COLUMBIA | SIPA
School of International and Public Affairs

A Fragmented Internet?

PROCEEDINGS OF
The 2017 Global Digital Futures Forum

May 5, 2017
Italian Academy

Microsoft
WEBCAST BY Internet Society NORTH AMERICA
CITI | Columbia Institute for Tele-Information
COLUMBIA UNIVERSITY Data Science Institute
Carnegie CORPORATION OF NEW YORK
TOW CENTER FOR DIGITAL JOURNALISM

WELCOME

The third annual Global Digital Futures Forum, convened by the Columbia University School of International and Public Affairs (SIPA) on May 5, 2017, in New York City, explored the dynamic tension between internet fragmentation and globalization.

This year's conference, "A Fragmented Internet?," brought together more than 200 scholars, practitioners, legal experts, technologists, policymakers, and entrepreneurs to discuss the potential harms and benefits of an internet that is increasingly splintered across social, business, geopolitical, technological, and economic dimensions.

The following documents comprise the proceedings of the conference, as well as breakthrough papers contributed by experts to inform the discussion. They address the effects of fragmentation upon global governance, international trade, trust and assurance, global platforms and international development, cyber conflict and democracy, the digital economy, and financial systemic risk.

The Forum is a project of SIPA's Global Digital Futures Initiative. Now in its fourth year, the initiative seeks to engage fundamental issues around the advent of new technology and its impact on society, to anticipate and examine digital public policy problems, and to formulate innovative solutions, with a focus on cyber security, internet governance, and the digital economy. Through this initiative, SIPA intends to bridge the gap between academics and policymakers and support the next generation of scholars producing interdisciplinary research.

We hope these proceedings, prepared by graduate students and young scholars, will stimulate thought and provide a basis for further discussion and action on this complex and evolving subject. We thank Carnegie Corporation of New York, Microsoft Corporation, and a number of Columbia University Institutes, including the Columbia Institute for Tele-Information at Columbia Business School, Columbia Data Science Institute, Tow Center for Digital Journalism for their support, guidance, and involvement in this year's forum, and the Internet Society for its help in livestreaming the conference. For further information, please visit https://sipa.columbia.edu/ideas-lab/techpolicy.

Sincerely yours,

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

TABLE OF CONTENTS

Part I: Proceedings

Part II: Framing Papers

TABLE OF CONTENTS

PART I: PROCEEDINGS

What Would Internet Fragmentation Mean for the Digital Economy?

Merit E. Janow, Moderator
Dean, Columbia SIPA

Eli Noam
Professor, Columbia Business School

William Drake
International Fellow and Lecturer, University of Zurich

Niloofar Howe
SVP Strategy & Operations, RSA

Rapporteurs: Fernanda Ribeiro Rosa and Anna Wennakoski

The opening discussion of the 2017 Global Digital Futures Forum introduced a key theme of the conference: the dynamic tension between internet fragmentation and globalization.

Dean Janow opened the forum by observing that the ubiquity of digital interconnection is "very much changing our world." In developed and developing countries, for businesses of all sizes, it has created dynamic opportunities for innovation, problem-solving, and commerce, as well as new risks. We have not yet established a full empirical understanding of the scale and consequences of the digital economy or its impact across major sectors, including healthcare, finance, construction, architecture, design, and the automotive sector. And, as Janow noted, the combination of technology and globalization has created "something of a political backlash" in the US and around the world, perhaps contributing to the rise of new barriers and more fragmented networks.

1. ON TERMINOLOGY

The discussion commenced with an evaluation of how to appropriately define "internet fragmentation." William Drake would reserve the term for situations in which different actors, including governments and companies, impose restrictions on the internet, limiting access to knowledge. Because such restrictions inevitably occur, "fragmentation" in this sense is a systemic property of the internet. However, levels of fragmentation should be monitored to prevent them from reaching "a broader structural, permanent, divisive point that is blocking a lot of people's ability to use the net." Commonly cited examples of fragmentation, such as variations in national regulatory environments and online linguistic diversity, would not fit under this definition.

Niloofar Howe agreed that impediments to internet access can be damaging. From a human rights perspective, an unfettered internet helps empower minorities and the disadvantaged and extend education. But at the same time, the tethering of private life, commerce, and governance to the internet makes intermediaries crucial to ensuring security and privacy. The question, "what is the appropriate level of national sovereignty?" cannot be dismissed, especially since "certain geographies absorb the pain and certain geographies benefit from for example criminal activity online." It's estimated that by 2019, over two trillion dollars will be lost to data breaches, with a disproportionate percentage coming from the US. Howe emphasized that, given the structural disadvantage regulators must overcome and the lack of enforcement for online crimes, there is an urgent need for governance that protects privacy and security without infringing on freedom.

Eli Noam questioned the use of the term "fragmentation" at all, especially given the anxiety it often provokes. This anxiety is a symptom of the internet "moving from audacity to orthodoxy," with a conservative


William Drake

enshrining of accepted models and values at the expense of future innovation. Noam sees fragmentation as not just inevitable but beneficial, in fact suggesting to the internet: "go disrupt yourself!" He predicted that this breakdown will occur along industry and technological, rather than national, lines, to create "super-across-country type arrangements that will interconnect." These arrangements will create a more efficient internet and foster progress, especially for American industry, leading the private sector to embrace the new models.

2. ON LEVELS OF REGULATION

The panelists offered nuanced perspectives on regulation. While they agreed that full harmonization was neither achievable nor desirable, important divergences emerged.

Eli Noam

Howe explained that a segment of the private sector would prefer less regulation and more opportunities for consumers to determine what services and platforms succeed in the market. From this perspective, the internet evolved from its initial uses into its current, ubiquitous form due in part to the absence of regulation. Regulation, then, is considered a barrier to businesses and industrial innovation.

Noam presented the counterargument that, rather than imposing barriers to innovation, regulation at times creates conditions for more dynamic competition. Several factors, including "network effects," make it difficult both for consumers to switch service providers and for companies to evolve from start-ups into large players in the internet ecosystem. Making it easier for new companies to enter the market and for consumers to switch from one platform to another may then be a public policy concern.

Drake highlighted the way in which the costs of data portability can constrain consumer choice. He also expressed concern that the primacy of the advertisement-based business model exacerbates some forms of inequality and makes it nearly impossible for companies that follow different models to compete. As a middle-ground solution, Drake suggested encouraging mechanisms that would allow platforms to engage with communities. In this way, companies could practice more "socially constructive thinking and planning" and contribute to broader development.

3. ON GOVERNANCE MODELS

The panelists also addressed the tension between the global reach of the internet and the sovereign decisions of states, along with the challenges this tension creates. For Howe, while rules at the national level might sometimes appear adequate, variations in social norms from one country to another complicate the creation of international governance models. She also noted the challenges that arise when governments must address pressing policy issues that fall in areas generally managed through industry self-regulation.


Niloofar Howe

Noam, in turn, argued that while the information and communications technology industry is growing at an exponential rate, government is becoming slower. As a result, openness and transparency comes at the cost of delaying the decision-making process. He suggested that this tension is insoluble, and that the best we can hope for is "partial solutions to partial problems in partial regions of the world."

Finally, Drake advocated for the multi-stakeholder model as a possible solution for the global governance challenge. As an example, he cited the Internet Corporation for Assigned Names and Numbers (ICANN), in which different parties work "side-by-side," independent of traditional forms of governance, in their search for solutions. He stressed the importance of "making sure that policy processes are not captured by the most powerful," and anticipated that decision-making will continue to be distributed geographically, with both successes and failures.

What Would Internet Fragmentation Mean for Global Governance?

Gordon Goldstein, Moderator
Managing Director, Silver Lake Partners

Ambassador Lana Nusseibeh
Permanent Representative of the UAE to the UN

Joseph Nye
University Distinguished Service Professor, Harvard University

Rapporteurs: Trey Herr and Sarah Myers West

This framing conversation revealed that hard fragmentation of the internet into truly disconnected networks is still a distant threat. However, the internet is already fragmented along content lines as well as some operational lines, and always has been. This state of fragmentation has left both private sector entities and international bodies, such as the United Nations, struggling to understand how the internet is evolving and to positively influence its direction. In the view of these speakers, the multilateral model of engagement will be an important tool to shift the pace of change and allow all parties to find equal footing as new technologies appear and reshuffle the balance of power between actors.

1. ON THE EXISTING STATE OF FRAGMENTATION

In his opening remarks, Joseph Nye pushed back against the idea that the internet isn't already in some ways fragmented. In his view, the ideals of universal internetworked communication upon which the internet was founded failed to map onto even their contemporary reality. As early as the debates over Yahoo and eBay in the mid-1990s, it was clear that, although the internet aspired to be global, the machinery powering it had to live somewhere, and the jurisdictions where the technology was housed imposed their own laws and values. Because the truly unified internet was a false utopia to begin with, it's a mistake to imagine that fragmentation will splinter one internet into many.

Joseph Nye

In keeping with this inherent fragmentation, internet governance is spread across a number of organizations and forums in what Nye describes as a "regime complex." One exemplar within this complex is the World Conference on International Telecommunications (WCIT), whose 2012 meeting has been described as the beginning of a "new Cold War." But in Nye's view, instead of a pitched battle between democracies and authoritarian states seeking to control the internet, WCIT-12 was a multifaceted debate with conflicting norms and political goals determining each state's voting position. Rather than

a struggle for control of the internet, ongoing debates cover a range of issues, including crime, trade, human rights, and intellectual property. These debates take place within a loose coupling of forums whose diversity yields resilience in the face of both political differences and technological change. This resilience breeds more sophisticated, and thus longer-lived, bargaining relationships. The US and China, for instance, can have different positions on speech and human rights but common interests in trade.

Ambassador Lana Nusseibeh described a spectrum of views among key stakeholders and raised concerns over the influence of non-political entities. Governments generally recognize the value and potential economic benefits of the internet and work to harness new technologies for growth and even positive social change. It would be "naïve to say there haven't been problems" in security and crime, but these are "real issues and very fundamental issues that governments have to address."

2. ON CORPORATE POWER AND CITIZEN PARTICIPATION

Nusseibeh raised concern over the influence exerted by technology companies like Facebook with less than two billion users but more "power" than many countries. Having become major economic powers, these firms threaten to undermine traditional political processes. Countries should sit "as equal partners," and companies must acknowledge that the United Nations, despite its many flaws, remains a trusted institution with a global reach that sets it apart from other fora. The internet is not a Wild West, and in fact, the regime complex Nye describes is alive and well. But it's important to be aware of the extent to which the individuals and companies running the technical standards of this complex exercise influence over the resulting architecture and operations.

Ambassador Lana Nusseibeh

The panelists addressed another pressing theme: the tension between the traditional social order within a defined political entity and the transnational web of challenges posed within the governance and operations of the internet. Trust was highlighted as a driver of this tension. In many countries, ordinary people look to the multilateral order, especially the United Nations, to protect their rights and facilitate economic development. This results in a curious state of affairs, with the balance of trust lying with multilateral organizations whose majoritarian tendencies are laudably democratic but whose technical competency and capacity is questioned even by their defenders.

According to Nye, it boils down to the question, "How do you get everybody into the act and still get action?" He suggested that models from other areas may be informative: for example, the Intergovernmental Panel on Climate Change (IPCC), a body of climate scientists, deals with a similar regime complex in an area in which many players have a mutual interest but which lacks a single hierarchy. The IPCC provides a baseline, which governments then use in their negotiations. Internet policymakers have taken a step in this direction by deferring to groups of technical experts when making decisions in certain areas of internet policy and management.

A consensus emerged in the discussion around the notion that civilian infrastructure should not be the target of cyberattacks, but the challenge of developing broad norms for the internet as a whole remains. While Nusseibeh saw the UN's involvement as relatively uncontroversial, different countries take different views of what its mandate should be, as the WCIT-12 illustrated. Additionally, other international bodies are also seeking roles in internet governance and oversight. The speakers considered whether the International Telecommunication Union's (ITU) mandate gives it more granular authority for policymaking in areas such as "data tariffs," artificial intelligence, and consumer safety and security. Nusseibeh pointed out that there is no clear mechanism for giving private citizens a say on issues such as data collection, use, and distribution. She argued that it is important

to establish shared principles for how citizens interact with cyberspace before technological innovation leads to unforeseen consequences.

3. ON THE ROLE OF TECHNOLOGIES

The panel concluded with a discussion of the role of privacy-enhancing technologies, especially encryption, in internet fragmentation. The Snowden revelations have already pushed companies to adopt wider use of encryption in their products, but the broader debate over encryption remains ongoing. Nye argued that law enforcement agencies need to learn to work in a world in which encryption is common and adopt new methods to gather the information they need to solve crimes. Citing a recent report from the Berkman Klein Center for Internet & Society, he suggested that claims that encryption results in "going dark" may be overblown. While cryptography does cast heavy shadows over some areas, others, such as the Internet of Things, are shining a bright light by producing new metadata streams through which law enforcement agencies can track user behavior. The privacy implications of the Internet of Things metadata will of course be a critical area for future work.

Sitting at the juxtaposition of many trends and questions, the encryption debate is suggestive of an evolving conversation over the fragmentation of the internet. Countries seek to regulate the internet, but regulations remain difficult to enforce. Ultimately, the debate must expand beyond terrorism and militarization to encompass fundamental questions about how data is processed and how it can be harnessed for positive development. Because few forums exist for discussing these complex issues, the panel urged further consideration of how best to balance the need for international agreement on underlying values and principles with action-oriented progress made through expert-driven organizations and industry players.

Fireside Chat with Eric Schmidt

Merit E. Janow, Moderator
Dean, Columbia SIPA

Eric Schmidt
Executive Chairman, Alphabet Inc.

Rapporteur: Hugo Zylberberg

Dean Merit E. Janow spoke with Eric Schmidt, Chairman of Alphabet Inc., about the sweep of issues that global technology companies face, from the free flow of data to complexities around jurisdiction and trust to platform competition, as well as anxieties related to automation.

1. ON THE FREE FLOW OF DATA

Janow started the discussion by asking Schmidt to give his sense of the extent to which the free flow of data and information across boundaries is necessary for digital innovation and the app economy. Is this cross-border flow truly crucial? Schmidt responded by highlighting the original intent and design of the internet, a "story of naiveté." It was built starting in the 1970s, under minimal supervision, by people with an idiosyncratic idea of how society would work in the future. Intended to create a "true sphere of communication [for] all," their design lacked "core security of identity." This disregard for security, Schmidt explained, has proven to be a problematic design shortcoming now that the internet is fundamental to so many aspects of life, especially innovation, much of which occurs either because of or in spite of the internet.

Merit Janow and Eric Schmidt

Janow and Schmidt considered together the importance of cross-border dynamics, the ways fragmentation has come to matter, and its differential impacts. Schmidt observed that it would be nearly impossible for very small countries to have their own internet; little countries are, by nature, codependent. Very large countries are better able to cut themselves off, or at least use the internet on their own terms. Americans, however, are critically dependent on cross-border integration because it is a foundation for global peace. By increasing global prosperity, it makes the world safer.

The international community currently faces the challenge of re-implementing security mechanisms on top of existing infrastructure. "The good news is that there's powerful encryption and [it is] unbreakable, at least for the rest of our lives, but the bad news is that these technologies are not applied uniformly," said

Schmidt. He cited government computers, which may be "highly porous" and infrequently upgraded, as a major vulnerability. However, he does not believe that implementing security measures will lead to a fragmented internet from country to country.

2. ON REGULATION AND JURISDICTION

The conversation then moved on to regulation, jurisdiction, and the globalized world. Schmidt argued that the issues we're litigating today aren't new: countries have disagreed on copyright law and free speech for years, and accommodating legal differences across countries has long been a challenge. To address them in the age of the internet, he advises that technology companies build systems that are flexible and respect local laws. For instance, France's "right to be forgotten" should apply on the French country code domain but not globally.

Janow observed that more and more areas of economic and policy management—including securities enforcement and antitrust—have become sources of friction between countries and firms and raised jurisdictional challenges as the world has globalized. In some of these cases, harmonization agreements, mutual recognition, trade agreements, and other instruments have helped build trust and cooperation. The discussion focused briefly on whether potential technological solutions might help when it comes to global content. This possibility, however, naturally raises the question of which rules would apply—the most censorious or the most liberal? Schmidt stressed the many different approaches to content and censorship around the world, as well as Google's commitment to open speech.

Drawing from her experience in international organizations and governance regimes in trade and other areas, Janow asked whether the US should champion a global framework for the internet. Schmidt agreed that the world has been much enhanced by international frameworks created in the postwar period, but emphasized that they arose in part because the US was a major source of global GDP. Although the US invented the internet, the world depends on it, complicating the question of how much control should reside in the US. Most agree that the Internet Corporation for Assigned Names and Numbers (ICANN) system has worked quite well, but it's unclear whether decisions and frameworks can keep up with the speed and volume with which new issues are arising. Despite these challenges, an attempt to develop a global treaty might be warranted in cases of particular importance and concern, such as the militarization of the internet.

Whatever form future regulations might take, Schmidt cautioned against impeding the efficiency of the internet: "the core thing about technological progress is time, and the core aspect of time is communication; we now have almost all of the interesting developments in science, which I care a lot about, occurring across national borders in nanoseconds because of fiber optics, [and] compression of time which is core to economic growth, core to efficiency, core to human health, core to prosperity… That's one of the greatest accomplishments of the internet, and I do not want to see anything that slows that down."

