, New York City conducted the first digital voting, with in person registration, providing an access code for people to use to vote online.

Boston New Urban Mechanics

In 2010, Boston launched the first Mayor's Office of New Urban Mechanics (MONUM) at the beginning of Mayor Menino's fifth term.[54] The office was designed to pilot experiments, and work directly with entrepreneurs, to leverage technology and innovation to improve the quality of City services and strengthen the relationship between citizens and the City for "peer-produced governance.[55]" Menino was long interested in the process of tinkering with tools, which gave him the nickname "The Urban Mechanic." Since 2010, the office quickly gained momentum, with the two co-heads receiving an award as the Public Officers of the Year by *Governing Magazine.*[56] MONUM has been recognized as a global example, including by the UK Innovation Unit NESTA and recently received $1.3 million as part of Bloomberg Philanthropies Innovation Team program to develop solutions to the middle-income housing challenge. The MONUM model has spread to Philadelphia and Salt Lake City and continues to serve as an international paradigm for cities to emulate. The success of MONUM illustrates the opportunity for digital technology to alter institutional culture to make it more amenable to experimentation and focused on residents.[57]

Rhode Island Civic Crowd Funding

Central Falls, Rhode Island is a densely populated community in a small geographic area, with Rhode's Island only majority Hispanic community. In 2011, Central Falls declared chapter 9 bankruptcy – the first time a city in Rhode Island has declared bankruptcy. In this socio-political climate, the city government decided to try something new to engage the community around a

[53] Michael Touchton and Brian Wampler, B. (2014). "Improving Social Well-Being through New Democratic Institutions." *Comparative Political Studies* 47, no. 10, pp. 1442–69.

[54] See http://newurbanmechanics.org/boston/

[55] See Ben Schreckinger "Boston: There's an Apps for That" *Politico Magazine* June 10, 2014.

[56] See Steve Goldsmith "An Old-School Mayor on the Forefront of Innovation" *Governing September 6, 2012.*

[57] See Susan Crawford and Walter (2013), "Citizen-Centered Governance: The Mayor's Office of New Urban Mechanics and the Evolution of CRM in Boston" *Harvard Berkman Center Case Study.*

shared project.[58] They partnered with Citizinvestor,[59] a crowdfunding and civic engagement that works similarly to Kickstarter for governments, to launch a civic crowdfunding campaign – one of the first in the United States. Municipalities post a project with a funding goal. Citizens donate online. If the goal is met, the municipality receives the funds minus fees. It's an all or nothing model -- in order for the entity to receive the funds, the fundraising goal must be met. Central Falls launched a Citizinvestor campaign that hit their goal of $10,044. Local residents were active participants in every part of the process; identifying the topic for fundraising, pledging their own dollars, and collaboratively designing artistic trash cans working directly with a local arts nonprofit The Steel Yard.

3 Policy Lessons: Civic Tech for More Inclusive Governance

(1) Leveraging Multi-Sector Partners

Each of the examples took advantage of talent and expertise and have partnered with external experts, such as the Citizinvestor platform itself and leveraging resources from external entities such as the Amazon Web Services in Chicago. OpenGrid has partnered with the Smart Chicago Collaborative, which is funded by the MacArthur Foundation and the Chicago Community Trust. The civic tech examples here also take advantage of University expertise. This can take the form of fellowships (e.g. MONUM), computing power (e.g. OpenGrid) or research support (PBNYC).

Policy makers can think more expansively about the resources at their disposable and structure civic tech experiments with deliberate intent to engage multi-sector stakeholders. The methods employed enable public private partnerships and create entry points for the public sector to leverage external resources.

(2) Embedding pilot programs to become institutionalized

Many of these examples moved from pilot processes to become more embedded and institutionalized structures. The Boston New Urban Mechanics were able to prototype several types of programs in a lean and agile way. Through gaining momentum and winning support from citizens, they now are being asked to solve critical problems for the city in a systematic way. PB in the United States began as a pilot with $1 Million in 2009 and now upwards of $50 Million is being allocated through the process. By starting out as small and nimble programs, many of these projects were able to take risks they otherwise would not have been able to. Importantly, this enables less pressure from the onset and the ability to think more creativity about implementation.

Policy makers can learn valuable lessons from pilot projects. The stakes are lower and they can try outreach to traditionally marginalized communities. Experiments offer an opportunity to reach citizenry in non-traditional way and

[58] See more at http://www.citizinvestor.com/project/clean-up-cf-new-bins-in-jenks-park.
[59] See http://www.citizinvestor.com/ for more information.

expand the traditional public service delivery model of citizen as only a customer. Pilots that are well structured can empower people for more inclusive decisionmaking.