3. ON ARTIFICIAL INTELLIGENCE AND ANXIETIES ABOUT THE FUTURE

Janow observed that recent years have seen an increase, in the US and around the world, of anxiety about globalization, technological change, and what this combination of forces might mean for job availability and the future workforce. Schmidt argued that technology has made the world infinitely better off. He pointed out that the jobless rate is down significantly in the US and that the internet has driven the creation of many new jobs. For instance, "there are more bank tellers now than ever because banks are more efficient." Schmidt argued that concerns about artificial intelligence are similarly unfounded because technology is now built openly and with the goal of benefitting people. In order to believe that globalization and technology are a net negative, "you have to believe that humans are not adaptable, that they're not creative, and [that they don't] respond to economic, political, and moral, and religious signals, which obviously we do." For this reason, he believes that the argument that technology will ultimately reduce job availability is, at core, wrong. In general, technology is making people smarter; this can only create more jobs and greater efficiency.

What Would Internet Fragmentation Mean for Global Trade?

Merit E. Janow, Moderator
Dean, Columbia SIPA

Usman Ahmed
Head of Global Public Policy, PayPal

Anupam Chander
Professor, UC Davis

Victoria A. Espinel
President and CEO, BSA | The Software Alliance

Malcolm Lee
Managing Director & Head of Policy, Alibaba Group

Ricardo Meléndez-Ortiz
Co-Founder and Chief Executive, ICTSD

Rapporteurs: Trey Herr and Sarah Myers West

Dean Janow opened the conversation by pointing out the significant role that debates about international trade played in the recent US elections and the negative posture to trade taken by both Democratic and Republican candidates—e.g., the argument that TPP was misguided, NAFTA was flawed, and the US was losing jobs as a result of these agreements. Panelists were asked to grapple with key issues in the trade domain, including data protection, data localization, and cross-border data flows, with special attention to emerging differences between national systems.

1. ON THE TRADE CONSEQUENCES OF FRAGMENTATION

Usman Ahmed started by evoking the sometimes dogmatic aspects of discussions about internet fragmentation. He noted that all data remains localized somewhere and is subject to a certain jurisdiction. He argued that the most important aspect of the internet-enabled system of international trade is not gains in efficiency but rather the idea that we could create a more inclusive economy. As an example, he cited a finding that businesses in the rural regions of the US had the same growth and export patterns as those in large coastal cities. He suggested that this democratization is the true benefit of the internet-enabled economy, and that the most worrisome consequence of internet fragmentation might be an undermining of inclusiveness.

Usman Ahmed

Victoria A. Espinel

Victoria Espinel agreed on the value of democratization and pointed out that what was true in terms of geography was also true in terms of size: the internet enables SMEs to compete for markets they could not otherwise reach. The internet's function as an economic leveler should be protected as we begin to address the holes in the existing trading system. Malcolm Lee reiterated the value of the internet to SMEs. He explained that Alibaba's objective is partly to empower SMEs within value chains, first domestically and then globally, by addressing the market failure of payments in the trade system and focusing on consumer finance, using mobile technology to leapfrog to the next generation of technologies. He sees fragmentation occurring in both the political and digital realms, and believes that the trade system should indeed protect the enabling aspect of the internet and avoid hindering the global engagement of SMEs.

2. ON THE PITFALLS OF PROTECTIONISM

Janow then turned to data localization as an example of the analog borders being imposed on digital trade. When is data localization of real economic or technological significance, as opposed to simply a nuisance factor or the cost of doing business? Anupam Chander started by re-stating that the overwhelming achievement of trade has been to pull billions of people out of poverty. The current trade system enables passage through existing national borders and initially reduced fragmentation in the trade domain. However, the most difficult thing to get across borders has never been a good or a bit—it has always been people. While the internet has reduced the impact of a certain kind of fragmentation, it has not affected others, such as visa requirements. Data localization is re-imposing forms of fragmentation that have always existed onto the global internet.


Anupam Chander

These new barriers have different consequences for different actors. Espinel addressed the barriers to the free flow of information from an industrial perspective. In her opinion, these barriers slow innovation, especially in the realm of artificial intelligence, where data must travel around the world. New technologies, such as cloud computing, rely on the free flow of information, and barriers imposed on the digital environment threaten their adoption and basic functioning.

3. ON THE INTERNATIONAL TRADE SYSTEM

Janow acknowledged that current trade discussions occur in an environment much more skeptical towards trade than it used to be; some bilateral relationships must be renegotiated after comprehensive regional agreements (TPP, TTIP) have lost steam or been abandoned. On this point, Espinel argued that going forward there was a need to "look at the reality and make the best of it," approaching regional and bilateral conversations (e.g., NAFTA, EU-Japan, EU-US) with a long-term strategy to bind these frameworks together. On the topic of long-term strategy for the trade community, Janow asked the panelists which current policy frameworks might be used as "best practice" models for future initiatives.

Ricardo Meléndez-Ortiz noted that the World Trade Organization electronic commerce working group began addressing these questions in 1994, highlighting inclusion, trust, and openness as key policy objectives to be achieved through international regulation. In the current environment, however, it's difficult to bring everyone

Ricardo Meléndez-Ortiz

to the table. Uncertainty about the fragmentation pressures that the trade system faces can lead to different perspectives from different actors, impeding formation of a consensus on how to go forward. The WTO Agreement on Services can be used as a model, but it does not help with thorny issues like determining when regulations on privacy are protectionist and when they are protecting the consumer. In the end, the WTO might not be the right forum for conceptualizing more than the digital trade of goods and services.

Chander agreed that there is no clear way forward. Some countries are banning or censoring services within their jurisdictions (e.g., Twitter in Turkey, WeChat in Russia). Meléndez-Ortiz observed that worry about a countries' capabilities in the digital economy can spur a return to industrial-era national policies that are sub-optimal from an international perspective and drive fragmentation. Chander pointed out that some companies experience legitimate difficulties in applying the rulings of certain jurisdictions globally (e.g., Google contending with France over whether the "right to be forgotten" should be applied globally). Chander sees a potential opportunity for trade institutions to have a say in cases when protectionist regulation serves no clear interest for the citizens. As an example, he explained that the European Union clearly recognizes the importance of cross-border data flows. But while attempting to liberalize the flow of data within its borders, it is simultaneously trying to limit the flow to other countries. This was for him a clear-cut case of potential fragmentation, in which trade regulation must help establish trust for both domestic and foreign actors.

Espinel added that different countries have different perspectives on what the Digital Single Market (the instrument through which the European Commission is seeking to liberalize cross-border data flows within the EU) is intended to achieve. For France, she argued, it means using data localization in order to compete against the US, whereas countries like Poland, Sweden, and the UK think about it very differently.

Stepping back, Ahmed reminded the group of the unequal distribution of the very understanding of what trade is. Trade is a set of tools regulating how governments treat foreign actors, and allowing them to treat those actors differently than domestic ones. Because digital issues only apply to trade insofar as this foreign/domestic tension applies, trade cannot significantly help in cases like Twitter in Turkey. As a limited tool applying to a limited set of circumstances, trade must be used only when relevant or runs the risk of delegitimization.

Malcolm Lee

Lee and Espinel also warned about the unforeseen consequences that can accompany the implementation of new policies. Lee gave the example of microloans on the Alibaba platform that could be squashed by regulations on the underlying data. As Janow later emphasized, so many areas of economic regulation create externalities that other countries feel they have the right to challenge secondary effects, whether intended or unintended. As another example, she offered the security and privacy implications of digital trade, and in the case of national security, argued that the international trade system was not set up for anything but deferring to the appropriate jurisdictions or, as the case may be, to the appropriate international organizations. In these instances, challenging the second-order effects of regulation might infringe upon other countries' self-definition of sovereignty.

Developing Trust and Assurance, a Global Issue with National Solutions

Steven Bellovin, Moderator
Professor of Computer Science, Columbia University

Joshua Corman
Director, Cyber Statecraft Initiative, Atlantic Council

Laura DeNardis
Professor, American University

Andrea Glorioso
Counselor, Digital Economy & Cyber, EU Delegation to the US

Angela McKay
Director of Cybersecurity Policy, Microsoft

Rapporteurs: Renata Barreto and Anna Aurora Wennakoski

This session explored the vicissitudes of trust in a digital environment and how it could drive fragmentation in the absence of comprehensive collaboration between actors. Trust is crucial to the operation of societies but, as applied to cyberspace, still little understood. After describing the current state of trust in an environment that cannot be trusted, the discussion shifted to how to enhance trust and which actors could do the most in this respect. While acknowledging the importance of national solutions under certain conditions, the panel concluded by addressing a coordination problem: how can cross-jurisdictional efforts be promoted over national ones that drive fragmentation?

1. ON TRUST IN AN UN-TRUSTABLE ENVIRONMENT

Laura DeNardis

Laura DeNardis started by referencing a book from 1999, Trust in Cyberspace (Fred B. Schneider, ed.). This book maintained that trust would be a precursor to authentication between people and operators in both social and technical infrastructures. But in the intervening years, DeNardis argued, society has developed an overwhelming dependence on the internet even as trust in traditional social infrastructures has eroded due to factors such as polling, surveillance, politicization of infrastructures, and breaches (e.g., the Yahoo email breach).

Quoting the CIGI-Ipsos "Survey on Internet Security and Trust," a poll with respondents from 24 countries, DeNardis noted that in recent years a majority of users have become more concerned about both their privacy and their own government. Only half of respondents trusted their government to behave appropriately in cyberspace. "So society is at a tipping point," DeNardis concluded, "in which improvements in digital trust are more than ever before necessary to sustain the global digital economy in the public sphere."

DeNardis also referred to computer scientist David Clark's use of "tussles" to describe areas where improvements in digital trust must be made: infrastructure stability, voting systems, news, data privacy, and of course, public cybersecurity. These "tussles" are key points for

measuring whether the internet is continuing as a global platform or splintering. Unease around fragmentation is easily explained: as the internet permeates offline spaces, new public policy problems emerge. An internet outage used to merely shut down a channel of communication; now it can prevent people from driving their cars. This migration from the strictly virtual to the physical realm raises the stakes of internet fragmentation significantly.

Joshua Corman

As Josh Corman put it, our dependence on software has become almost as ubiquitous as our trust in concrete and steel. Yet steel and concrete are much more dependable and infinitely less vulnerable than software. We must face, he said, some "uncomfortable truths": nearly all the Fortune 100 companies have lost trade secrets and Personally Identifiable Information as a consequence of software failures, compromising individuals' credit card data and identities in the process.

DeNardis views such breaches as a serious threat, calling cybersecurity "the great human rights issue of our time." But despite massive breaches, digital trust remains, perhaps because systemic failures have not yet occurred "where bits and bytes meet flesh and blood," in cyber-physical systems such as cars or hospitals. "We are at the point where these uncomfortable truths demand uncomfortable responses," she added. Complexity might be desirable for security purposes, fragmentation and segmentation might provide valuable answers, and any response must be multinational in nature.

DeNardis returned to "tussles," observing that they are increasingly the locations where states express power, e.g., with domain name systems being re-directed or used for intellectual property, censorship, or data localization laws, or even to tamper with the underlying infrastructure. These are not local problems but instead international relations challenges because the permeability of borders and both physical and virtual spaces raise the stakes. Since the technical structure of the internet does not map to geopolitical borders, state actions can have significant international repercussions. States' efforts to protect their national infrastructure from interference could drive fragmentation.

Although fragmentation would come with consequences, having only one internet is not ideal in every context. In highly trust-dependent areas for instance, DeNardis maintained that fragmentation could actually be desirable.

2. ON TRUST-ENHANCING FRAMEWORKS

Angela McKay

Angela McKay focused her comments on the way companies, rather than governments, can drive trust. Trust may seem for companies like a secondary concern to profit, but McKay argued that it is in fact a prerequisite for businesses to operate with customers, partners, and governments. Several policies could help private companies generate trust and cohesion. Requiring operational security, for instance, could be regarded as a trust-enhancing internal policy. After the Snowden case, many companies responded to customer concerns by encrypting data in order to remain a trusted partner. Such steps are crucial because, as McKay emphasized, once lost, trust is almost impossible to regain.

Andrea Glorioso examined the assumptions underlying trust, helping shed light on why it is so difficult to regain. Taking supermarkets and credit cards as examples, Glorioso observed that "we have developed

Andrea Glorioso (left)

systems within systems, and those systems are based in trust—99.9 % of the population doesn't care at all about this discussion (…) they really don't care what's happening behind the curtain, they just want it to work. However, when systems break down, they are surprised." Collectively, he argued, we "underestimate the power of this assumption" of trust. When trust is breached, we demand accountability and look to public or private institutions (perhaps more to public in the EU) to repair the relationship. Because these institutions, more often than not, operate at the national level, breaches of consumer trust increase internet fragmentation. Trust is the silent enabler of multinational institutions, and these institutions fail when trust is breached.

3. ON CROSS-JURISDICTIONAL EFFORT AND LEGITIMATE FRAGMENTATION

McKay raised a key question: Will security concerns drive national regulation, or can we build trust-enhancing frameworks in a cross-jurisdictional manner? To dispel misconceptions, she emphasized that fragmentation is occurring and that progress towards regulation is underway at both national and cross-jurisdictional levels. We are already living with a fragmenting internet in which national and regional regulations such as the General Data Protection Regulation in Europe and the NIST Cybersecurity framework in the US simultaneously enhance, constrain, and challenge how businesses operate.

Steven Bellovin

The need to meet national or regional demands can alter corporate solutions, as occurred when companies adopted the data-custodian model in response to EU regulation. McKay noted that Microsoft is running a data center in partnership with Deutsche Telecom, which acts as data custodian. This new joint venture addresses valid data access concerns while "foster[ing] harmonization" between national frameworks.

The conversation took a different turn when Steven Bellovin asked to what extent fragmentation can occur, given that we are so dependent on the cloud. He referred to one of his cardinal laws: "networks always interconnect." Panelists came to a rough consensus that in some cases, fragmentation is in the public interest and does not take away from the universality of networks. Important future work includes finding those cases and managing fragmentation. They also concluded that, while trust will never be absolute, we collectively must agree upon an "acceptable level of distrust."

Global Platforms, National Citizens and International Development

Ronaldo Lemos, Moderator
Director, Instituto de Tecnologia & Sociedade do Rio de Janeiro

Jeff Brueggeman
VP, Global Public Policy, AT&T

Ambassador Karen Kornbluh (ret.)
Senior Fellow for Digital Policy, Council on Foreign Relations

Peter Micek
General Counsel, Access Now

Rapporteurs: Fernanda Ribeiro Rosa and Sarah West

The panel on global platforms, national citizens, and international development featured a wide-ranging discussion on the role of regulators and the technology industry in shaping the flow of information online. The panelists discussed the implications of globalization for internet access, MLAT reform, and data protection, among other topics. Though their perspectives differed, they shared a concern about the decline of trust in institutions and its implications for internet policy-making.

1. ON EMPOWERMENT OF LOCAL STAKEHOLDERS

A key theme of the discussion was the need to reconcile the concept of a global internet with local governance, and the challenges posed for the interoperability of human rights frameworks, as well as the appropriate fora and mechanisms for reconciling different perspectives. The audience and panelists asked: what is the best way to balance sovereignty and national governance with the platforms' appetite for cross-border flows of information?

Jeff Brueggeman framed his response in terms of barriers to entry: that although the capacity exists for developing nations to harness technology for healthcare and economic innovation, "these services and the technology are being viewed as a threat (…), as a disruptor in a negative way." From a telco standpoint, technology is a "win-win." He advocated for solid economic arguments that demonstrate how technology can overcome barriers, pointing to trade agreements as places for building interoperable frameworks to deal with issues like data localization, privacy, and security.

Given the challenging nature of human rights issues, Brueggeman expressed concern about the possibility of creating more interoperable frameworks that allow for respect of human rights while maintaining a free flow of information. Though local laws and cultural norms must be navigated, he thought some actions could be taken "in the name of security and privacy that really have either economic motivations or human rights impacts."

Ambassador Karen Kornbluh (left)

"We have to take the backlash against globalization that we've seen most recently exhibiting itself in elections as a sign that we need to go back and rethink some of our frameworks and approaches," answered Ambassador Kornbluh. As an example, she pointed out that while freedom of information is often presented as a trade issue, it would be ineffective and burdensome to handle it through trade agreements. Multi-stakeholder communities are the right venues for dealing with certain questions, particularly those relating to technology.

Kornbluh also pointed to the OECD principles, which set up a distinction between national policy and international jurisdiction to prevent interference with free flows of information and "universal rights." She said, "I think the reason we load up trade agreements with other things is we've given up on working through these things through domestic politics or internationally." She advocated pursuing mechanisms such as MLAT reform and capacity-building in order to effect change.

Peter Micek agreed with Kornbluh's critique of trade as a mechanism for upholding human rights, though for different reasons. Micek noted that the process of negotiating trade agreements tends to be opaque rather than multi-stakeholder and inclusive. Later, Micek also pushed for the inclusion of redress mechanisms in agreements such as data protection principles, saying it was important that negotiators not assume they know what a community wants.

2. ON CAPACITY-BUILDING

With regards to capacity-building, the panelists shared a concern about policy decisions taken without consideration of the consequences for other actors as well as the broader internet ecosystem. From a policy perspective, Brueggeman saw the need to set up a model and work towards greater consensus among countries. He also mentioned the negative consequences of policymakers, regulators, government officials, judges, and law enforcement misunderstanding technology.