(3) Learned Lessons Across Contexts

Because civic tech is not bound to one geographic region, many of these examples take a more network approach. This enables an opportunity to take lessons learned from various contexts and apply these principles. Participatory budgeting first began in the Global South and is quickly spreading across the North. Philadelphia was the first city to experiment with a Citizinvestor public funding campaign and though they did not reach their goal, valuable insights from their process directly improved the process in subsequent cities. The Chicago DoIT ensures that all the code for the city is open source and available on GitHub. Other cities, in turn, can use this code for their own public interfaces to spawn more open and democratic open data.

Policy makers can take lessons from many types of actors across diverse contexts. Best practices from global experiments can be translated to fit specific contexts and ensure local, community needs are front and center. These experiments do not need to be viewed in isolation from one another, but rather can serve as a useful petri dish to shed light on further implementations. The result can be a more expansive approach to innovation, which is inclusive of diverse cultures and backgrounds. The critical factor is applying these lessons to a context specific locality that is sensitive to the local socio-political context and environment.

Practitioner Points

- Public sector officials can leverage multi-sector partnerships to capitalize and harness the expertise of academia, civil society, industry and philanthropy to spur civic tech and data for governance.
- Creating centralized repositories of interested funders, open source digital tools, collaborations, and best practices for civic engagement can streamline multi-stakeholder partnerships in order to circumvent some of the current institutional barriers facing government officials eager to implement change.
- In order to incorporate civic tech for more inclusive governance, practitioners can start small by piloting civic tech experiments and then move to embed and institutionalize new practices into governance.
- Public officials in the United States can learn best practices from a variety of global examples. Lessons learned can be shared internationally.

Appendix 1: Full Conference Agenda

Start	End			
Monday 25 April, 2016				
8:00	9:00		**Registration & Breakfast**	
9:00	10:00		**Opening Keynotes: How Digital Technologies & Data are Changing our World** **Merit E. Janow**, Dean, Columbia SIPA (Moderator) **Arati Prabhakar**, Director, Defense Advanced Research Projects Agency **Kenneth Prewitt**, Professor and Special Advisor to the President, Columbia University	
10:00	11:15		**Panel 1: Global Security Challenges and Data: Intelligence Gathering, Encryption, and Sharing in a Time of ISIS** **Laura DeNardis**, Professor, American University (Moderator) **Steve Bellovin**, Professor, School of Engineering, Columbia University **Alan Butler**, Senior Counsel, Electronic Privacy Information Center **David Omand**, Visiting Professor, King's College London	
11:15	11:30		Coffee Break	
11:30	12:30		**Panel 2: National Data Governance in a Global Economy** **Merit Janow**, Dean, Columbia SIPA (Moderator) **Usman Ahmed**, Adjunct Professor of Law, Georgetown Law **Anupam Chander**, Professor, UC Davis Law School **Gordon Goldstein**, Managing Director, Silverlake Partners **Mark Wu**, Assistant Professor, Harvard Law School	
12:30	1:15		Lunch	
1:15	2:00		**Lunch Keynote: The Future of Digital Technologies for International Affairs** **Laura DeNardis**, Professor, American University (Moderator) **Dian Triansyah Djani**, Permanent Representative of the Republic of Indonesia to the United Nations **Daniel Sepulveda**, Deputy Assistant Secretary, Bureau of Economic and Business Affairs, U.S. Department of State	
2:00	2:15		Coffee Break	
2:15	3:15		**Panel 3A: Potential and Pitfalls of an Algorithmic Society** **David Madigan**, Professor and Executive Vice President, Columbia University (Moderator) **Solon Boracas**, Postdoctoral Research Associate, Center for Information Technology Policy, Princeton University	**Panel 3B: Cyber Conflict: Prevention, Stability and Control** **Jay Healey**, Senior Research Scholar, Columbia SIPA (Moderator) **Fred Kaplan**, Columnist, Slate **Angela McKay**, Director of Cyber Security Strategy, Microsoft