Ronaldo Lemos provided an example of a court ruling in Brazil that resulted in the shutdown of access to WhatsApp. The Brazilian police sought access to conversations taking place on WhatsApp in a criminal investigation. Facebook, which owns WhatsApp, was unable to provide the information because it was encrypted. A lower court judge sought to compel the company to provide the data by ordering the entire service to be shut down. WhatsApp was inaccessible in Brazil for several days, until the Court of Appeals reversed the shutdown. Lemos asked: "You see that happening in Thailand, you see that happening in Turkey. (…) When that happens, do telcos stand with their users, or do they comply with these orders? How do you react to these issues?"

Jeff Brueggeman

The panelists agreed on the importance of supporting a single open internet, but differed on the approach. Brueggeman said, "We need to have rule of law for what the process is going to be. The reality is: if we have people on the ground in a country and we have a legal order to do something, you're really at risk if you don't comply. So the way to fix that in the law is due process and having protections in place. I also think it goes back to the education point. We need to make sure countries need to understand that the internet is not a content platform anymore. It is physical safety, health, and anything else. There are major implications of implement[ing] these orders and often times … there are unintended consequences."

Kornbluh suggested that dealing with the issue through MLAT reform would help to clarify the situation by differentiating whether it's a speech issue, unfair treatment of a US company, or a privacy and law enforcement issue. She observed, "There's not a concerted single effort that says, let's take a whole of government approach. It's in our interest in so many ways to support a single open internet... So how can we be a little less parochial?"

Micek noted, "There is a lot of work to be done with governments. There is a role for the ITU (International Telecommunication Union), but the ITU should not run the internet. There is a role for national governments, but those national governments should not get to decide international rules." He said that there is value to decentralized management of the internet's resources and the capacity to make decisions about different issues, provided that there's a clear central commitment to one internet.

The panelists expressed more optimism about technological capacity-building, both in fostering innovation to address new problems and in increasing efficiencies to lower costs. They also discussed the role of the ITU in capacity-building, though generally the panelists agreed on the importance of keeping multi-stakeholder internet governance forums such as ICANN and the Internet Engineering Task Force (IETF) insulated from "political pressure." They suggested that the ITU might instead take a role in creating universal service funds, decentralizing networks, and opening spectrum policy.

Finally, they agreed on the value of the internet as a tool for empowerment, while recognizing that it can exacerbate existing problems. Though it did not create gender inequality, violence, or conflict, it can amplify them. To counter these harms, they suggested building capacity in areas where the internet can bridge gaps and guarding against misuse by focusing on what values should be embedded in institutions.

3. ON THE ROLE OF INTERMEDIARIES AND SELF-ENFORCEMENT

The panel also discussed the privatization of governance and the lack of accountability on the part of companies. This question came up in the context of recent critiques of fake news and France's "right to be forgotten" framework. Lemos noted that the framework places the onus for decision-making on companies. His concern is that, "You don't create a body of court decisions when you do that, you don't create jurisprudence."

Micek noted a difference between the sentiment in the room and that in the EU: in the EU, there's more frustration with corporate monopolies. "Facebook is the internet in a lot of the world, and they have waded into a whole lot of media-like services, service provision and distribution without being totally transparent about their content moderation policies, about their revenue sharing with the media that are forced to depend on them for survival."

Kornbluh shared the concern about internet intermediaries being turned into police, saying, "I think it raises the cost for everybody." Brueggeman agreed, noting that protection for intermediaries is a core value that has contributed to internet growth. He said, "I do worry as an internet service provider, that we can be next." He expressed concern that governments may be deferring responsibility for decisions, saying, "I do worry that governments will look to the platforms to say, you solve it."

Finally, in response to questions about government and corporate surveillance, the panelists discussed the role of industry players in increasing privacy protections online. Micek noted that companies have a real incentive to improve privacy protections at the device level, particularly given reports of phones being taken and searched by security agencies upon entrance to the US. At the same time, he noted, "this is not what we should be spending our time thinking about, how to cat and mouse our way around bad government policy." Rather than trying to engineer individual solutions, finding scalable ways to circumvent surveillance—such as policies requiring remote data storage for large organizations—would help protect users who would otherwise be at risk of getting flagged for scrutiny.

The panelists agreed that there is a broad move towards increased encryption for security reasons and acknowledged the difference between issues related to combating terrorism and those of day-to-day law enforcement and crime prevention.

Cyber Conflict and Democratic Institutions

Susan McGregor, Moderator
Assistant Director, Tow Center for Digital Journalism, Columbia Journalism

Camille François
Principal Researcher, Jigsaw

Sean Kanuck
Affiliate, Stanford CISA

Ronaldo Lemos
Director, Instituto de Tecnologia & Sociedade do Rio de Janeiro

Matthew Waxman
Professor, Columbia Law School

Rapporteurs: Renata Barreto, Aude Géry, and Poorvi Goel

While the internet allows for greater communication and a wider spread of information, its structure makes it especially vulnerable to security threats. Democratic governance in the 21st century requires a re-evaluation of the role of the internet in civil society. For example, there has been a lot of concern recently about manipulation of electoral politics. This panel asked two interrelated questions: What major threats does increased dependence on cyberspace pose to democratic processes? What kind of international institutions or private sector initiatives can foster cooperation in addressing them?

1. ON THE CONSEQUENCES OF DIGITIZATION FOR DEMOCRATIC PROCESSES

The panelists observed that, although initially thought to enhance democracy, insecure digitization can undermine liberal democratic processes, especially elections. By disrupting critical institutions and infrastructure, demagogues, dictators, hackers, and foreign powers can shake the international order. The panelists emphasized that this problem is not new but also that because democracies rely on the ability of their populaces to make informed decisions, increased dependence on insecure ICT poses considerable threats.

Quantitative data is playing an increasingly important role in electoral politics. There is a distinction between direct intervention in elections (e.g. tampering) vs indirect influences (e.g. false identities). The latter type of influences are the most cause for concern in the United States. There is a qualitative imbalance in the information that is presented because of how effective cyber espionage can be. Espionage and influencing foreign elections are nothing new, but Sean Kanuck raised a question about whether we have hit a qualitative tipping point because of over exposure to quantitative data. At a societal level, he observes that that seems to be the objection we're hearing.

On the issue of leveraging social media platforms to reach a new level of democratic engagement, Ronaldo Lemos observed that platforms like Facebook were not designed for political debates. On social

media platforms, it is hard to find a synthesis between two opposing political positions because these platforms do not have memory. For example, to reconstruct debates in the US around presidential elections, one would have to go through millions of timelines to reconstruct these debates. There is a need for designing of platforms capable of producing informed debates and increasing levels of information. The important issue in this regard will be accountability, for example, when fake news gets reported.

This observation led, in turn, to another line of questioning: how can the public differentiate truth from falsehood with certainty? In addressing this challenging question, panelists directed attention to how misinformation can destabilize society. In this regard, Camille François pointed out that there is a need to put analytical tools to distinguish between what is true and what is fake in the hands of the users. For example, Gmail has a government backed attack warning, which is issued to users when Google has reason to believe that state sponsored actors are trying to intervene in their inboxes.

Susan McGregor

The moderator, Susan McGregor raised the question of when state sponsored activity constitutes an act of war. Matthew Waxman noted that there may be a few reasons for declaring election interference an act of war. One of them could be to motivate and harness domestic policies to elevate the importance of an issue and to encourage private resources to be brought to the fore on that issue. The downside to that is that the government's hands get tied and it has to respond accordingly. In not doing so, the government fails to fulfil its responsibility to protect the citizens and the

Matthew Waxman (center)

state from attack. Another reason for treating it as act of war is to establish international norms prohibiting certain content.

2. ON THE FRAGMENTED LEGAL INTERPRETATIONS OF FREE SPEECH

In answering these questions, panelists used the concept of fragmentation as a framework for analysis. In particular, they addressed fragmented legal interpretations of free speech and fragmented truth-making institutions, as well as the role of private companies. The moderator raised the question of how to reduce the influence of fragmentation and what tools can be used. Ronaldo Lemos highlighted the importance of building trust in this matter. A lot of countries that do not have advanced cyber capabilities may view technology as a military tool, but technology can be used to foster transparency, accountability and build participation. Camille François agreed that infusing information back into the public sphere will help to rebuild trust.

3. ON THE POSSIBILITY OF ACCOUNTABILITY

Ronaldo Lemos (right)

Sean Kanuck

Finally, panelists addressed the need for a high level of accountability from systems that are part of the political process. Matthew Waxman highlighted that no one is regulating this space, so one way regulation can take place is through imposing obligations for states to police activities that are going on in their territories. Sean Kanuck raised the questions, "Who guards the guardians? Who is the ombudsman of truth and who do you want to be the regulator?" He observed that democratic free speech and democratic elections can be horribly inefficient and can lead to horrible

Camille François

outcomes, but they are still the best choice out of all the worst. He said of democractic process that "They're the fastest three-legged gazelle." Camille François said that there does not need to be central node responsible for accountability. As long as we make sure that as many people as possible have access to information, and distribution of information is transparent, we will have accountable networks. Ronaldo Lemos asked which institutions we can rely on for "truth." He gave the example of some countries which are trying to pass laws to counter fake news. This passes on the power to the judiciary to determine what the truth is. The only function of the judiciary should be to decide what is legal and what is not. The most important issue in accountability is how to rebuild and promote the institutions that safeguard and propagate truth.

Financial Institutions and Systemic Risks

Jason Healey, Moderator
Senior Research Scholar, Columbia SIPA

Christine Cumming
Adjunct Senior Research Scholar, Columbia SIPA

Siobhan MacDermott
SVP, Global Cyber Policy Executive, Bank of America

Katheryn Rosen
Senior Fellow, Cyber Statecraft Initiative, Atlantic Council

Paul Twomey
Co-Founder, Stash.Global

Rapporteurs: Aude Géry and Wouter Schmit-Jongbloed

Jason Healey (at the dais)

The financial system, envisioned atomically as individual nodes/branches, has suffered from fraud and (cyber-)attacks since its creation. The preferred response thus far has been for individual nodes to absorb the related losses, as they posed no discrete threat to the system as a whole. The deep integration of the financial system, at a variety of levels, that occurred as a result of its participation in the digital economy has changed this proposition: the system has become vulnerable in new and newly intricate ways.

In his introduction, Jason Healey noted the growth in scope and breadth of the financial sector throughout the economy. Its presence in the digital economy has both accelerated and emphasized its lack of substitutability. No longer is the financial sector a passive participant: it has become a critical (and highly regulated) component. This development has coincided with a broader loss of faith in the stability and purpose of the system as it functions currently.

Financial stability can be defined as the system's resilience to a negative shock that has the potential to cascade or cause an amplification of stress. The central "bad case" starts with a large initial shock, which causes net worth to drop. When an unexpected negative occurrence impacts valuation without being offset elsewhere, a sudden drop in net worth can quickly become critical if the target is highly leveraged in a way that causes liquidity mismatches. The initial shock can thus be amplified over a short period, causing households and the financial sector to scramble for liquidity at the same time. This, in turn, sets off the next hit to net worth and restarts the cycle.

In response to this new type of threat, the panel discussed three potential areas for improvement: the harmonization of emergency responses, avenues for improving the resilience of the overall financial system, and paths towards better global financial governance.

1. ON HARMONIZATION OF EMERGENCY RESPONSES

Christine Cumming suggested that banks should now be thought of as interconnected networks instead of brick-and-mortar institutions. The main difference between "finance" and a lot of the transactions on the broader internet is that its transactions occur in real time. Resilience in this context is a dynamic process, with analysis occurring as threats are identified and evidence uncovered. The shock to the system following Hurricane Sandy provided an instructive showcase of efforts by the financial sector to keep money moving globally. This type of learning goes on at an international level and helps build a template for dealing with cyber issues more generally.

Christine Cumming

The question of who reaches into the structure of these networks and ensures continued corporate hygiene in real time is a pressing concern. According to Katheryn Rosen, most banking institutions approach questions of hygiene in terms of compliance with relevant regulation. Cumming observed that while this approach is insufficiently systematic (and potentially problematic), it should still be recognized and regulated accordingly to monitor risks at the system level and to banks directly.


Katheryn Rosen

To this end, there's much to recommend stress testing. Banks tend to approach the question of emergency response in the manner most familiar to the financial sector—as a risk assessment: How much revenue would you lose? Estimates of such losses (i.e., sizing the breadbox) are a useful and central approach.

However, not all cyber risks imply systemic risk. It is useful to distinguish a (systemic or non-systemic) cyberattack from human error that triggers a circuit breaker. Market-trading-information frameworks can prove useful in uncovering the contagion and transmission channel. But distinguishing between different kinds of emergencies requires the mapping of language and of the propagation of various shocks. Only a proper classification of all types of risk can indicate which emergency response is suitable to counter the immediate threat. Precise knowledge of financial sector infrastructure and operations is also crucial.

Healey pointed out that the difficulty of determining what and where to hedge makes systemic risk in this context the "longest" position banks can take. New technologies are introducing new types of lending and mechanisms for payment to the system—it is as yet unclear whether they will have a stabilizing or destabilizing impact. In fact, according to Paul Twomey, governments seem to be using "fintechs" deliberately to fragment the systemic banks.

2. ON RESILIENCE

Healey explained that financial markets are very fragmented, and that the pieces talk to each other in increasingly fragile ways. The US Treasury tried to map "the market," but had to admit that no single mapping is currently possible. Legacy systems, independent conduits, and new technologies are superimposed and made interoperable, leading to a fragmented system-of-systems. Markets are vulnerable, and it's unclear where we can find a measure of substitutability that could control for and limit the consequences of contagion. Here, by contrast with other sectors, there is no single clear control mechanism to abate shocks

Paul Twomey

Twomey noted that the financial services sector is currently rather isolated (in both deliberate and accidental ways) through policy and regulation, but Siobhan MacDermott argued that it is also globally interconnected. One of the key challenges to the system is overcoming (analytically as well as politically) the implicit and explicit loss of leverage when approaching systematic questions of fragmentation and fragility at an international level. Whereas an international response to an emerging threat is cumbersome and difficult, domestic responses are often timely and, in the US, the result of close cooperation between financial and technology companies. Things become more difficult once you leave the US. Rosen suggested that, when addressing an emerging issue, the tech community responds quickly on a national level, but fundamental debates around international infrastructure invariably take longer.

Unsurprisingly, given its complexities and vulnerabilities, the financial infrastructure is the most attacked part of the national economy. A hostile force that manages to crash the financial sector can create chaos in even the most powerful countries. To minimize chaos, MacDermott explained, nation states not only step in as regulators and monitors but also function as providers of liquidity in times of systemic tension and attack. Until recently, a state's response was mainly about cybercrime, but it has increasingly incorporated a geopolitical aspect as well.

3. ON GLOBAL FINANCIAL GOVERNANCE

With the transformation of financial institutions into technologically driven actors within, and architects of, the digital economy, certain banks, in addition to serving as financial hubs, have become IT institutions that are too central to fail. Collaboration between banks is close and extensive, and built upon the common understanding that the system must be protected. Banks may compete on everything else, but when it comes to resilience, there is no limit to cooperation.

Siobhan MacDermott

In addition, as MacDermott explained, the US government has designated the financial infrastructure as "critical" through an Executive Order. The largest banks in the US have gathered in dedicated sector-specific organizations to share ideas, as well as classified and unclassified data, and to evaluate key questions, such as, what happens in times of a great shock? How can we assure liquidity and prevent brand name losses?

But while this cooperation is encouraging, MacDermott warned that regulations are in conflict with each other internationally. Given that half of the over 200 frameworks are incompatible, conflict mitigation infrastructure must be improved. The most promising strategy for gathering international commercial cooperation around cyber threats and enhancing the system's resilience to an initial adverse shock is by

quantifying that risk. The challenge, then, is to translate a cyber event into dollars. This process is complicated when geopolitical concerns limit information sharing. With many examples (e.g., Sony) illustrating this predicament, initial work could address loopholes that have already been exploited. Structurally addressing these loopholes can add meaningful resilience to the present system.

At the same time, system duplication could also add to long-term resilience. While duplication might slow innovation, extra measures are needed to protect the payment system, which is particularly vulnerable and has already been the target of massive attacks.

Healey concluded by reiterating a major theme that had emerged over the course of the day: public trust is key, and should be a priority for policymakers.

PART II: FRAMING PAPERS

Working Paper
For circulation at the 2017 Global Digital Futures Forum
May 5, 2017

COLUMBIA|SIPA
School of International and Public Affairs

Framing Conversation: What Would Internet Fragmentation Mean for the Digital Economy?

By William J. Drake

1. Introduction

The theme of this year's Forum is very timely, as the question of Internet fragmentation has been the focus of a good deal of discussion of late in both generalist and specialist policy circles. But before we can explore the potential impact of Internet fragmentation on the digital economy, global governance, and global trade, it would be useful to step back and consider what we mean by the term in the first place. Some references in popular media seem to suggest that the term connotes a singular phenomenon on which there is broad agreement so we can simply invoke it and move on from there.

In fact, Internet fragmentation remains a contested concept. A cursory review of its usage in various publications and public pronouncements suggests that people often speak of it when discussing a variety of problems and tensions that arise on the Internet that do not all originate from the same source. For example, some in the business community have used the term as a generalized reference to variations in national policies that add to the cost of doing business globally. While some such policies may indeed be related to fragmentation, many other simply reflect differences in national legal systems, policy traditions, and so on that may antedate and arguably do not fragment the Internet. Similarly, some people have described the increasing linguistic diversity of cyberspace as an example of fragmentation, when of course this is simply a matter of a diverse humanity getting on line.

Another tendency among at least some observers is to suggest that the Internet is in imminent danger of falling apart. Because there is so much variation in national policies and practices, it is said, the Internet is likely to "break up" into a series of disconnected islands. This seems to be an overly dramatized misreading of some troubling trends. In fact, no cataclysm is around the corner; the underlying infrastructure remains stable and secure in its foundations, and it is incorporating new capabilities that open up new horizons, from the Internet of Things and services to the spread of block chain technology

and beyond. But there are fragmentary pressures accumulating which, if left unattended, could reduce to varying degrees the Internet's enormous vitality and contributions to the world.

Conversely, while the examples just mentioned concern overly broad applications of the term, other observers tack in the opposite direction and say that "fragmentation" can only be properly used in reference to the Internet's underlying infrastructure rather than the creation of significant closed digital spaces. In one variant of this thinking, fragmentation would only happen if there was a massive defection from the unified Internet to entirely separate and non-interoperable systems running off different zone files. Since such a defection does not appear to be likely in the near future, voilà, there is no fragmentation, and people who argue to the contrary are needlessly hyperventilating, perhaps in hopes of looking prescient.

With these conditions in mind, in this memo I will briefly address three matters in the hope of helping to frame the conversation. First, I will advance working definitions of Internet fragmentation drawing on a white paper I wrote with colleagues for release at the World Economic Forum's (WEF) Annual Meeting in Davos in January 2016. [1] Second, I will highlight the variability and fluidity of Internet fragmentation in order to underscore that we are not talking about a simple binary condition that flicks on or off like a light switch. Third, I will conclude by raising a few concerns about the potential impacts of fragmentation on the evolving global digital economy.

2. Defining Internet Fragmentation

A useful starting point is to consider what we mean by an unfragmented Internet. What is the baseline from which fragmentation departs and against which it can be assessed? From a technical standpoint, the original shared vision guiding the Internet's development during the research and education era was that

[1] William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, *Internet Fragmentation: An Overview* (Geneva: The World Economic Forum, January 2016). A few bits of this memo derive from that earlier paper.

every willing endpoint on the Internet should be able to exchange data packets with any other endpoint that was willing to receive them. Universal "connectivity among the willing" was the guiding objective, and it could be achieved if autonomously controlled and even separately designed networks were internetworked and made interoperable via a shared protocol stack, TCP/IP, and related standards and protocols. Such interoperability needed to be to be seamlessly coherent on an end-to-end basis and consistent, so that users' actions would yield the same responses irrespective of location or the service providers involved.

These core features of universal, consistent interoperability and communicability between consenting end points were fundamental from a design standpoint. Every end point that wanted to send and receive bits with any other should be able to do so, so that the network of networks functioned as a free and open system. Actions or conditions that impaired this seamless functioning and blocked users from reaching each other could be said to constitute fragmentation.

Imagine, by way of analogy, an international telephone network on which people in country A could communicate with people in countries B, D, and F but not with people in countries C, E and G, while people in country B could communicate with people in countries A, C and E but not D, F and G, and so on across 196 countries. If humanity's ability to reach the full range of willing correspondents were this barrier-laden and segmented into go and no-go zones, would we characterize the global telephone network as open and unfragmented? Probably not. But on the Internet this sort of highly variable geometry of communicability is fairly standard and taken for granted, especially if one considers the infinite substantive variety of the bits that could be shared if allowed. We know that over 700 million users in China cannot access major platforms that are used by billions of people elsewhere; that billions of downloaders encounter messages like "the content you requested cannot be displayed;" that the transfer of certain classes of data out of certain countries is blocked or requires government permission; and so on, endlessly.

My contention, which like others is certainly contestable, is that the pervasive limitations on users' abilities to freely access, create, and dissemination information indicates an endemic condition of Internet fragmentation. The Internet is not a wide-open medium in which "anything goes," popular characterizations notwithstanding. It is certainly far more open than any global medium we have ever had

before, and the limitations on its openness are frequently the focus of efforts to bypass or reverse by various actors, but they are there. And, as Eli Noam has argued in a provocative essay, they were inevitable. [2] There was simply no chance that the conditions that obtained in the early years when the Internet was a vehicle for the non-commercial sharing of research and educational information among computer scientists in various organizational settings could survive the transition to the Internet becoming a global mass medium used for an endless variety of social, commercial and political information sharing and resource discovery. Inevitably, governments were going to work to embed the Internet in frameworks of public authority that involved a wide variety of prescriptions and proscriptions, and companies were going to work to monetize peoples' access to and use of different kinds of contents by erecting a wide variety of enclosures and requirements. At the same time, with millions of technical people around the world working to deploy new capabilities, increase security and various other objectives, conditions could develop that, often unintentionally, had the effect of reducing or at least complicating the seamless functioning and interoperability of the infrastructure.

Hence, from this standpoint, it makes little sense to pose questions like "will the Internet fragment?" The Internet has long been fragmented to varying degrees in varying ways. A better question might be, will "Internet fragmentation increase in a manner that becomes much more problematic for a much wider range of uses and users?" Such a formulation turns our attention to the direction of change, rather than whether change might commence.

While Internet fragmentation has a common root---limitations on the ability of every willing endpoint to exchange data packets with any other willing endpoint---it is not a singular phenomenon. Fragmentation varies in its sources and manifestations in ways that are worth assessing separately on their own terms. Hence, in the above-mentioned paper for the WEF, my co-authors and I advanced three different "working definitions," so-called because the paper was an initial exploration and mapping and we were cognizant that more precise formulations might be desirable after our colleagues in the field

[2] Eli M. Noam, "Towards a Federated Internet", *InterMEDIA* (41, 4, 2013), pp. 10 –13.

kicked us around a bit on points that needed rethinking. We began from the proposition that a single "narrow definition" focused only on conditions in the underlying infrastructure would not capture how people use and experience the technology in order to construct digital social formations and engage in information, communication and commercial transactions, or by extension the sorts of political and economic forces that may impede their abilities to do so. We therefore amended the standard four-layer characterization of the Internet based on the TCP/IP Protocol Stack by adding a fifth

Content and Transactions layer to capture the substantive information exchanged and the interactions and behaviors involved.

Figure 1: Internet Layers

5. Content and Transactions Layer
4. Application Layer
3. Transport Layer
2. Network/IP Layer
1. Physical/Link Layer

Beginning from this amended baseline, we advanced the following working definitions of fragmentation:

- *Technical fragmentation:* conditions in the underlying infrastructure that impede the ability of systems to fully interoperate and exchange data packets and of the Internet to function consistently at all end points. These generally pertain to layers 1-4 of the model above.
- *Governmental fragmentation:* Government policies and actions that constrain or prevent certain uses of the Internet to create, distribute, or access information resources. These generally are targeted at the 5th layer in our model, but they may involve actions taken at the lower technical layers as well.

- *Commercial fragmentation:* Business practices that constrain or prevent certain uses of the Internet to create, distribute or access information resources. These generally are targeted at the 5th layer in our model, but they may involve actions taken at the lower technical layers as well. [3]

As is evident, one of our concerns was to distinguish sources and locations of fragmentation based in part on the question of intentionality. Technical fragmentation of the underlying physical and logical infrastructure is a complex evolutionary process that has unfolded slowly but is gathering pockets of steam in the contemporary era. Some of it has been intentional and motivated by operational and other concerns, but more often it has been the unintended by-product of actions taken with other objective in mind. In contrast, governmental and commercial fragmentation usually have been due to the intentional efforts of these third parties to establish limitations on users' abilities to create, distribute or access information. As a general matter, one could argue that such limitations are much more problematic and difficult to remediate than technical problems, for which engineers often can devise "fixes." In contrast, governmental and commercial fragmentation can be difficult to engineer "work arounds" for with lasting effects, e.g. people confronting censorship may rely on virtual private networks to mask their locations, but then governments figure out ways to block and monitor these and another technique must be found, at least until that too is found out.

[3] Drake, Cerf and Kleinwächter, p. 14.

3. Variability and Fluidity

Just as fragmentation is not singular in its form or the domain of its effects, the extent of fragmentation within and across the three categories also is highly variable. One could imagine a number of dimensions on which such variation could be found, but here are just three that merit consideration.

Occurrence: The first and most fundamental consideration is whether a given form of fragmentation exists. This is not an entirely straightforward question; as is noted above, fragmentation as a systemic property is not a simple binary condition that is either present or not present, and a specific instance of fragmentation in some domain may involve gradations with different values along a continuum. In some cases those values can be precisely quantified (e.g. the number of websites or other information resources to which access is fully blocked), but in others the best we can do is to devise ordinal measures. Similarly, there can be variations in duration. Fragmentation may be a short-term phenomenon that is rectified fairly quickly, as with recovery from some an attack that blocks access to resources, or it can be sustained as a long-term condition. In time sensitive situations, even short-term fragmentation can be very damaging to users or transactions. In general though, we should be most concerned with sustained fragmentation that has ongoing consequences.

A final issue here is that fragmentation does not need to be currently present to be of concern. That is, in many of the instances that people cite when worrying about the matter, what is at stake is the emergence of tendencies and pressures that could give rise to something significant in the future. As in any policy arena, we need not wait for a problem to become full blown and wreaking havoc for awareness and action to be well advised.

Intentionality: Fragmentation, particularly in the technical arena, may be the unintended by-product of decisions and actions guided by unrelated objectives. People who deploy or fail to deploy a particular technology in addressing a localized operational challenge may not be setting out to fragment the Internet. Nevertheless, their actions, especially if replicated by others, could come to have cumulative effects. Divergences between individually rational choices and systemically suboptimal consequences are a standard feature of collective actions problems generally and the same logic can apply to the openness or fragmentation of the Internet.

Alternatively, fragmentation may be intentional. The character of these intentions obviously matters quite a bit. On the one hand, organizations, communities and individuals may seek to separate themselves somewhat from the open public Internet for entirely defensible reasons. Installing a firewall to limit access and communication to only authorized and consenting parties and to protect resources from unwanted interference is a benign act of self-separation. In our WEF discussions last year, some participants argued that self-separation, such as the construction of firewalls or the use of encryption on a network, could be thought of as "positive fragmentation." I tend to think of this as being a different sort of activity that may involve some protective segmentation but is not preventing willing end points from communicating, since one end point is choosing to mediate its boundaries.

Of more concern, and more properly a matter of fragmentation in my view, is when actors such as governments seek to shape, constrain or fully block the activity of others who have not consented to this. Imposing limitations on others is a malign act of forced separation. Both unintentional and intentional fragmentation can be problematic, but the best approach to remediation may vary accordingly.

Impact: Fragmentation may be deep, structural and configurative of large swaths of activity or even the Internet as a whole. Consider, for example, the implications if significant categories of data flows were to be widely blocked around the world, or if an alternative root system with its own name space were to be established with the backing of powerful governments or organizations. The scope of the processes, transactions and actors impacted by such breakage would be substantial. But fragmentation also can be more shallow, malleable and applicable to a narrowly bounded set of processes, transactions and actors. The impact could be significant for some people but go unnoticed by others.

As with the other dimensions just mentioned, it can be difficult to measure the intensity of fragmentation and say with certainty exactly where on the continuum a given instance lays. Even so, in considering examples, we should be mindful that fragmentations are not all created equal in terms of magnitude and import. Indeed, a number of the examples one could mention are relatively low-impact or low-intensity matters – bothersome and concerning enough to engineers and operators that attention to them is merited, but not so significant that they endanger the fundamental integrity, openness and utility of the Internet. In contrast, some other action are higher-impact and arguably in need of concerted responses.

Given the above, from a systemic standpoint fragmentation is something of a shape shifter. It is always with us, particularly at the fifth level of content and transactions, but its specific manifestations are highly fluid and variable in scope, depth and duration. What should be of most concern are intentional forms that are deep, structural and configurative of large swaths of activity or even the Internet as a whole.

4. Implications for the Global Digital Economy

Some forms of fragmentation of this character are of relevance to the opening session on the digital economy. For example, with regard to technical fragmentation, if governments engage in widespread blocking of new generic top-level domains, opportunities for additional economic growth and social empowerment would be foreclosed. A massive defection by a leading country or countries to another root system, while presently unlikely, undoubtedly would have a very pronounced negative impact on the global digital economy. In general though, technical fragmentation at present does not seem likely to take on the sort of character that would in any dramatic way spoil the party.

Commercial fragmentation probably raises greater risks. There is growing concern today as to whether divergent corporate preferences may result in inadequate technical standardization of the emerging Internet of things. The adoption and locking in of proprietary standards in key arenas like this could produce fragmenting effects, with important products and processes not working well across corporate boundaries and national borders. The current push in the United States to abandon network neutrality as an organizing principle, driven in particular by traditional network operators and government ideologues, could result in widespread discrimination against applications and entrepreneurs and produce a fragmentary, multi-speed environment. Overly expansive and rigid intellectual property rules could curtail entrepreneurial dynamism as well as free expression and human empowerment. And as we move ever further into a platform-dominated online economy that absorbs an increasing share of advertising dollars and economic activity, the ways in which terms of service are constructed, the possibilities for anti-competitive behavior, and the prevalence of “walled garden” strategies may alter the character of the digital economy in ways that attenuate existing inequalities. Arguably, this may be particularly a concern with respect to the participation of developing countries in the digital trade arena.

Finally, and most importantly, governmental fragmentation of a structural nature seems to be a particularly pressing concern. The widespread "securitization" of Internet policies and the growth of so-called "cyber-sovereignty" strategies is already producing trends toward more widespread censorship and digital protectionism. These measures can be very difficult to roll back, and can impose significant costs on global companies and national economies and citizens alike. The potential scope of the challenge is underscored by the current trend toward forced data localization policies and the erection of barriers to cross-border data flows, which are the subject of a follow-up study to the above-mentioned fragmentation paper that will be released later this year.[4] In the opening session we may wish to delve into these and related questions.

[4] William J. Drake, *Data Localization and Barriers to Cross-Border Data Flows: Toward a Multistakeholder Approach,* (Geneva: The World Economic Forum, September 2017).

Normative Restraints on Cyber Conflict

March, 2017

By Joseph S. Nye, Jr.

1. Introduction

Where does the world stand in the development of norms to restrain conflict in cyber space? Elsewhere I have compared learning about cyber security with the way states learned to cooperate in regard to nuclear weapons. ("Nuclear Lessons for Cyber Security," *Strategic Studies Quarterly*, Winter, 2011). While cyber and nuclear technologies are vastly different in their characteristics and effects, at a meta level, the processes of how societies and states learn to cope with a highly disruptive technology have interesting similarities. In terms of chronology, it took states about two decades to reach the first cooperative agreements to limit conflict in the nuclear era. If one dates the cyber security problem not from the beginning of the Internet in the 1970s but from the period since the late 1990s when burgeoning participation made the Internet a substrate for economic and military interdependence (and thus vulnerability), cooperation in cyber is now at about the two decade mark.

The first efforts in the nuclear era were unsuccessful UN centered treaties. In 1946, the US proposed the Baruch plan for UN control of nuclear energy, and the Soviet Union promptly rejected locking itself into a position of technological inferiority. It was not until after the frightening Cuban Missile Crisis, that a first arms control agreement, the Limited Test Ban Treaty was signed in 1963. The NPT followed in 1968 and the bilateral Strategic Arms Limitation Treaty in 1972. In the cyber field, in 1999, Russia proposed a UN treaty to ban electronic and information weapons (including propaganda). With China and other members of the Shanghai Cooperation Organization, it has continued to push for a broad UN based treaty. The US resisted what it saw as an effort to limit American capabilities, and continues to view a broad treaty as unverifiable and deceptive. Instead, the US, Russia and thirteen other states agreed that the Secretary General should appoint a Group of Government Experts (UNGGE) which first met in 2004. It initially had meager results, but by July 2015 it issued a report which proposed norms for limiting conflict as well as confidence building measures that was endorsed by the Group of 20 summit. Groups of experts are not uncommon in the UN process, but only rarely does their work rise from the basement of the UN to a summit of the twenty most powerful states. The success of this group was above the ordinary.

2. The UN Group of Government Experts

The GGE issued reports in 2010, 2013 and 2015 that have helped to set the negotiating agenda for cybersecurity, but despite this initial success, the GGE has limitations. The participants are technically advisors to the Secretary General rather than fully empowered national negotiators, and although their number has increased from the original 15 to 20 to 25, most nations do not have a voice. According to one diplomat who has been central to the process, some seventy countries have expressed interest in participating. But as the numbers expand, the problems of reaching agreement increases. Some observers worry that entropy will set in and they express concern whether this process can continue to succeed.

To understand the GGE, it helps if one puts it in a broader context of normative constraints upon states. The three canonical sources of international law are treaties, customary international law, and expert juridical opinion. Some observers draw a sharp distinction between international law and international norms. The Tallinn Manual, for example, is an important effort by a group of international lawyers to write down what is agreed to be international law. it is clear that lawyers do not always agree, but on many matters they do agree on law that is supposed to be binding on states. A norm, as distinguished from law by Martha Finnemore and Duncan B Hollis,("Constructing Norms for Global Cybersecurity," 110 *American Journal of International Law*, 2016) is a collective expectation of proper behavior of actors with a given identity. Norms apply to multiple actors and are not legally binding. "Laws can serve as a basis for formulating norms, just as norms can be codified by law."(p442) Norms play a role in constituting new roles as well as constraining existing ones. The "oughtness" of their constraints can grow out of law, politics and cultures.