			Roxana Geambasu, Assistant Professor, Dept. of Computer Science and Data Sciences Institute, Columbia University **Bernard Harcourt**, Professor, Columbia Law School **Frank Pasquale**, Professor, University of Maryland	
3:15	4:15		**Panel 4A: Massive Data Collection and Automation: Preserving Individuals' Rights** **Anya Schiffrin**, Lecturer, Columbia SIPA (Moderator) **Joseph Cannataci**, UN Special Rapporteur for Privacy **Ashkan Soltani**, former Chief Technologist, Federal Trade Commission **Alexis Wichowski**, Adjunct Professor, Columbia SIPA	**Panel 4B: On Notice: The Coming Transformation of Key Economic Sectors** **Vikram Pandit**, Founding Principal, The Orogen Group (Moderator) **Daniel Gallancy**, CEO, SolidX Partners **Eli Noam**, Professor, Columbia Business School **Andrew Saltzberg**, Global Mobility Policy Lead, Uber **Joah Sapphire**, Adjunct Professor, Columbia SIPA
4:15	4:30		Coffee Break	
4:30	5:30		**Panel 5: Civic Entrepreneurs: Global Perspectives on Open Data, Engagement and Urban Governance** **Hollie Russon Gilman**, Post-Doctoral Fellow for Technology and Public Policy, Columbia SIPA (Moderator) **Ania Calderón**, General Director, Open Data, Office of the President, Republic of Mexico **Michael Mattmiller**, CTO, City of Seattle **Cathy Wissink**, Senior Director, Technology and Civic Engagement, Microsoft	
5:30	6:00		Break	
6:00	7:00		Cocktail Reception (by invitation)	
7:00	9:00		**Dinner w/ Keynote (by invitation)** **Elliot Schrage,** Vice President of Global Communications, Marketing and Public Policy, Facebook **David Kirkpatrick**, CEO, Techonomy (Discussant) **Merit E. Janow**, Dean, SIPA, Columbia University (Moderator)	

Appendix 2: Speaker Bios

OPENING KEYNOTE DISCUSSION: HOW DIGITAL TECHNOLOGIES & DATA ARE CHANGING OUR WORLD

Moderator: ***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 1994. She was appointed Dean of the Faculty in 2013. She teaches at SIPA and Columbia Law School. In December 2003, Professor 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). Professor 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. She has a JD from Columbia Law School, where she was a Stone Scholar, and a BA in Asian Studies with honors from the University of Michigan.

Arati Prabhakar, *Director, Defense Advanced Research Projects Agency (DARPA)*

DARPA's director since 2012, Arati Prabhakar has spent her career investing in world-class engineers and scientists to create new technologies and businesses. She first came to DARPA in 1986 as a program manager and was the founding director of the Agency's Microelectronics Technology Office. Arati served as director of the National Institute of Standards and Technology from 1993 to 1997. She then spent 15 years in Silicon Valley, including a decade as a partner at U.S. Venture Partners, an early-stage venture capital firm. Arati is a member of the National Academy of Engineering and an Institute of Electrical and Electronics Engineers (IEEE) Fellow. She received her PhD in applied physics and MS in electrical engineering from the California Institute of Technology and her BS in electrical engineering from Texas Tech University.

Kenneth Prewitt, *Carnegie Professor of Public Affairs, SIPA, Columbia University*

Kenneth Prewitt is the Carnegie Professor of Public Affairs and the vice president for Global Centers. He taught political science at the University of Chicago from 1965 to 1982, and for shorter stints was on the faculty of Stanford University, Washington University, the University of Nairobi, Makerere University, and the Graduate Faculty at the New School University (where he was also dean). Prewitt's professional career has also included serving as director of the United States Census Bureau, director of the National Opinion Research Center, president of the Social Science Research Council, and senior vice president of the Rockefeller Foundation. He is a fellow of the American Academy of Arts and Sciences, the American Academy of Political and Social Science, the American Association for the Advancement of Science, the Center for the Advanced Study in the Behavioral Sciences, and the Russell-Sage Foundation; and a member of other professional associations, including the Council on Foreign Relations. Among his awards are a Guggenheim Fellowship; honorary degrees from Carnegie Mellon and Southern Methodist University; a Distinguished Service Award from the New School for Social Research; the Officer's Cross of the Order of Merit from the Federal Republic of Germany; the Charles E. Merriam Lifetime Career Award, American Political Science Association; and Lifetime National Associate of the NRC/NAS.

Prewitt holds a BA from Southern Methodist University (1958); MA from Washington University (1959), and Harvard Divinity School (1960) as a Danforth fellow; and PhD from Stanford University (1963).

PANEL 1: GLOBAL SECURITY CHALLENGES AND DATA: INTELLIGENCE GATHERING, ENCRYPTION, AND SHARING IN A WORLD OF ISIS

Moderator: ***Laura DeNardis,*** *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, DC. 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.

Steven Bellovin, *Professor, 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 works 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.

Alan Butler, *Senior Counsel, Electronic Privacy Information Center*

Alan Butler is Senior Counsel at the Electronic Privacy Information Center (EPIC) in Washington, DC. In that capacity, Mr. Butler manages EPIC's appellate litigation, including the Amicus Program, and files briefs in emerging privacy and civil liberties cases before the U.S. Supreme Court and other appellate courts. Mr. Butler has argued on behalf of EPIC in privacy and open government cases. He has authored briefs on national security, open government, workplace privacy, and consumer privacy issues. He has also published articles on emerging privacy issues in the Duke Journal of Constitutional Law and Public Policy, the New England Law Review, and the American University Law Review.