Parsing the differences between laws, norms and other types of constraints is sometimes useful but it is not my purpose here. By lumping together a wide range of normative constraints, I want to illustrate nine potential arenas for action in the following matrix. Horizontally, in terms of formalism, normative constraints on states range from formal treaties to conventional state practice to codes of conduct and norms. Vertically, in scope of membership, the groups thus constrained can range from global, to plurilateral, to bilateral. Such groups can include both states and non-state actors. The totality can also be described as a regime complex.

3. Normative Constraints on States and Non-State Actors

	Agreements	State Practice	Norms and codes
Global	ICANN	Routing practices and exchanges	UNGGE
Plurilateral	Budapest Convention	Like minded groups	G 20, OSCE Regional orgs.
Bilateral	US/China on commercial CNE	Entanglement and self restraint	CBMs, US-Russia hot line

Non-state actors can be constrained by domestic law, punishment, culture, but in a world without overarching international government, why do sovereign states themselves sometimes let normative considerations constrain their behavior? Among the considerations, one reason is fear. Another is external reputation. A third is domestic political pressure.

4. Fear, Prudence and Norms

What can history tell us about the effectiveness of these normative instruments of policy in other areas? In the decade after Hiroshima, tactical nuclear weapons were widely regarded as "normal", and the U.S. military incorporated nuclear artillery, atomic land mines and nuclear anti-aircraft into its deployed forces. In 1954 and 1955, the Chairman of the Joint Chiefs of Staff told President Dwight Eisenhower that the defense of Dien Bien Phu in Vietnam and the defense of offshore islands near Taiwan would require the use of nuclear weapons, but Eisenhower rejected the advice in part because of fear of unintended consequences. (See my "Deterrence and Dissuasion in Cyber Space," *International Security*, Winter 2017).

Over time, this prudence developed into a norm of non-use of nuclear weapons which has added to the cost that a decision maker must consider before taking an action to use them. The Nobel Laureate economist Thomas Schelling argued that the development of a norm of non-use of nuclear weapons was one of the most important aspects of arms control over the past 70 years. Ironically, Eisenhower (and other leaders) was unwilling to sign onto a formal norm of no-first use of nuclear weapons because the residual uncertainty of potential use was needed to deter Soviet superiority in conventional forces. It was

not until the era of Gorbachev and Reagan that leaders were willing to agree that nuclear war could not be won and must never be fought. The norm of non-use has had an inhibiting effect on leaders of major states, but for new nuclear states like North Korea, one cannot be sure whether the costs of breaking the taboo would be perceived as outweighing the benefits.

In cyber, fear of destroying the benefits reaped from the Internet (which are increasingly important to economic growth) may constrain attacks on the Domain Name System or the IANA function. In addition, the very newness of cyber war and fear of unforeseen consequences in unpredictable systems may contribute to prudence that could develop into a norm of non-use or limited use or limited targets. As Brandon Valeriano and Ryan Manness point out in *Cyber War vs. Cyber Reality* (Oxford University Press, 2015), on a number of occasions when faced with a choice in wartime, political and military leaders have preferred the predictability of kinetic weapons. Sometimes fear of unintended consequences can lead to prudence which can develop into a norm.

5. External Reputation

After World War I, a consensus taboo developed about poisons, and the 1925 Geneva Protocol prohibited the use (though not possession) of chemical and biological weapons. They existed but were not used in World War II because of deterrence through fear of retaliation. Then in the 1970s, two treaties were negotiated that prohibited the production and stockpiling of such weapons. That meant that there is a cost associated not only with their use but even their very possession. Verification provisions for the Biological Warfare Convention are weak (merely reporting to the UN Security Council), and such taboos did not prevent the Soviet Union from cheating by continuing to possess and develop biological weapons in the 1970s. The Chemical Weapons Convention did not stop either Saddam Hussein or Bashir al Assad from using chemical weapons against his own citizens, but they did have an effect on the perceptions of costs and benefits of actions, such as the international dismantling of most Syrian weapons in 2014. With 173 states having ratified the Biological Warfare Convention, states that wish to develop biological weapons have to do so secretly and illegally and face widespread international condemnation if evidence of their activities leak. External reputational harm, along with uncertain benefits in use, appear to be the main reasons that norms seem to have limited possession such weapons.

Normative taboos may become relevant in the cyber realm as well, but not against mere possession of weapons. The difference between a computer program that is a weapon and a non-weapon depends on intent, and it would be difficult to forbid the design, possession, or even implantation for espionage of particular programs. In that sense, cyber arms control cannot be like biological arms control or the nuclear arms control that developed during the Cold War which involved elaborate detailed treaties regarding verification. Unlike physical weapons, it would be impossible to reliably prohibit possession of the whole category of cyber weapons.

A more fruitful approach to normative controls on cyber arms is not to focus a taboo against *weapons* but against *targets*. The United States has promoted the view that the internationally recognized Laws of Armed Conflict (LOAC) which prohibit deliberate attacks on civilians apply in cyber space. Accordingly, the U.S. proposed not a pledge of "no first use" of cyber weapons, but a pledge of no use of cyber instruments against civilian facilities in peacetime.

This approach to norms was adopted by the GGE. The taboo would be reinforced by confidence building measures such as promises of forensic assistance and non-interference with the workings of Computer Security Incident Response Teams (CSIRTs). The GGE report of July 2015 focused on restraint on attacks on certain civilian targets rather than proscription of particular code. At the 2015 summit between American President Barrack Obama and China's President Xi Jinping, the two leaders agreed to set up an expert commission to study the GGE proposal (as well as a separate agreement limiting cyber espionage for commercial purposes). As noted above, the GGE report was endorsed by the leaders of the G-20 and referred to the UN General Assembly. On the other hand, an attack on the Ukrainian power system occurred in December 2015, and was widely attributed to Russia, a GGE member (though Russia might argue that given its hybrid war with Ukraine, it was not bound by a peacetime norm.) Similarly, in 2016, the U.S. accused Russia of using cyber means to interfere in the American election. Despite the fact that the US had added electoral processes as a 17th item on its list of critical infrastructures, Russia clearly did not include the election process in the U.S. as a critical civilian infrastructure covered by the taboo. At this point the development of normative controls on cyber arms remains a slow and incomplete process. In general, the multi-lateralization of norms helps raise the reputational costs of bad behavior. It is worthy of note that the Missile Technology Control Regime and the Proliferation Security Initiative began as voluntary measures and gathered momentum, members, and normative strength over time.

6. Domestic Factors

There is a third process which can lead to statesmen accepting normative constraints on their actions and that arises out of domestic politics. In cyber as in other domains, theorists like Martha Finnemore and Kathryn Sikkink ("International Norm Dynamics and Political Change," *International Organization* 1998) have hypothesized that norms have a life cycle starting with norm entrepreneurs, tipping points into cascades, and then internalization which translate their effects into beliefs that have domestic costs that deter external actions. If one looks at the historical development of norms against the slave trade in the 19th century or in favor of human rights in the second half of the 20th century, one can see that some states are constrained by the effect of norms on domestic opinion. Of course, one would expect such constraints to be stronger in democracies than in authoritarian states (though not totally absent in the latter – witness the effects of Basket Three of the Helsinki Process). Today, in cyber norms the world is largely at the first stage with the GGE as one of a number of important norm entrepreneurs. Perhaps norms are beginning to enter the second phase of a cascade. But the internalization of norms remains weak and limited to narrow elites. Moreover, there is no metric for measuring time in this hypothesized cycle, and indeed no guarantee of a cycle at all. For example, if relations between states become bitter over all, retrogression is certainly possible.

7. Next Steps

There is a wide range of views about the next steps for the GGE process. A first draft of a new report existed at the beginning of this year, but it was a long way from agreement. At the February 2017 Munich Security Conference, the current chair argued that the group should not try to rewrite the 2015 report, but should say more about the steps that states should take in peacetime. Some states suggested new norms dealing with data integrity and maintenance of the core structures of the Internet, but other states believed such expansion would open up a Pandora's box. There was general agreement about more discussion of confidence building measures and of capacity building, but also concern about how states will implement what has already been agreed.

If the GGE norms are to "cascade", states must raise awareness in a broader public. It is noteworthy that the Ukrainian disruption was not flagged and debated as possibly contrary to the GGE report of 2015. A representative of a small country argued that international law was crucial to small states without power, and made the case for more attention to the Tallinn Manual 2.0. The representative

of a major power said the GGE should dig deeper on questions such as what is meant by civilian processes. A UN under-secretary argued that the norm development process had to be broadened to include more countries to increase its legitimacy among the 193 UN members, and should relate cyber to other issues such as arms control in space and terrorism. In his view, the 5th GGE should dig deeper and then the 193 members of the UN should debate the report and task the next GGE to examine specific areas.

The GGE process reflects the positions of the states that nominate the experts and their strong views on state sovereignty. Certain normative issues are not discussed. The questions of contents and human rights are finessed by saying that all states agreed to the Universal Declaration of Human Rights though they interpret and implement it in different ways. Further progress on such subjects would probably be limited to plurilateral discussions among like-minded states rather than universal agreements. Other norms that may be ripe for discussions outside the GGE process could include a protected status for the core functions of the Internet; supply chain standards and liability for the Internet of Things; treatment of election processes as protected infrastructure; and more broadly norms for sub-LOAC issues such as crime and information warfare. All these are among the topics that may be considered by the new informal International Commission on Stability in Cyberspace announced by the Dutch Foreign Minister at Munich.

As member states contemplate next steps in the development of cyber norms they are faced with the dilemma of maintaining the effectiveness of the GGE while expanding participation in order to develop a broad legitimacy for norms that will help them to cascade and internalize. The answer may be to avoid putting too much burden of a burden on any one institution like the GGE. Norms are affected by their institutional homes, and in the long run many homes may be better than one. Progress on the next steps of norm formation may require simultaneous use of many of the nine cells for action identified in the matrix above. It will also require a strategy for mutual reinforcement among the cells. For example, the bilateral agreement between China and the US on cyber espionage for commercial purposes was taken up by the G20 as well in bilateral negotiations between China and a number of other states. In some instances, development of norms among like-minded states can lead to norms to which others may accede at a later point. In other instances, norms for security on the Internet of Things may benefit from codes of conduct where the private sector or non-profit stakeholders take the lead. And progress in some areas need not wait for others. The development of a regime complex may be more robust when linkages are not too tight. (See my “The Regime Complex for Managing Cyber Activities,” Research Paper #1, The

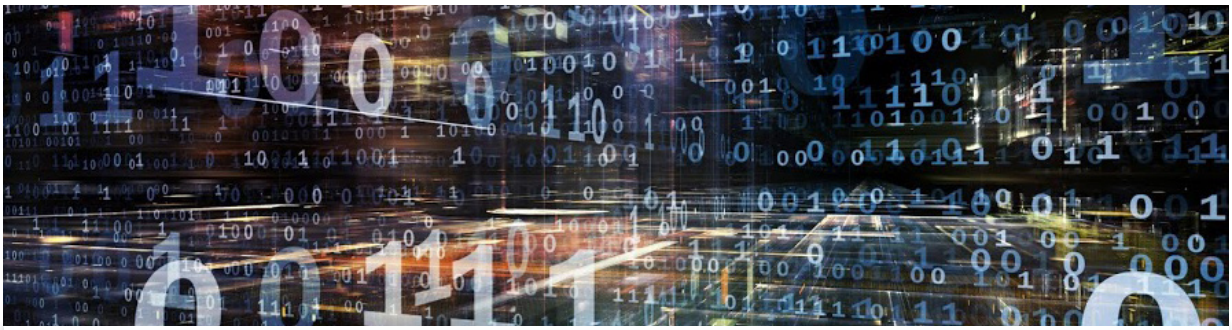
Global Commission for Internet Governance, 2014). Such flexibility would be incompatible with an over-arching UN treaty at this point. Expansion of participation is important for the acceptance of norms, but progress on norms will require action on many fronts. We are still in the early stages in the formation of normative constraints on cyber activity.

ICTSD
International Centre for Trade and Sustainable Development

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

The E15 Initiative

STRENGTHENING THE GLOBAL TRADE AND INVESTMENT SYSTEM FOR SUSTAINABLE DEVELOPMENT



Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows

Usman Ahmed and Anupam Chander

November 2015

E15 Expert Group on the Digital Economy

Think Piece

ACKNOWLEDGMENTS

Published by

International Centre for Trade and Sustainable Development (ICTSD)
7 Chemin de Balexert, 1219 Geneva, Switzerland
Tel: +41 22 917 8492 – E-mail: ictsd@ictsd.ch – Website: www.ictsd.org
Publisher and Chief Executive: Ricardo Meléndez-Ortiz

World Economic Forum
91-93 route de la Capite, 1223 Cologny/Geneva, Switzerland
Tel: +41 22 869 1212 – E-mail: contact@weforum.org – Website: www.weforum.org
Co-Publisher and Managing Director: Richard Samans

Acknowledgments

This paper has been produced under the E15Initiative (E15). Implemented jointly by the International Centre for Trade and Sustainable Development (ICTSD) and the World Economic Forum, the E15 convenes world-class experts and institutions to generate strategic analysis and recommendations for government, business and civil society geared towards strengthening the global trade and investment system for sustainable development.

For more information on the E15, please visit www.e15initiative.org/

Usman Ahmed is the Head of Global Public Policy at PayPal, Inc. Anupam Chander is Professor of Law at the University of California, Davis.

With the support of:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Canada

And ICTSD's Core and Thematic Donors:

Department for International Development

SWEDEN

Ministry of Foreign Affairs

Ministry of Foreign Affairs of Denmark
Ministère des Affaires étrangères du Danemark

Ministry for Foreign Affairs of Finland

Citation: Ahmed, Usman and Anupam Chander. *Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows.* E15Initiative. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum, 2015. www.e15initiative.org/

The views expressed in this publication are those of the authors and do not necessarily reflect the views of ICTSD, World Economic Forum, or the funding institutions.

Copyright ©ICTSD and World Economic Forum, 2015. Readers are encouraged to quote this material for educational and non-profit purposes, provided the source is acknowledged. This work is licensed under the Creative Commons Attribution-Non-commercial-No-Derivative Works 3.0 License. To view a copy of this license, visit: http://creativecommons.org/licenses/by-nc-nd/3.0/ or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.
ISSN 2313-3805

ABSTRACT

This paper addresses the question of whether it is possible to balance the need for a free flow of information across borders with legitimate government concerns related to public order, consumer privacy, and security. The paper begins by highlighting the risks associated with limitations on free information flows and the policy concerns that lead to these limitations. The paper then provides an analysis of the current international regime on cross-border information flows. The authors argue that specific binding trade language promoting cross-border flows— combined with continued international cooperation — will enhance, rather than undermine, public order, national security, and privacy.

CONTENTS

LIST OF ABBREVIATIONS

EU	European Union
GATS	General Agreement on Trade in Services
KORUS	U.S.-South Korea Free Trade Agreement
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
SPS	Sanitary and Phytosanitary
TISA	Trade in Services Agreement
TPP	Trans-Pacific Partnership
TTIP	Transatlantic Trade and Investment Partnership
US	United States
WTO	World Trade Organization

INTRODUCTION

The newest battleground in international trade is over the flow of information. Governments seek to exercise control over data flows as part of their broader efforts to assert what they see as "digital sovereignty." Some governments believe that the free flow of information poses a threat to public order, consumer privacy, or national security. Privately, many governments also worry about the competition for domestic businesses from foreign service providers, especially in domains traditionally insulated from foreign competition. In response, excessive government assertions of national borders in cyberspace may "balkanize" the Internet and erode the enormous benefits of this global medium. This tension raises a crucial question: is it possible to balance the free flow of information across borders with legitimate concerns related to public order, consumer privacy, and security?

The importance of the free flow of information across the world is difficult to overstate. The free flow of data, including across borders, is a key part of what makes the Internet the powerful force for information and economic development that it has proven to be over the past two decades.[1] McKinsey sees the Internet as "the great transformer," accounting for one-fifth of GDP growth in developed countries.[2] Perhaps McKinsey's most surprising conclusion is that "[m]ost of the economic value created by the Internet falls outside of the technology sector, with 75 percent of the benefits captured by companies in more traditional industries." As McKinsey describes, traditional industries benefit from "increased productivity, opportunities to expand into domestic and foreign markets, the means for radical product development, and the rapid deployment of game-changing ideas."[3] These game-changing ideas can be rapidly deployed globally, which is why digital trade has become a key part of modern economies.

The significance of the free flow of data becomes even more apparent when taking into account the crucial role of such flows in enabling the most recent technological innovations. Consider the following 10 innovations that rely on information flows:

1. **The Internet of Things.** Devices like an Apple Watch or a Samsung Smart TV — or even a Caterpillar 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.[4]

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, 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.[5]

This list demonstrates what is at risk if the free flow of information across national borders is eroded.

---

1 Business Roundtable, Putting Data to Work: Maximizing the Value of Information in an Interconnected World, Jan. 2015, http://businessroundtable.org/sites/default/files/reports/BRT%20Putting DataToWork.pdf

2 McKinsey Global Institute. Internet matters: The Net's sweeping impact on growth, jobs, and prosperity, May 2011; McKinsey Global Institute. The great transformer: The impact of the Internet on economic growth and prosperity, Oct. 2011.