David Omand, *Visiting Professor, King's College London*

Sir David Omand GCB is visiting professor in the War Studies Department, King's College London, and at Sciences-Po in Paris. He was appointed in 2002 as the first U.K. security and intelligence coordinator, having previously been permanent secretary of the Home Office 1997–2001 and, before that, director of GCHQ, the United Kingdom's signals intelligence and cybersecurity organization. Previously, in the Ministry of Defence, he served as deputy under secretary of state for policy. He served for seven years on the U.K. Joint Intelligence Committee. He is the senior independent director of Babcock International Group plc and is on the senior advisory board of Paladin Capital. His book, *Securing the State,* was published in paperback by Hurst in 2011 (available in a Kindle edition).

PANEL 2: NATIONAL DATA GOVERNANCE IN A GLOBAL ECONOMY

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

See opening keynote discussion for full bio.

Usman Ahmed, *Head of Global Public Policy, PayPal Inc.*

Usman Ahmed is the head of global public policy at PayPal Inc. His work covers a variety of global issues including financial services regulation, innovation, international trade, and entrepreneurship. He has given talks on these subjects at conferences and universities around the world and has published in the *World Economic Forum Global Information Technology Report, Journal of World Trade,* and the *Michigan Journal of International Law.* Ahmed is also an adjunct professor of law at Georgetown University Law School, where he teaches courses on international law and policy issues related to the Internet. Prior to PayPal, Usman worked at a number of policy think tanks in the Washington, DC, area focusing on good governance issues. Ahmed earned his JD from University of Michigan, his MA from Georgetown University's School of Foreign Service, and his BA from University of Maryland.

Anupam Chander, *Professor, UC 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.

Gordon Goldstein, *Managing Director, Silver Lake Partners; Adjunct Senior Fellow, Council on Foreign Relations*

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.

Mark Wu, *Assistant Professor, Harvard Law School*

Mark Wu is an assistant professor of Law at Harvard Law School, where he teaches international trade and inter- national economic law. Previously, he served as the director for intellectual property in the Office of the U.S. Trade

Representative, where he was the lead U.S. negotiator for the IP chapters of several free trade agreements. He also worked as an engagement manager for McKinsey & Co., where he focused on high-tech companies. He began his career as an economist and operations officer for the World Bank in China, working on environmental, urban development, health, and rural poverty issues. He has also served as an economist for the United Nations Development Programme in Namibia. After earning a JD from Yale Law School, he clerked for Judge Pierre Leval on the U.S. Court of Appeals for the Second Circuit and was an academic fellow at Columbia Law School. He received his MSc in development economics from Oxford University, which he attended on a Rhodes Scholarship, and his AB summa cum laude in social studies and East Asian studies from Harvard University.

LUNCH KEYNOTE: THE FUTURE OF DIGITAL TECHNOLOGIES FOR INTERNATIONAL AFFAIRS

Moderator: ***Laura DeNardis,*** *Professor, American University*

See panel 1 for full bio.

Dian Triansyah Djani, Ambassador/Permanent Representative, Permanent Mission of the Republic of Indonesia to the United Nations

His Excellency Dian Triansyah Djani is the ambassador/permanent representative of the Republic of Indonesia to the United Nations in New York. Prior to his current post, he was the director general for America and Europe as well as director general for ASEAN of the Ministry of Foreign Affairs; and head of delegation/ambassador/permanent representative of Indonesia to the UN, WTO, and other international organizations in Geneva.

Throughout his career, he has represented Indonesia in various UN organizations, APEC, ASEAN, WTO, FEALAC, ASEM, etc. Since 2014, he is a commissioner on the Global Commission on Internet Governance. Mr. Djani graduated from the University of Indonesia and Vanderbilt University. He is a guest lecturer at various higher learning institutions on multilateral negotiations and political and security, as well as international trade/ economic, issues, both in Indonesia and abroad.

Daniel Sepulveda, Ambassador and Deputy Assistant Secretary, U.S. State Department

Ambassador Daniel A. Sepulveda currently serves as deputy assistant secretary of state and U.S. coordinator for international communications and information policy. Prior to joining the State Department, Mr. Sepulveda served for more than a decade in the Senate advising Senators Barbara Boxer, Barack Obama, and John Kerry. Sepulveda also worked in the Clinton administration at the Department of Labor and during the first term of the Obama administration as an assistant U.S. trade representative leading a team that managed relations with Congress.

Additional prior work experience includes service advocacy at the nation's largest Latino organization, the National Council of La Raza (NCLR).