3 McKinsey, Internet Matters at 7.

4 See, e.g., Kushner, David. "The Flight of the Birdman: Flappy Bird Creator Dong Nguyen *Speaks Out,*" Rolling Stone, Mar. 11, 2014, http://www.rollingstone.com/culture/news/the-flight-of-the-birdman-flappy-bird-creator-dong-nguyen-speaks-out-20140311#ixzz3gl1tVGLO; Curtis, Sophia. "Quarter of the world will be using smartphones in 2016," *The Telegraph*, Dec, 11 2014.

5 See, for example, http://www.engadget.com/2015/07/18/shenmue-3-kickstarter-record/.

Data localisation (requiring that Internet content providers store their data in country) and other barriers to cross-border flows of information tear at the fabric of global cyberspace. Information services that might have been supplied globally now must build out or pay for national data infrastructures in the countries in which they operate, carefully separating their services by country rather than offering a global service. This dramatically raises the costs of those services, often making them uneconomic to provide, particularly in the case of small- and medium-sized businesses.

Equally important, the free flow of information across borders not only benefits economic development and technological growth, but also supports free expression, as political dissidents often rely on foreign speech platforms to disseminate information.[6]

Even with these clear benefits of free flows of information, many governments have sought to curb these flows. The next section describes such efforts.

GOVERNMENT CONCERNS ABOUT DATA FLOWS

The Internet was developed largely without paying much heed to borders. But, even in the Internet's early days, governments found reasons to assert themselves with respect to cross-border flows of information. Authoritarian governments, in particular, fretted about the loss of control over speech they had previously exercised with respect to traditional media, such as newspapers, radio, and television. Even liberal governments sought to interfere with information flows when those flows ran afoul of national laws related to hate speech. A French court ruled that Yahoo! Inc. violated French law when it did not halt the auction of Nazi materials to a French audience. An effort in the United States (US) to target "foreign rogue websites" hosting copyright infringing content (the Stop Online Piracy Act) would have interfered with the domain name server system and potentially threatened the security of the Internet.

Some governments see the free flow of data across borders as a threat to national security, with reports about the National Security Agency (NSA) surveillance program arguably justifying those fears (though the NSA's reach is hardly contained in the US). Governments are also concerned about the threat to consumer privacy, when services gather personal data without consent and then use that data in a variety of ways around the world. Governments are driven also by the competitive challenge that the Internet poses to domestic businesses, owing to the ability of an Internet-based competitor to efficiently deliver products or services. Finally, some governments see the Internet as a threat to national efforts to control information, owing to its nature as a global platform for speech.

Increasingly government concerns over cross-border flows of information take the form of mandates for what has come to be called "data localisation"—efforts to keep information from leaving its home country. These mandates range widely. Australia, for example, requires that personally identifiable health information not leave the country without the consent of the individual to whom it pertains. British Columbia and Nova Scotia prevent personal information held by government agencies from leaving Canada without the consent of the data subject. The European Union (EU) permits personally identifiable information to leave the Union only under certain conditions, and it is considering tightening those conditions. Russia has begun putting in place a strict data protection regime, requiring that companies keep personal information of Russians in the country.[7] The Russian rules apply, for example, to Netherlands-based travel website Booking.com, which, according to the Russian authorities, "accumulates a large database of personal data of our citizens."[8]

Such national regulations around the world require information service providers to locate servers or other physical infrastructure in country in order to provide services.[9] These requirements result in the de facto blocking of information, as many firms, particularly smaller ones, are unable to locate servers in countries around the world.

6 Freedom of expression across national borders is one of the rights protected by the International Covenant on Civil and Political Rights, Art. 19(2): "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." On the importance of foreign speech intermediaries to dissidents in repressive states, see Chander, Anupam. "Googling Freedom," 99 *Calif. L*. Rev. 1, 2011.

7 Bauer, Matthias, Hosuk Lee-Makiyama, Erik van der Marel, and Bert Verschelde, Data Localisation in Russia: A Self-imposed Sanction. *ECIPE,* 2015. http://www.ecipe.org/app/uploads/2015/06/Policy-Brief-062015_Fixed.pdf.

8 Kurochkin, Dmitry, Marat Agabalyan and Saglara Ildzhirinova, of Dechert Russia LLC, Moscow, "Russia's New Server Localization Law: Implications for Foreign Companies," *World Data Protection Report,* Feb. 2015.

9 Chander, Anupam and Uyen P. Le. "Data Nationalism," 64 *Emory Law Journa*l 677, 2015.

THE CURRENT INTERNATIONAL REGIME FOR CROSS-BORDER DATA FLOW

Early international interventions on data processing recognized the importance of both privacy and cross-border data flows. In 1984, an executive at American Express described transnational data flows as the "lifeblood of virtually every major economic activity."[10] In its 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the Organisation for Economic Co-operation and Development (OECD) noted the need for privacy protection amidst the development of vast databases, but also worried that "disparities in national legislations [on privacy] could hamper the free flow of personal data across frontiers." The OECD recognised that "transborder flows of personal data contribute to economic and social development" and that "domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows." The Council of Europe's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) required state parties to enact laws to protect privacy. At the same time, Convention 108 prohibited any party from "prohibit[ing] or subject[ing] to special authorisation transborder flows of personal data going to the territory of another Party." While open to all states for membership, Convention 108 remained exclusively European, until the addition of Uruguay as a member state in 2013.

The WTO, by contrast, counts most of the countries of the world as members. When the WTO came into being in 1995, the Internet was in its relative infancy as a global communications platform. The General Agreement on Trade in Services (GATS), negotiated in the early 1990s, did not explicitly deal with data flows across borders. The focus, instead, was on the general provision of services across borders and across multiple modes of service provision. Yet, the characterisation of how services might be provided across borders—including "cross-border supply" and "consumption abroad"—makes clear that the cross-border supply of information services was intended to be encompassed by GATS.

Indeed, the first WTO decision focused on GATS makes this clear.[11] In *United States – Gambling,* the WTO's Appellate Body ruled that US rules barring the cross-border supply of Internet-based gambling services were subject to the services liberalisation obligations of GATS. The US argued that even so, its rules were necessary to prevent underage gambling and to reduce fraud and money laundering and were thus an exception to the GATS obligations as a regulation of public morals. The WTO sided with Antigua in part, because US-based gambling services were treated differently from Antiguan Internet-based services and authorized Antigua to engage in limited retaliatory sanctions against the US. The application of the WTO agreements to information services is further confirmed in the WTO's ruling in the *China – Publications and Audiovisual Products* dispute. There, the US challenged a number of Chinese restrictions on the distribution of certain publications and audiovisual products, restrictions designed ostensibly to serve Chinese state censorship requirements. China argued that the electronic distribution of audio products was not covered by the agreement, but the Appellate Body concluded that China's commitment "would encompass distribution in electronic form."[12] The WTO went on to conclude that the Chinese restrictions were barred by that country's free-trade commitments.

Whether GATS applies to a particular measure that might restrict information flows depends on whether the country applying that measure has scheduled a relevant liberalisation commitment. Some 77 WTO members have made commitments on "data processing," but the scope of these commitments is not entirely clear, because computer-mediated services can be characterised in multiple ways, some of which might be liberalised and others not.[13] It could be argued, for example, that an accounting service provided online should not be considered "on-line information or data processing" when there is a separate category for "accounting services."

The GATS provides that states might impose measures that would otherwise run afoul of the agreement if necessary to comply with laws protecting the privacy of individuals.[14]

10 Drake, William. "Territoriality and Intangibility: Transborder Data Flows and National Sovereignty," in Beyond National Sovereignty: International Communications in the 1990s, edited by Kaarle Nordenstreng and Herbert I. Schiller, 259, 271, 1993.

11 Burri, M. & Cottier, T. Introduction: Digital technologies and international trade regulation, in Trade Governance in The Digital Age, p. 4, 2012.

12 China — Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products, Dec. 21, 2009, ¶ 377. Chander, Anupam. The Electronic Silk Road: How the Web Binds the World in Commerce 156, 2013.

13 Berry, Renee and Matthew Reisman, Policy Challenges of Cross-Border Cloud Computing p. 22 (US International Trade Commission, May 2012) (noting that 60 countries have commitments on "on-line information and/or data processing," while 76 have commitments in for data processing). Our own review suggests that there are as many as 77 countries with "CPC 843" commitments for data processing services, though some of these commitments may be narrower than all data processing services.

14 General Agreement on Trade in Services, Art. XIV(c)(ii).

This exception to the free-trade obligations under GATS, however, will likely be interpreted narrowly so as not to undermine the agreement. After all, it is easy to claim that privacy can be protected only if information remains within a country, but it is much harder to demonstrate that this is necessary to protect privacy, an issue to which we return in Section 5 below.

HOW 21ST CENTURY AGREEMENTS WILL ADDRESS CROSS-BORDER FLOWS OF INFORMATION

The issue has also found its way into recent debates outside the WTO. The European Court of Justice has considered issues of cross-border Internet gambling provided from within the EU, but has been inconsistent in requiring liberalisation of trade.[15] With the US-South Korea Free Trade Agreement (KORUS), the US began asking its trading partners to explicitly affirm the value of the free flow of information. KORUS states: "Recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders." While the language is hortatory, it still provides a basis for political pressure in case of noncompliance.

There are several trade agreements currently being negotiated that will likely incorporate language designed to safeguard cross-border information flows from national protectionist barriers. Because of their focus on such contemporary issues, these agreements have been described as "21st century trade agreements." While the negotiations are ongoing and secret, both leaks of negotiating texts and official statements of negotiating objectives shed some light on their likely content.[16] This section will look at the issue of cross-border information flows in three major ongoing trade negotiations: the Trade in Services Agreement (TISA), the Trans-Pacific Partnership (TPP), and the Transatlantic Trade and Investment Partnership (TTIP).

TRADE IN SERVICES AGREEMENT (TISA)

The TISA is a plurilateral agreement being negotiated between 24 parties, including the EU, the US, and a diverse group of countries, such as Pakistan, Panama, South Korea, and Turkey.[17] TISA negotiating parties represent nearly 1.6 billion people and a combined GDP that is nearly two-thirds of the world's economy.[18] TISA seeks to build on the language of the GATS and further liberalise service sectors, including telecommunication, delivery, and technology.[19] In July 2015, Wikileaks published a set of documents from the TISA negotiations.[20]

The Annex on Electronic Commerce includes a proposal from Canada, Colombia, Japan, Taiwan, and the US that would strongly discourage data localisation mandates. The proposal would prohibit parties from blocking cross-border information transfers, including personal information when the activity is carried out in connection with the service supplier's business.[21] Colombia and the US further propose language that would bar local infrastructure requirements for cross-border information service providers.[22] Japan similarly proposes that no state be permitted to require information service suppliers to establish a local presence as a condition to supply services. Such TISA obligations would bar efforts to force information service providers to locate data servers within particular countries, subject to exceptions for national security and conservation of living and natural resources.[23]

The free flow of information obligations set forth in the Electronic Commerce chapter are still subject to negotiation and possible narrowing. For example, South Korea has proposed that movement of information across borders must be based on "informed consent," with full protection and recourse under the law in regards to use of personal information.[24] We return to the issue of consent in the final section below.

15 Lovejoy, Katherine A. "A Busted Flush: Regulation of Online Gambling in the European Union," 37 *Fordham Int'l L.J.* 1525, 2014.

16 De Pillis, Lydia. "The catch-22 of trade deals done in secret," *Washington Post*, May 15, 2015.

17 European Commission, Trade in Services Agreement http://ec.europa.eu/trade/policy/in-focus/tisa/

18 Government of Canada, Trade in Services Agreement http://www.international.gc.ca/trade-agreements-accords-commerciaux/topics-domaines/services/tisa-acs.aspx?lang=eng

19 Office of the United States Trade Representative, Trade in Services Agreement https://ustr.gov/TiSA#

20 Dayen, David. "The Scariest Trade Deal Nobody's Talking about just Suffered a Big Leak," *New Republic* (July 4, 2015); Wikileaks, July TISA Release https://wikileaks.org/tisa/.

21 TISA Annex on Electronic Commerce https://wikileaks.org/tisa/ecommerce/05-2015/page-3.html

22 Id. at pg.8 https://wikileaks.org/tisa/ecommerce/05-2015/page-8.html

23 On the national security exceptions to the WTO agreements, see Abdel-Latif, Ahmed. How to deal with the security exception in the digital economy, E15 Initiative paper (2015)

24 Id.

TRANS-PACIFIC PARTNERSHIP (TPP)

Another diverse group of countries has concluded negotiating a text for the TPP. The 12-country partnership among a group of Pacific nations from Australia to Vietnam covers a zone with 39 percent of the world's GDP.[25] The subjects of the negotiations are quite broad, dealing with cross-cutting issues, including agriculture, customs, and electronic commerce.[26]

If enacted, the TPP will include some of the strongest general commitments to the free flow of data in the world trade system. TPP member states make two broad commitments in this area: first, to permit the cross-border transfer of information, and second, to not impose regulations that require companies from TPP member states to use local computer servers. Specifically, Article 14.11 mandates that member states must allow the cross-border transfer of data. However, the TPP permits restrictions on that transfer if the restrictions are (1) designed to achieve a legitimate public policy objective; (2) not applied in a manner that constitutes unjustifiable discrimination; and (3) not greater than those required to achieve the objective. The provisions do not apply to the information that TPP member governments themselves collect or, relatedly, to government procurement.[27]

In sum, legitimate public policy objectives such as privacy can limit cross-border flow of data or require the use of a local computing infrastructure, as long as they meet the criteria specified above. But if protection of consumer or business privacy can be achieved consistently with international data flows, then such flows should be allowed. This lends support to the U.S. government's characterization of the TPP as "the most ambitious trade policy ever designed for the Internet and electronic commerce."[28]

THE TRANSATLANTIC TRADE AND INVESTMENT PARTNERSHIP (TTIP)

The TTIP represents an effort to create a liberal trade zone across the Atlantic between the US and the EU.[29] The agreement would cover one-third of global goods and services trade as well as nearly half of global economic output.[30] Also, like the TPP, the negotiation covers a wide array of subjects.[31]

While the negotiations have been conducted largely in secret, the British Broadcasting Corporation (BBC) released a document described as the EU's "initial offer" in the negotiations with respect to the schedule of commitments, but excluding its offers with respect to modes 1 and 2 (cross-border trade in services and consumption abroad).[32]

It is quite likely that the US proposal on data flows will be similar to the one it proposed in both TISA and the TPP, both because of the strategic importance of information flows and the inherent usefulness of harmonised trade agreements. The EU has stated that it believes that its data protection laws will not be affected by the TTIP, but the issue remains a focus of the discussions. In March 2015, Juhan Lepassar, head of EU Digital Commissioner Andrus Ansip's cabinet, stated that the EU is on the same page as the US on information flows and the issue could be considered in the TTIP negotiations.[33]

The European Parliament has recommended that the cross-border flows of data provisions in the TTIP should be consistent with existing EU privacy law.[34] We turn now to the question of whether the free flow of data across borders is indeed compatible with privacy and security.

25 United States Trade Representative, The Trans-Pacific Partnership: Economic Benefits, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2013/December/TPP-Economic-Benefits.

26 Stoller, Matt. Trans-Pacific Partnership: The biggest trade deal you've never heard of, Oct. 23, 2012.

27 TPP Art. 14.2.

28 https://medium.com/the-trans-pacific-partnership/electronic-commerce-87766c98a068; David Fidler, The TPP's Electronic Commerce Chapter: Strategic, Political, and Legal Implications, Council on Foreign Relations Blog, Nov. 9, 2015, http://blogs.cfr.org/cyber/2015/11/09/the-tpps-electronic-commerce-chapter-strategic-political-and-legal-implications/.

29 Office of the United States Trade Representative, Transatlantic Trade and Investment Partnership https://ustr.gov/ttip

30 Office of the United States Trade Representative, Fact Sheet: United States to Negotiate Transatlantic Trade and Investment Partnership with the European Union https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2013/february/US-EU-TTIP

31 Directorate-General for Trade of the European Commission, http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153635.pdf.

32 Campbell, Glenn. "TTIP: Transatlantic trade deal text leaked to BBC," BBC News, Feb. 2015. http://www.bbc.com/news/uk-scotland-scotland-politics-31631461

33 Fleming, Jeremy. "Brussels makes overture on 'data flow' agreement in TTIP," EurActiv.com, Mar. 30, 2015.

34 European Parliament, Resolution of 8 July 2015 containing the European Parliament's recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP) (2014/2228(INI)): to ensure that the EU's acquis on data privacy is not compromised through the liberalisation of data flows, in particular in the area of e-commerce and financial services, while recognizing the relevance of data flows as a backbone of transatlantic trade and the digital economy; to incorporate, as a key point, a comprehensive and unambiguous horizontal self-standing provision, based on Article XIV of the General Agreement on Trade in services (GATS), that fully exempts the existing and future EU legal framework for the protection of personal data from the agreement without any condition that it must be consistent with other parts of the TTIP; to negotiate provisions which touch upon the flow of personal data only if the full application of data protection rules on both sides of the Atlantic is guaranteed and respected to cooperate with the United States in order to encourage third countries to adopt similar high data protection standards around the world…

PROTECTING PRIVACY AND SECURITY

Critics of cross-border information flows argue that such flows jeopardise privacy and national security. We suggest that privacy and national security can be protected in international trade agreements if they are properly structured. We go further to argue that international flows can even strengthen privacy and national security, while avoiding the economic losses that result from cutting off foreign suppliers of goods or services.[35]

We begin by observing that international trade law has long dealt with concerns about consumer protection in a world of liberalised trade. Take the case of what is perhaps the most important product area related to consumer protection—food. Each member of the WTO crafts its own food safety standards, and imposes those standards on the food it imports. The WTO's Sanitary and Phytosanitary (SPS) Measures Agreement affirms nations' right to set their own food safety standards[36] Food safety standards, however, cannot be arbitrary. Rather, they must be based on science, so that they are not used as a disguise for protectionism.[37] The SPS Agreement also encourages nations to agree on international standards, guidelines, and recommendations, although again it permits nations to establish higher health standards as long as they are based on science.[38] The food safety standards demonstrate that even when international trade law applies, "foreign products can be denied market access, unless they meet the established requirements."[39] The ultimate result is this: consumers have access to food from around the world, while governments can still restrict unsafe foreign or domestic foods.

Similarly, can we allow global information flows and still protect public order, privacy, and security? It is important to note that the TISA E-commerce chapter draft does not ban national public order, privacy, and security rules. Rather, the draft rules target government regulations that require foreign service providers to keep information within the country. The draft rules provide that no country can require a foreign service supplier to, "store or process data in its territory."[40] Relatedly, a member state could no longer prevent a foreign service supplier from transferring information outside that member state. Thus, the TISA or the TPP would interfere with privacy rules, for example, only to the extent that they require that information stay within a country.

The question then is whether rules that bar information from being placed outside the country advance the privacy and security of that country's citizens. Like money stored under the mattress, information is not necessarily more secure if it is kept at home. Criminals may gain illicit access even if the information is stored within the individual's home country. After all, criminal hackers do not stop at national borders. Indeed, data localisation obligations reduce the choice of information providers available to consumers and businesses. As a recent cover feature of the *IEEE Computer Society* magazine observes, "The most common threats to data in the cloud involve breaches by hackers against inadequately protected systems, user carelessness or lack of caution, and engineering errors."[41] Thus, prohibitions on data localisation increase access to service providers from around the world, allowing individuals and businesses to choose service providers with the best privacy and security practices.

Furthermore, countries can still insist that their public order, privacy, and security requirements be followed by foreign providers wherever they store or process data. This is a common practice in cross-border outsourcing arrangements, where the outsourcing provider commits to protect information consistent with local standards. Indeed, permitting cross-border flows is likely to enhance privacy and security as it allows consumers and businesses to select from a wider range of providers that are subject to global competition.

One approach has been to require a person's consent before his or her personal information can be transmitted across borders. But, this approach is likely to prove a major impediment to many kinds of information flow. We do not typically require a special consent before a consumer purchases a good, or even food, from a foreign source. There are reasons to believe that a consent requirement for information transfer will prove difficult to satisfy, and thus itself function effectively as a barrier to cross-border flows of information. It may be difficult to know, for example, whether consent has been meaningfully obtained, as companies simply add "cross-border data transfer" to their lengthy list of terms and conditions. Imagine the difficulties of obtaining such consent when it comes to devices that capture information about more than one person. Many

35 For an important discussion of the application of the General Agreement on Trade in Services to national privacy standards, see Weber, Rolf H., Regulatory Autonomy and Privacy Standards. Under the GATS, Asian Journal of WTO & International Health Law and Policy, Vol. 7, No. 1, pp. 25-48, March 2012.

36 Agreement on the Application of Sanitary and Phytosanitary Measures (SPS Agreement), Art. 2.1.

37 SPS Agreement, Art. 2.2.

38 SPS Agreement, Arts. 3.1 & 3.3.

39 Mavroidis, Petros C. Trade in Goods 709. 2d ed., Oxford 2012.

40 TISA Draft, Art. 9, https://wikileaks.org/tisa/ecommerce/05-2015/page-8.html.

41 Ryan, Patrick S., Sarah Falvey, and Ronak Merchant, "When the Cloud Goes Local: The Global Problem with Data Localization," *COMPUTER,* Dec. 2013, at 54, 56.

applications will involve personal data not only of the contracting counterparty, but also of third parties. An email, for example, might include personal information not only about the person receiving the message, but also about others, as might a device that monitors a particular environment. Will a self-driving car need the consent of every other inhabitant of a vehicle it encounters if the self-driving car processes information about road conditions remotely?

Finally, both the TPP released text and the TISA draft proposal include language that would oblige member states to adopt consumer protection laws and promote cooperation among national consumer protection agencies.[42] Both texts also require each member state to provide a legal framework to protect personal information.[43] Ultimately, the protection of privacy and security online will turn not on counterproductive and mostly futile bars against cross-border information flows, but on both international cooperation between states and international competition between suppliers.

On the issue of public order, trade policy could adopt a model used for aspects of Internet governance, namely the multi-stakeholder process with publication of best practices.[44] Such a process could help governments understand similarities and divergences in the treatment of content on the Internet. Governments could share tactics on how to effectively target and combat content that is considered a threat to public order, while avoiding unilateral executive branch censorship determinations likely to violate the freedom of expression. For example, the positives and negatives of proposals for data localisation, domain name takedowns, or filters could be discussed in an open forum before domestic actions are taken. Such a discussion would not create binding commitments, but rather improve the sharing of information, including best practices. Such informal discussions could greatly improve outcomes for governments in their efforts to support domestic public order concerns, and might reduce actions that would harm the open-interconnected network that is the Internet.

While privacy laws across the world will likely continue to differ, there are several related principles that are shared across regions. The importance of dignity, free association, and the security of personal data are universally recognised. These ideas can and should be included as part of trade discussions about the free flow of information. Even if trade policy cannot achieve harmonisation on privacy rules, it can promote the interoperability of different privacy rules. The existing US-EU Safe Harbor enables US businesses that would not otherwise qualify under the EU's data protection directive to meet some of the important goals of the EU framework, subject to enforcement by the Federal Trade Commission.[45] This system thus operates to create interoperability between two otherwise different systems.

CONCLUSION

Cross-border information flows underlie nearly every aspect of the modern economy. Governments are legitimately concerned with ensuring that cross-border information flows support public order, national security, and consumer privacy. Trade policy has only begun to address this issue in the past few years, and there has to date been binding language on the topic. We argue that specific binding trade language on cross-border information flows — combined with continued international cooperation — will enhance, not undermine, public order, national security, and privacy.

42 TPP, Art. 14.7; TISA Draft, Art. 3.

43 TPP, Art. 14.8; TISA Draft, Art. 4(2).

44 Waz, Joe and Phil Weiser. " Internet Governance: The Role of Multistakeholder Organizations," 10 *J. on Telecomm & High Tech L.* 331, 338, 2013.

45 Mcbride, Naomi, Lisa J. Sotto, and Bridget Treacy, Privacy & Data Security: The Future of the US-EU Safe Harbor, Hunton Privacy Blog, 2013. Available at: https://www.huntonprivacyblog.com/files/2013/12/Privacy-Data-Security-The-Future-of-the-US-EU-Safe-Harbor.pdf

ADDITIONAL REFERENCES

Makiyama, Hosuk Lee. "Digital Trade in the U.S. and Global Economies," *European Centre for International Political Economy*, accessed February 10, 2015, http://www.ecipe.org/app/uploads/2014/12/USITC_speech.pdf.

Kuner, Christopher. Transborder Data Flow Regulation and Data Privacy Law. Oxford, 2013.

Pélissié du Rausas, Matthieu. et al., "Internet matters: The Net's sweeping impact on growth, jobs, and prosperity," *McKinsey Global Institute,* May 2011, http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.

Castro, Daniel andMcQuinn, Alan. Cross-Border Data Flows Enable Growth in All Industries, Feb. 2015, http://www2.itif.org/2015-cross-border-data-flows.pdf.

Meltzer, Joshua. "The Internet, Cross-Border Data Flows and International Trade," *Asia & the Pacific Policy Studies*, vol. 2, no. 1, pp. 90–102.

Chander, Anupam. The Electronic Silk Road: How the Web Binds the World Together in Commerce. Yale, 2013.

Implemented jointly by ICTSD and the World Economic Forum, the E15Initiative convenes world-class experts and institutions to generate strategic analysis and recommendations for government, business, and civil society geared towards strengthening the global trade and investment system for sustainable development.

International Centre for Trade and Sustainable Development

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Software is Eating World Trade, But Will Fragmentation Bite Back?

May, 2017

By Usman Ahmed[i]

1. Introduction

Venture Capital Marc Andressen famously quipped in 2011, "Software is eating the world."[ii] Research that we have been conducting at PayPal demonstrates that software, and in particular Internet-enabled software, is eating every sector and segment of the global trade value chain.[iii] Internet-enabled trade has resulted in a number of positive developments: enhanced growth for overlooked sectors and segments of society, as well as small and medium sized enterprises (SMEs) that have traditionally been unable to reap the benefits of global globalization. But, this positive story is limited by several factors, one of which is the fragmentation of the Internet. Divergent national rules on technical, social, and policy issues undermine the global opportunity provided by the Internet. Resolving the issues surrounding Internet fragmentation would help to fully unlock the positive potential of Internet-enabled trade.

2. The Good Story: Growth and Trade

The Internet has changed the calculus of who can fully engage in globalization by eliminating traditional barriers like distance, trust, and communication. Breaking down these barriers can enable businesses in sectors outside of manufacturing and agriculture to trade for the first time. Smaller businesses that traditionally could not find customers or establish relationships with international customers now can. Moreover, businesses no longer need to locate in large cities or coastal areas if they want to engage directly in trade.

Pioneering research done by eBay in 2012 demonstrated that even the smallest retail business could now go on the eBay platform and sell physical products around the world.[iv] Research we have been doing at PayPal builds upon the work of eBay, demonstrating that the benefits of digital are not limited to a sole platform or business model.

We analyzed a sample dataset of over 29,699 small businesses using PayPal across the United States from 2015 and 2016. We did a robustness check using a broader dataset of over 100,000 small businesses. We define small businesses in the PayPal dataset as those selling between $30,000 and $3

million per year. The National Small Business Association's 2016 year-end economic report found that over 65% of small businesses were in this revenue range.[v] We found that small businesses that used PayPal demonstrate growth and exporting trends that are significantly different from traditional small businesses.

2.1 Small Business Export and Grow

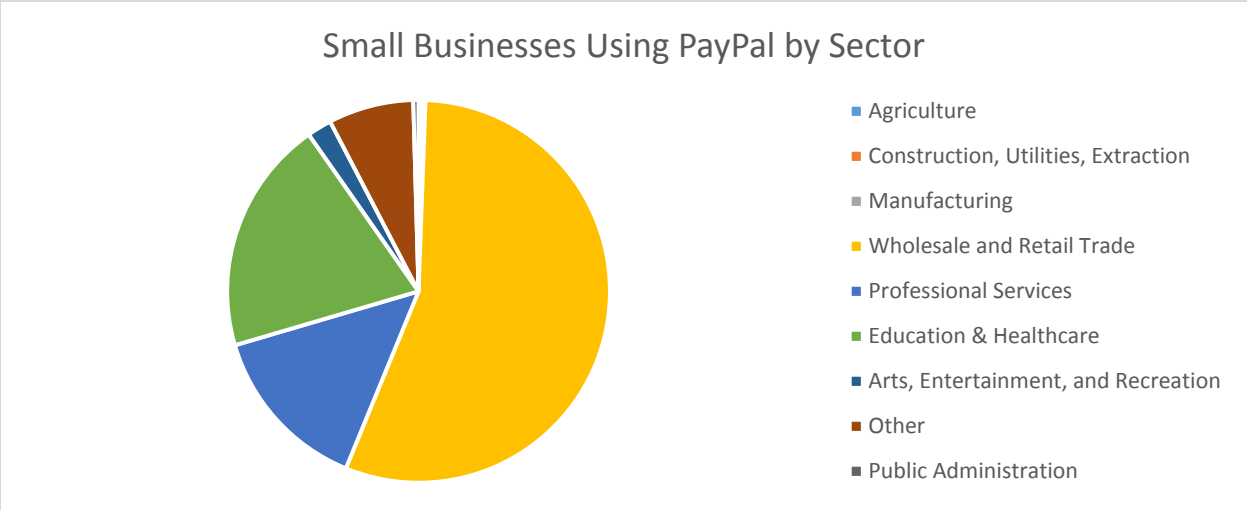
Less than 5% of small businesses in the US engage in exporting.[vi] Businesses that use PayPal are disproportionately likely to be engaged in exporting; over 75% of the small businesses in our sample data set engaged in exporting in 2016. This makes intuitive sense. The Internet is a borderless platform that enables instant connection with customers on the other side of the world.

Exporting products and services yields enhanced productivity and employment.[vii] Literature on the gains from exporting have looked at total factor productivity (TFP) and found that exporters experience a premia of 4-18% in TFP vis-à-vis their non-exporting counterparts.[viii] We found that exporters using PayPal experienced a revenue premia of 43% over non-exporters using PayPal, and a 421% premia over traditional small businesses. Exporters using PayPal grew 32.8% year-over-year in 2016.

2.2 Services Business Export and Grow

Most research on exporting has looked at agriculture and manufacturing, in part because services were not often traded across borders. Services typically required physical presence in order to be delivered across borders. Retail sales were conducted in person; administrative services required the employees to be in the same office; and, technical services required onsite support. These were considered nontradeable services. Research from eBay has demonstrated that retail is now no longer nontradeable. Our research now demonstrates that the impact of the Internet on trade extends to nearly every subsector within services.

We excluded all eBay businesses from our sample set to eliminate the effect of the marketplace and to expand the insights beyond retail trade. While a large number of the small business exporters that we looked at were in the retail sector, we also found a significant number of businesses in professional services, education, the arts, and other categories. The chart below reflects the sectoral subdivisions of businesses we looked at on PayPal based upon the North American Industry Classification System (NAICS).



In comparison, a recent survey by the Export-Import Bank of exporting small businesses found that just 15% export only services. Sean Luke, Vice President of Sales and Marketing at the Export-Import Bank stated that, "this fits our understanding that **many firms that deal in services struggle to find safe ways to export**, while firms that export physical goods are often able to do so".[ix]

2.3 Non-Urban Businesses Export and Grow

Economies across the US did not grow equally in 2015; the most recent year for which data on state-by-state growth is available. Coastal states with large city centers like California, Florida, and Massachusetts grew above the national average. Whereas heartland states with large rural areas like Louisiana, Oklahoma, and North Dakota saw growth rates well below the national average and in some cases negative growth rates.[x] This recent data demonstrates a trend that has been occurring for some time, which is the clustering of growth and trade in a few city centers, generally located on the coasts.

The Internet is enabling small businesses in the heartland and in rural areas to grow at unprecedented rates. Heartland small business exporters actually outperformed their coastal counterparts in 2016. In US towns with less than 50,000 people, small businesses using PayPal were just as likely to export and had similar growth rates the exporters had similar growth rates to their large city counterparts.

3. The Not So Good Story: Fragmentation and Localization

Fragmentation has been a concern for stakeholders since the inception of the Internet. The initial concern was with technical fragmentation (the use of alternative protocols), but now government policies related to the content layer of the Internet is where fragmentation concerns are increasingly being raised.

In recent years, a range of legal and regulatory proposals in countries around the world have sought to limit or prohibit the transmission of cross border data flows.[xi] These restrictions can come in the form of broad-based economy wide legislation or targeted sectoral regulation. Oftentimes, these proposals are meant to address important policy concerns, but the result can sometimes be to restrict legitimate trade.

Some governments are concerned about national security and therefore utilize localization mandates to prevent flows coming from certain jurisdictions or through certain entities. Concerns about dissent and speech can also motivate localization mandates. Governments are also concerned about privacy, in particular when the Internet enables companies to engage in the gathering and use of personally identifiable information. Governments can also be motivated to act by competitive concerns about the proliferation of large foreign Internet companies. Lastly, as the Internet pervades every sector of the economy, traditional regulation of transportation, health care, financial services, and other sectors can also run head long into the global nature of the Internet.

The reaction of many governments to these concerns has been to propose some form of data localization. The proposals can be as innocuous as requiring the use of a local domain name to a blanket requirement to localize all services and systems. Requirements can be sectoral or economy wide. The most commonly discussed proposal in the literature is a requirement to locate domestic consumer information on local servers.

Data localization has negative implications from both an economic and security perspective. A 2014 analysis by the European Centre for International Political Economy found that if the EU were to implement proposed data protection measures, GDP and foreign investment would decline by nearly one-half of one percent and four percent, respectively.[xii] Moreover, security networks are only as vulnerable as their weakest link. Proliferating data centers will reduce the ability of businesses to maintain security and newly formed data centers will be particularly subject to security threats.

The target of these data localization measures are often large companies that are sectoral leaders, have large technology footprints, or provide key Internet services. The research described in the section above, however, demonstrates that SMEs, non-traditional sectors, and underserved businesses would also be hit by localization measures that fragment the global Internet. That is why getting the global rules for Internet-related regulation and legislation is so critical.

4. The Tool of Trade Policy: One Among Many in the Fight against Fragmentation

Many trade scholars view data localization as a "new issue," but it is merely a modern manifestation of a classic trade concern. Domestic policymakers have for many years responded to foreign competition with requirements to localize. Recent data localization requirements have led trade policymakers to prioritize commitments on cross border data flows in modern trade agreements.

The Trans-Pacific Partnership (TPP) was the first trade agreement to include binding language on data flows. Unfortunately, the US voted to withdraw from the TPP and the future of the agreement remains unknown. But, it is worth noting that the TPP language was not perfect. The Electronic Commerce chapter of the TPP, which contains the important language on free flow of information and localization explicitly excludes "financial institutions" and "cross border financial services."[xiii] Meaning that the financial services sector would not be able to take advantage of the TPP language.