Mr. Sepulveda received a Master of Public Affairs from the LBJ School of Public Affairs at the University of Texas at Austin as a Woodrow Wilson Fellow in Public Policy and International Affairs. He received a Bachelor of Arts in political science and history from Emory University.

PANEL 3A: THE POTENTIAL AND PITFALLS OF AN ALGORITHMIC SOCIETY

Moderator: *David Madigan,* *Executive Vice President and Dean of Faculty of Arts and Sciences, and Professor of Statistics, Columbia University*

David Madigan serves as the ninth executive vice president for the Arts and Sciences and dean of the faculty, a position he assumed on September 3, 2013. Since March 2013, he had served as the interim executive vice president. He is a professor of statistics at Columbia University, and served as the department chair from 2007 to 2013. Before coming to Columbia in 2007, Professor Madigan was dean of physical and mathematical sciences at Rutgers University. He is a fellow of the American Statistical Association, the Institute of Mathematical Statistics, and the American Association for the Advancement of Science. He received a bachelor’s degree in mathematical sciences and a PhD in statistics, both from Trinity College Dublin. He has previously worked for AT&T Inc., Soliloquy Inc., the University of Washington, Rutgers University, and SkillSoft, Inc. He has over 150 publications in such areas as Bayesian statistics, text mining, Monte Carlo methods, pharmacovigilance, and probabilistic graphical models. He recently completed a term as editor-in-chief of Statistical Science and is the current editor of *Statistical Analysis and Data Mining.*

Solon Barocas, *Postdoctoral Research Associate, Center for Information Technology Policy, Princeton University*

Solon Barocas is a postdoctoral research associate at the Center for Information Technology Policy at Princeton University. His research explores issues of fairness in machine learning, methods for bringing accountability to automated decisions, the privacy implications of inference, and the role that privacy plays in mitigating economic inequality. Solon completed his doctorate in the Department of Media, Culture, and Communication at New York University, where he remains an affiliate of the Information Law Institute. He also works with the Data & Society Research Institute and serves on the National Science Foundation–sponsored Council for Big Data, Ethics, and Society.

Roxana Geambasu, *Assistant Professor of Computer Science, School of Engineering and Data Science Institute, Columbia University*

Roxana Geambasu is an assistant professor of computer science at Columbia University. She joined Columbia in fall 2011 after finishing her PhD at the University of Washington. For her work in cloud and mobile data privacy, she received an Alfred P. Sloan Faculty Fellowship, a Microsoft Research Faculty Fellowship, a 2014 “Brilliant 10” *Popular Science* nomination, an NSF CAREER award, an Early Career Award in Cybersecurity from the University of Washington Center for Academic Excellence, an Honorable Mention for the 2013 inaugural Dennis M. Ritchie Doctoral Dissertation Award, a William Chan Dissertation Award, two best paper awards at top systems conferences, and the first Google PhD Fellowship in Cloud Computing.

Bernard Harcourt, *Professor, Columbia Law School*

Bernard E. Harcourt is a contemporary critical theorist and writes in the fields of punishment and political theory. He is the author, most recently, of *Exposed: Desire and Disobedience in the Digital Age* (Harvard, 2015) and *The Illusion of Free Markets: Punishment and the Myth of Natural Order* (Harvard, 2011). He is also the editor of several of Michel Foucault’s lectures at the Collège de France, including *La Société punitive* (Gallimard, 2013) and *Theories et institutions pénales* (Gallimard, 2015).

Harcourt is the Isidor and Seville Sulzbacher Professor of Law at Columbia University, the founding director of the Columbia Center for Contemporary Critical Thought, and *directeur d’études* (chaired professor) at the *École des Hautes Études en Sciences Sociales* in Paris. He moved to Columbia from the University of Chicago in 2014, where he was the chairman of the political science department and Julius Kreeger Professor of Law and Political Science.

Harcourt earned his bachelor’s degree in political theory at Princeton University, his law degree at Harvard Law School, and his PhD in political science at Harvard University. After law school, he clerked for the Honorable Charles S. Haight Jr. of the U.S. District Court for the Southern District of New York and then worked as an attorney at the Equal Justice Initiative in Montgomery, Alabama, representing death row inmates. Harcourt continues to represent death row inmates pro bono and has also served on human rights missions in South Africa and Guatemala.

Frank Pasquale, *Professor, University of Maryland*

Frank Pasquale, JD, MPhil, is an expert on the law of big data, predictive analytics, artificial intelligence, and algorithms. His scholarship and public speaking translates complex law and policy into accessible writing and presentations. He has advised business and government leaders in the health care, Internet, and finance industries, including the U.S. Department of Health and Human Services, the U.S. House Judiciary Committee, the Federal Trade Commission, and the European Commission. Routinely quoted in top global media outlets, including the *Financial Times,* the *New York Times,* and the *Economist,* he is the author of *The Black Box Society* (Harvard University Press, 2015) and a member of the Council on Big Data, Ethics, and Society.

He has been named to the advisory boards of the Electronic Privacy Information Center, the Data Competition Institute, Patient Privacy Rights, and the *Journal of Legal Education.*

He has blogged at *Concurring Opinions* since 2006. His popular writing has been published by the *New York Times, Los Angeles Times, Chronicle of Higher Education, Boston Review,* and many other media outlets.

PANEL 3B: CYBER CONFLICT: PREVENTION, STABILITY, AND CONTROL

Moderator: *Jay Healey,* *Senior Research Scholar, SIPA, Columbia University*

Jay Healey is a senior research scholar at Columbia University’s School for International and Public Affairs specializing in cyber conflict, competition and cooperation. Prior to this, he was the founding director of the Cyber Statecraft Initiative of the Atlantic Council, where he remains a senior fellow. He is the editor of the first history of conflict in cyberspace, *A Fierce Domain: Cyber Conflict, 1986 to 2012,* and has unique experience working on issues of cyber conflict and security spanning nearly twenty years across the public and private sectors. As director for cyber infrastructure protection at the White House from 2003 to 2005, he helped advise the president and coordinated U.S. efforts to secure U.S. cyberspace and critical infrastructure. He has worked twice for Goldman Sachs: first to anchor their team for responding to cyber attacks; and later in Hong Kong to manage Asia-wide business continuity and create the bank’s regional crisis management capabilities to respond to earthquakes, tsunamis, or terrorist attacks. Immediately after the 9/11 attacks, his efforts as vice chairman of the Financial Services Information Sharing and Analysis Center created bonds between the finance sector and government that remain strong today.

Angela McKay, *Director of the Government Security Policy and Strategy Team within Trustworthy Computing, Microsoft*

Angela McKay is director of the Government Security Policy and Strategy team within Trustworthy Computing at Microsoft. Ms. McKay leads Microsoft's public policy work on cybersecurity, cloud security, and norms, and on public sector use of the cloud. Her team includes professionals working on these topics across Africa, Asia, Europe, Latin America, and the United States.

Ms. McKay serves on the Board of Councilors for the EastWest Institute and as Microsoft's point of contact for the president's National Security Telecommunications Advisory Committee.

Before joining Microsoft in 2008, she worked at Booz Allen Hamilton and at BellSouth Telecommunications. Ms. McKay holds a bachelor's of industrial and systems engineering from the Georgia Institute of Technology.

Fred Kaplan, *Columnist,* Slate

Fred Kaplan is the national security columnist for *Slate* and author of *Dark Territory: The Secret History of Cyber War* (Simon & Schuster, 2016). A former fellow at the Council on Foreign Relations and the New America Foundation, as well as a former Pulitzer Prize–winning journalist at the *Boston Globe,* he has also written four other books: *The Insurgents: David Petraeus and the Plot to Change the American Way of War* (a Pulitzer Prize Finalist); *1959: The Year Everything Changed; Daydream Believers: How a Few Grand Ideas Wrecked American Power;* and *The Wizards of Armageddon.* He has a BA from Oberlin College and a PhD in political science from MIT.

PANEL 4A: MASSIVE DATA COLLECTION AND AUTOMATION: PRESERVING INDIVIDUALS' RIGHTS

Moderator: ***Anya Schiffrin,*** *Lecturer in Discipline of International and Public Affairs, SIPA, Columbia University*

Anya Schiffrin is the director of the International Media, Advocacy, and Communications specialization at Columbia University's School of International 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 most recent book is *Global Muckraking: 100 Years of Investigative Reporting from Around the World* (New Press, 2014).

Joseph Cannataci, *Special Rapporteur on the Right to Privacy, United Nations Human Rights Council*

Professor Joseph A. Cannataci is head of the Department of Information Policy & Governance at the Faculty of Media & Knowledge Sciences of the University of Malta. He is also a full professor, holding the chair of European Information Policy & Technology within the Faculty of Law, at the University of Groningen, The Netherlands, where he cofounded the STeP Research Group. Additionally, he has been adjunct professor at the Security Research Institute and School of Computer and Security Science, Edith Cowan University Australia, and scientific coordinator of multiple EU FP7 and H2020 research projects focusing on privacy. He was appointed special rapporteur on the right to privacy by the United Nations Human Rights Council in July 2015. His latest book, *The Individual and Privacy,* was published by Ashgate in March 2015.

Ashkan Soltani, *Former Chief Technologist, Federal Trade Commission (FTC)*

Ashkan Soltani is an independent researcher and technologist specializing in privacy, security, and behavioral economics. His work draws attention to privacy problems online, demystifies technology for the nontechnically inclined, and provides data-driven insights to help inform policy.

He’s previously served a brief stint as a senior advisor to the U.S. chief technology officer in the White House Office of Science and Technology Policy and as the chief technologist for the Federal Trade Commission, advising the commission on its technology-related policy as well as helping to create its new Office of Technology Research and Investigation. He also served at the FTC in 2010 as one of the first staff technologists in the Division of Privacy and Identity Protection, helping to lead investigations into major technology companies such as Google, Facebook, Twitter, HTC, and PulsePoint.

Ashkan was recognized as part of the 2014 Pulitzer-winning team for his contributions to the *Washington Post*’s coverage of National Security issues. He was also the primary technical consultant on the *Wall Street Journal*’s investigative series “What They Know,” which was a finalist for the 2012 Pulitzer Prize for Explanatory Reporting.

Alexis Wichowski, *Adjunct Professor, Columbia SIPA*

Alexis Wichowski teaches in Columbia SIPA's Technology, Media, & Communications specialization. Her course "E-Government & Digital Diplomacy" won one of SIPA's "Top Five Course" awards out of almost 200 courses. She also teaches "Technology, National Security & The Citizen," exploring how technology affects power dynamics between governments, citizens, and non-state actors. Previously, Wichowski served as Director of Research at Harmony Institute, a *Buzzfeed*-founded think-tank exploring media impact; Director of Media Analysis & Strategy at the US mission to the UN; Presidential Management Fellow at the State Department's Office of eDiplomacy; and Disaster Relief Field Representative for the Red Cross (NY). Wichowski holds a PhD in Information Science (University at Albany) and a BA in Chinese (Connecticut College).

PANEL 4B: ON NOTICE: THE COMING TRANSFORMATION OF KEY ECONOMIC SECTORS

Moderator: ***Vikram S. Pandit,*** *Founding Principal, The Orogen Group*

Vikram Pandit is the founding principal of The Orogen Group, a platform that identifies and leverages investment opportunities created by the rearchitecture of financial services.

He joined Morgan Stanley in 1983 and ultimately became president and COO of its institutional securities and investment banking businesses. He left Morgan Stanley to found Old Lane, LP, which was acquired by Citigroup in 2007. He eventually became CEO of Citigroup and successfully recapitalized, restructured, and revitalized the company before he left in October 2012.

Mr. Pandit is a member of the board of directors of Bombardier Inc. and is chairman of TGG Group. He earned BS and MS degrees in engineering from Columbia University and received his PhD in finance from Columbia in 1986.

Daniel Gallancy, *CEO, SolidX Partners*

Daniel H. Gallancy is the CEO and a founding member of SolidX Partners Inc., which delivers blockchain-based software for identity management, records administration and asset transfer.

Beyond software development, SolidX provides blockchain-related consulting services, including advisory work for private corporations, investment management firms, central counterparties, and US State and Federal regulators. SolidX has partnered with McKinsey & Company and The Boston Consulting Group on various consulting engagements.

Mr. Gallancy has worked on several blockchain-related private investments and projects. He speaks regularly on the topic of blockchain technology. Recent conference and speaking topics include: "The Economic Impact of the Blockchain for Institutional Investors," "Blockchain-based Anti-Money Laundering Strategies and Tactics," "Resource Scarcity and Certainty-as-a-Service within the

Blockchain," and "The Blockchain as a Secure Record Keeping and Settlement System."

Prior to founding SolidX Partners Inc., Mr. Gallancy spent ten years in the asset management industry. Mr. Gallancy was an investment professional at Beaconlight Capital and, before that, at Alson Capital Management. Mr. Gallancy's areas of focus included semiconductors, semiconductor capital equipment, IT hardware, software and telecommunications. Mr. Gallancy was responsible for corporate diligence, financial analysis and investment decision-making.

Mr. Gallancy earned an MBA from Columbia Business School and holds a BA in Physics and a BSE in Electrical Engineering from the University of Pennsylvania. Mr. Gallancy is a CFA Charterholder.

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 is the director of the Columbia Institute for Tele-Information, a research center focusing on management and policy issues in communications, Internet, and media. Noam has published 30 books and over 300 articles. Recent books and projects include *Who Owns the World's Media* (Oxford); *Media Management* (three volumes, forthcoming); and the project *A National Initiative for Next Generation Video.*

Noam's advisory board memberships have included the federal government's telecommunications network, the Nexus Mundi Foundation (chairman), the Electronic Privacy Information Center, Oxford Internet Institute, Jones International University, and several committees of the National Research Council. 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 Aix-la-Provence (2008).

Andrew Saltzberg, *Global Mobility Policy Lead, Uber*

As Uber's Global Mobility Policy Lead, Andrew focuses on making Uber an integral part of the future of urban transportation through research, partnerships, and policy development. He joined Uber in 2013 and became the Senior Operations Manager for New York City, Uber's largest global market, before joining the global policy team. Prior to joining Uber, Andrew worked at the World Bank supporting public transportation investment projects in East Asia. He holds a bachelor of civil engineering degree from McGill University and Master in Urban Planning degree from Harvard University.

Joah Sapphire, *Adjunct Professor, SIPA, Columbia University*

Joah Sapphire leads Internet of Things solutions in highly regulated industries, leveraging twenty years of experience in the public and private sectors. Joah is founder and president of Global Dynamic Group, LLC. Previously, he was founding partner of Verulam LLC, China representative of Ospraie Management, CFO of NROTB, deputy commissioner of Suffolk County, finance director of Nassau County, and senior analyst in New York State Assembly.

Joah serves as adjunct professor for Columbia University's School of International and Public Affairs. He is an industry affiliate of Cornell University's Program in Infrastructure Policy and a member of the Advisory Board of University at Buffalo's Institute for Sustainable Transportation and Logistics. He received a BS from Cornell University and an MPA from Columbia University.

PANEL 5: CIVIC ENTREPRENEURS: GLOBAL PERSPECTIVES ON OPEN DATA, ENGAGEMENT, AND URBAN GOVERNANCE

Moderator: ***Hollie Russon Gilman,*** *Fellow in Technology and Public Policy, SIPA, Columbia University*

Hollie Russon Gilman is a postdoctoral research scholar at SIPA and fellow in Technology and Public Policy. In spring 2016, Hollie is co-teaching Technology and the Future of Governance and Public Policy. Dr. Gilman most recently served as open government and innovation advisor in the White House Office of Science and Technology Policy. Dr. Gilman recently published *Democracy Reinvented: Participatory Budgeting and Civic Innovation in America* as part of Harvard Kennedy School's series on Innovative Government. She holds a PhD and MA from the Department of Government at Harvard University and an AB from the University of Chicago with highest honors in political science.

Ania Calderón, *General Director of Open Data, Office of the President, Mexico*

Ania Calderón is the general director of open data at the Coordination of National Digital Strategy in the Office of the President of Mexico, where she leads the Open Data, Data for Development, Digital Inclusion, and Innovation for Resilience initiatives. She holds a master's degree in public administration from Columbia University's School of International and Public Affairs, with a specialization in Urban Policy and International Media Advocacy and Information and Communication Technologies, and obtained the Fulbright-García Robles Fellowship. She was part of the Digital Government Delegation of the Transition Team of the president-elect (2012–2018) of Mexico. Before this, Ania was cofounder of Pase Usted AC, a nonprofit organization focused on creating platforms to promote citizen engagement around the public agenda of Mexico City. She directed the program Genera, “technology for the city,” an incubator of digital innovation projects that seek to improve the quality of urban life.

Michael Mattmiller, *Chief Technology Officer and Director of the Department of Information Technology, City of Seattle*

Michael Mattmiller is the chief technology officer and director of the Department of Information Technology for the City of Seattle. In this role, Michael is responsible for connecting the City to the public, providing the City’s workforce with productivity-enhancing technology solutions, and ensuring the public can equitably participate in the City’s high- tech economy. Since joining the City in 2014, Michael has focused on delivering solutions that optimize the City’s use of technology resources, build trust in how the City uses the public’s information, and increase the availability of gigabit broadband service to homes and businesses throughout Seattle.

Prior to his work at the City, Michael was a senior strategist at Microsoft, focused on data privacy and protection practices across the company’s enterprise cloud solutions, and a consultant with PricewaterhouseCoopers.

Cathy Wissink, *Senior Director of Technology & Civic Engagement, Microsoft New England*

Cathy Wissink is senior director of Technology & Civic Engagement at Microsoft New England. Her job focuses on partnering with civic leaders in greater Boston to use technology to solve large challenges and capitalize on impactful and inclusive opportunities. Cathy works directly with local tech leaders and policy influencers on issues critical to both Microsoft and the tech sector. She also plays a key role in overseeing the Microsoft Innovation & Policy Center – New England. A 20-plus-year veteran of the tech industry, Cathy joined Microsoft in 2000 and spent her first nine years working on Windows, focusing on software globalization and helping ensure diverse countries were on the right side of the digital divide. She moved to the Legal and Corporate Affairs team at Microsoft in 2009, working on global government affairs, and then took her current role in Cambridge in October 2013.