The Trade in Services Agreement (TISA) is a plurilateral agreement being negotiated between a diverse group of countries including Pakistan, Panama, South Korea, and Turkey. A leaked version of the Annex on Electronic Commerce includes a proposal from Canada, Colombia, Japan, Taiwan, and the US that would strongly discourage data localization mandates.[xiv]

The Transatlantic Trade and Investment Partnership (TTIP) is an effort to create a free trade zone across the Atlantic between the United States and the European Union. It seems likely that the TTIP would include a US proposal on data flows similar to the one it proposed in both TISA and the TPP. Notably, The European Parliament has recommended that the cross border flows of data provisions in TTIP should be consistent with existing European Union privacy law.[xv] Political changes in the US and UK have thrown both the TISA and the TTIP into limbo for the time being.

Despite the struggles to get individual trade agreements ratified, trade policy would seem to be an ideal tool to govern cross border data flows and prohibit improper localization requirements. Trade law contains important exceptions for national security and privacy. The jurisprudence of trade law, however, enables a reviewing court to "look behind the veil" of national legislation to determine if it is being, "applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade."[xvi] This standard is objective and one that should enable legitimate policy regimes to stand, while challenging regimes that are actually designed to further protectionist motives.

Trade policy on data localization does not take place in a vacuum; it interweaves with conversations in other stakeholder fora where issues related to fragmentation are discussed. Telecommunication stakeholders like the International Telecommunications Union will note when countries sign binding trade agreements on cross border data flows. Multistakeholder fora like the Internet Governance Forum have taken a strong interest in trade policy in recent years. Moreover, as the Internet begins to transform traditionally regulated sectors like health care and financial services, international financial and health regulatory bodies will also likely reference anything done in the trade policy context.

Stakeholders in these other fora are concerned about rules being created in the trade arena that will limit the flexibility to create rules in other contexts. This concern, however, should be assayed by the idea that trade policy is primarily focused on preventing domestic legislation that is "more trade restrictive than necessary," not to prevent domestic policymakers or other international fora from creating rules related to security, privacy, consumer protection, or other matters of domestic and international concern. Trade policy has successfully played this role in other sectors like food safety and there is no reason to think that a similar role could not be played in the Internet context.

Trade policy should be considered just one tool among many in the fight against fragmentation. Discussions among telecom regulators, finance regulators, health ministers, multistakeholder fora, and countless other international discussions will also touch upon the topic of fragmentation. These discussions should inform one another, and each should champion the vision of a single interconnected Internet.

5. Conclusion

The Internet does not discriminate based upon size, sector, or location of a business. A small services business in a rural town can now leverage the Internet to grow and export. The Internet presents an unprecedented opportunity for inclusive growth. If we truly want to see a democratization of globalization, however, we need a truly global Internet.

The problem of fragmentation is a global one. Domestic policymakers are concerned about the consumer protection, privacy, and security practices of Internet-related services. The use of data localization to mitigate these concerns, however, can have negative economic and security consequences both for domestic and international stakeholders.

Trade policy has a role to play in preventing the further fragmentation of the Internet, but it is a limited role. Trade policy is designed to ensure that domestic policymaking does not create unnecessary barriers to trade. Trade policy also contains important exceptions for issues of domestic concern like privacy and security. This tool should work alongside policy created by international policymakers as well as multistakeholder fora in an effort to limit fragmentation.

---

[i] Head of Global Public Policy, PayPal; Adjunct Professor of Law, Georgetown University
[ii] Marc Andressen, Why Software Is Eating The World, Wall Street Journal (Aug. 20, 2011)
[iii] PayPal, Democratizing Globalization (2017)
[iv] Lendle, et. al. There Goes Gravity, The Economic Journal (2016)
[v] NSBA, 2016 Year-end Economic Report
[vi] SBA Office of Advocacy, US Small Business Profile, 2016
[vii] Andrew B. Bernard and J. Bradford Jensen, Exporting and Productivity, NBER Working Paper 7135 (May 1999)
[viii] Andrew B. Bernard and J. Bradford Jensen, Exceptional Exporter Performance: Cause, Effect, or Both?, Journal of International Economics (1999)
[ix] Sean Luke, 7 Exporting Takeaways from the 2016 Small Business Exporting Survey (May 7, 2016)
[x] SBA Office of Advocacy, US Small Business Profile, 2016
[xi] Ahmed & Chander, Information Goes Global, E15 Think Piece (Nov. 2015)
[xii] ECIPE, The Costs of Data Localisation: Friendly Fire on Economic Recovery (2014)
[xiii] TransPacific Partnership, Chapter 14.1
[xiv] TISA Annex on Electronic Commerce, Wikileaks release June 3, 2015
[xv] European Parliament, Resolution of 8 July 2015 containing the European Parliament's recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP) (2014/2228(INI))
[xvi] General Agreement on Trade in Services, Article XIV

The Fragmentation Mismatch:

Deficiency of Dealing with Fragmentation through Trade Policy

By Hosuk Lee-Makiyama

1. The context to fragmentation

As we are two decades into the digitalisation, data is an established concept in trade policy. Yet fragmentation of the internet is still a matter of great urgency: In pursuit of "re-territorialisation" of digital economic space, 86 data localisation measures are applied in at least 36 jurisdictions (a number that has quadrupling in fifteen years).[1] The eagerness to regulate every new innovative use of data have created regulatory divergences between the economies. Even the trade agreements that are supposed to curb these divergences are fragmented and impose different standards due to irreconcilable policy objectives.

Internet is not the first time in history where a pre-existing model of global governance is caught in a dilemma between maintaining an open economic order, and a sovereigns' right to regulate. But the mismatch between internet and global economic governance is a unique challenge: The rule based system is based on a "bottom-up" approach, that integrates national markets through various instruments of cooperation between them. However, internet was already an open and seamlessly global architecture by the time it became relevant to the trading and financial systems. Hence, bilateral or regional integration (perhaps best exemplified by the Digital Single Market in the European Union) could lead to fragmentation by atomising an open structure that was already global at onset.[2]

This note illustrates how fragmentation occurs across several layers of the economy, serving national objectives on security, political authority and market stability. Such objectives go beyond historical pretexts for economic protectionism. So far, 'hard', strategic objectives have

[1] For a full catalogue of data localisation measures, see ECIPE *Digital Trade Estimates*, accessed at: http://ecipe.org/DTE
[2] Legrain, Lee-Makiyama, *Open Up: How to Fix the Flaws in the EU's Digital Single Market*, OPEN, 2017

trumped the self-punitive damage brought by fragmenting the internet, where data localisation generate net economic losses from 0.7 to 1.7% of GDP, from severe productivity losses.[3]

With few other incentives, digital trade barriers are difficult to address even amongst jurisdictions with similar interests and sensitivities. Negotiations amongst like-minded countries do not necessarily generate positive outcomes. This policy-induced balkanisation is therefore unlikely to be addressed in existing forums for economic cooperation and in the prevailing climate of economic diplomacy.

But fragmentation does not just restrict new services – it is an undoing of the existing framework and revocation of existing liberalisation achieved in trade, investment and taxation, and here lies culmination of the mismatch between internet and governance:

- As 56% of international trade in services relies on access to data,[4] market access in offline services (typically banking, professional services, transports and retailing) can be revoked by simply restrict access to data, despite prior commitments to liberalise such services. This condition has achieved a roll-back of existing GATS and FTA schedules.[5]
- Similarly, notion of 'digital presence' allow tax authorities to withdraw from the territoriality principle on taxation and tax entities that are outside their jurisdiction.[6] As market access via commercial presence (mode 3 in trade parlour) is far more restrictive than cross-border modes of supply, extraterritorial taxation impels towards less cross-border economic exchange;
- On investments, the current provisions against performance requirements in BITs can be easily circumvented through privacy and financial regulations, forcing investors to place their operations in the host country.

2. Taxonomy of fragmentation – extraterritoriality, technical, regulatory and commercial fragmentation

[3] Bauer, Lee-Makiyama, van der Marel, *The Costs of Data Localisation: A Friendly Fire on Economic Recovery*, ECIPE, 2014
[4] Based on assumption used first by *UNCTAD Information Economy Report*, UNCTAD, 2009
[5] Lee-Makiyama
[6] OECD Addressing the Tax Challenges of the Digital Economy, OECD, 2014; see critique thereof, Lee-Makiyama, Verschelde, OECD BEPS: Reconciling global trade, taxation principles and the digital economy, ECIPE, 2014

The conflict between the global nature of internet and the territorial nature of law has led to disputes between different state jurisdictions, producing conflict of forums or inconsistent results. The internet has become subject to a myriad of overlapping jurisdictions and conflicting obligations. Unlike other aspects of international law (e.g. law of the high seas) domestic laws are routinely enforced extraterritorially on online activities. Extraterritorial jurisdiction is often based on the nationality of the legal subject, i.e. a natural person who is a citizen, or a corporation is headquartered in the jurisdiction.

For example, the US tax code is based on worldwide income, that created the current problems of deferment of profit remittances from abroad. Similarly, US Department of Justice has claimed – albeit unsuccessfully – its jurisdiction over e-mail data stored on Microsoft's servers overseas based on the Stored Communications Act (18 U.S.C. §§ 2701) in a criminal investigation.[7]

But the most consequential case of extraterritorial jurisdiction over online space is found in the EU, which typically avoided extraterritoriality.[8] But the General Data Privacy Regulation (GDPR) is applied worldwide for personal information on any European citizen:[9] Applicability of GDPR is not territorially limited, and prohibits international transfers of personal information. Exceptions are limited to jurisdiction that the EU deems to have 'adequate protection', or by using legal instruments (binding corporate rules and model contracts) that impose strict liability for data processors and controllers that transfer the data.

Europe's fragmenting approach is beginning to establish a template for privacy regulation worldwide. In contrast to Europe, China goes extraordinary lengths to avoid extraterritoriality – yet produce similar results. The Great Firewall of China (or Golden Shield, as it is called within China) was initially a technical gateway for monitoring and controlling all internet traffic passing through Chinese borders. The Great Fire Wall balkanised the internet *technologically* rather than through extraterritorial applications of Chinese security laws to the rest of the world. Numerous other examples of *technical fragmentation* exist, such as the long-practiced online censorship in

[7] *Microsoft Corporation v. United States of America*, 829 F.3d 197 (2d Circ. 2016); rehearing request by US Department of Justice *en banc* denied, No. 14-2985, 2017 WL 362765 (2d Cir. Jan. 24, 2017)
[8] Blocking of sales of Nazi memorabilia in *Yahoo v LICRA*, TGI de Paris, 2000; US video streaming of a fashion show where certain logotypes were visible in a manner that violated French copyright laws, but falling under fair use in the US in *SARL Louis Ferarud v Viewfinder*, 489 F 3d 474, New York, 2007
[9] General Data Protection Regulation, Regulation 2016/679

some religiously conservative countries, to the more recent political censorship of Wikipedia and social media in Turkey.[10]

However, China's case differs greatly from Turkey. China had made several relevant commitments in its accession to the WTO for some of the most common online services,[11] and evidently had access to less-trade restrictive censoring techniques (thereby failing the two-tier test of GATS art XIV).[12] As a result, China has gradually moved towards a *regulatory* fragmentation rather than a technical one. China has introduced the Internet Content Provider (ICP) licence, a positive list of services that are deemed safe to use by the Chinese public, while other services may be subject to shut-downs. A licensing regime is more consistent with WTO rules thanks to its weak disciplines on domestic regulation (GATS art VI:4). Foreign investors were also restricted from operating wholly-owned e-commerce or voice over-IP services in China as such services require licenses for value-added telecom services (VAS). Clearly, such regulatory measures have both commercial and public security objectives. China's industrial policies on using indigenous, "secure and controllable" technologies and extremely strict requirements for participation in government procurement support the same dual objectives.

In other countries, the regulatory fragmentation supports objectives have justifications that appear equally uncompromising: A majority (58%) of data localisation measures are due to privacy regulations,[13] based on public perceptions of 'fundamental human rights',[14] an argument that has been proven to be difficult to counter by pointing to their economic costs. Other causes of regulatory fragmentation – such as copyright (disabling content portability across border) or banking regulations (financial supervisors demanding localisation of account data) are by their very nature national instruments confined to their jurisdiction. Such cases of localisation are even exceptions of supranational entities like the EU, addressing geo-blocking only for *pro tempore* cross-border use.

But even in the case where fragmentation does not serve 'hard' national objectives, digital protectionism differs from traditional protectionism, making them more complex to address. The post-war industrial policy engaged in regulatory protectionism to foster national champions,

[10] Turkeyblocks.org, *Facebook, Twitter, YouTube and WhatsApp shutdown in Turkey* and *Wikipedia blocked in Turkey*, 2017, accessed at: http://Turkeyblocks.org
[11] Online processing services (CPC843)
[12] Hindley, Lee-Makiyama, *Protectionism Online: Internet Censorship and International Trade Law,* ECIPE, 2009
[13] See note 1
[14] See *inter alia* EU GDPR, art 45 for international transfers

but online protectionism does not always follow that logic. To start, traditional protectionism would be pointless for the digital economy that rewards economy of scale in demand (ability to aggregate users), not production (a large factory that enable cheap production and exporting the surplus). For example, Germany's Industrie 4.0 strategy is built on a logic that the country must slow down competition through restrictive intermediary liability to cope with necessary reforms to protect its manufacturing supremacy and domestic media ownership – not necessarily to develop German search engines or social media.

Similarly, some of China's online protectionism is often linked to SOEs as they happened to be a fiscal income source for Chinese provinces, which are prohibited by the central government to raise taxes. Sectors where SOEs were absent (e.g. car-sharing, e-commerce) have been largely left unregulated, or the first sectors be liberalised for foreign ownership. Inability to decentralise China's fiscal structure thereby defers online reforms. Similarly, protectionism of online payments and *fintech* is linked to lack reforms of Chinese capital account and its banking sector that are constantly on the verge of systematic collapse.

Aside from such examples of commercial *objectives* for protectionism, *commercial* fragmentation by abusing pricing and other commercial terms. Absence of fair, reasonable and non-discriminatory (FRAND) terms for interconnection between a foreign and domestic telecom operator bars infrastructural and business services to provide a global service.

Commercial fragmentation by telecom operators often involves telecom SOEs, or wholesale prices that are set a national regulator (as in the *Telmex* case).[15] But non-state commercial entities could achieve same degree of fragmentation, if one local provider is allowed to dominate a market, or if all local telecom operators are colluding. Such allegations have been made against the US telecom and internet markets by foreign entities.[16] Such barriers are horizontal antitrust issues between private players. Similarly, network prioritisation is dominance abuse by an upstream player against a downstream one.

In this context, it should be noted that commercial fragmentation is the only kind of fragmentation that has been reasonably addressed using existing instruments: Antitrust laws

[15] Mexico — Measures Affecting Telecommunications Services, DS204
[16] FCC, WC Docket 16-143 and Docket 05-25, filed by the European Delegation to the United States, accessed at: https://ecfsapi.fcc.gov/file/10419110631001/Ma419.pdf

generally afford national treatment to foreign complainants, and effective WTO remedies against horizontal anticompetitive practices exist in the GATS Telecom Annex, albeit underused.

3. Whither trade governance?

In absence of other effective remedies, extraterritoriality is the new international customary law. This is particularly true for privacy law, an area which is forcefully advocated by the EU. But indirectly, the US is also arguing the case for data localisation and much more fragmenting privacy laws in Russia, Vietnam, China and India. Meanwhile bilateral instruments like adequacy decisions, only enforce existing extraterritorial regimes, rather than become a construct of free internal exchange amongst the signatories, as data is not allowed to flow to a third country. In that regard, they are similar to the limited reach of bilateral tax agreements.

Mutual legal assistance and extradition treaties (MLATs) could have curbed the need for extraterritoriality to address cybercrime, terrorism and privacy violations. However MLATS are today largely discounted. There is a lack of expediency, trust, and a great difficulty in achieving normative harmonisation on privacy and criminal law, making them impractical tools – which was demonstrated between two like-minded countries like Ireland and United States in *Microsoft v. United States*. This is also why harmonisation of privacy laws in international forums like APEC have its natural limits: As regulatory divergences are simply too wide, they contend to best endeavour guidelines based on minimum standards and proportionality. Enforceable rules under the WTO or other multilateral forums seem far off: After all, this is a world where even the 82 signatories of the ITA agreement cannot agree on the most basic non-tariff measures for electrical interference.[17]

As the economic and judicial cooperation fails to address fragmentation, trade disciplines against data localisation and data flows have been singled out as the only way forward – at least to deal with *regulatory* fragmentation. But FTA/RTA negotiations on these matters are effectively about expanding the exceptions, in particular for privacy, security and politically sensitive sectors: A hypothetical renegotiation of GATS art XIV and GATT art XX would most certainly lead to worse results than today.

[17] Electro-magnetic interference and compatibility (EMC/EMI) have been reformed to self-declaration of conformity (SDoC) practice.

Moreover, final TPP texts left generous exceptions for financial services, while the EU is keen to exempt privacy from the two-tier test – or move the burden of proof to the complainant. There are far-reaching consequences of such reversal as securing evidence of bad faith and behind a privacy law, or to prove that its intent is mere disguised protectionism, ought to be impossible. Any data localisation measure currently in place stand a scrutiny against such lax standards.

Given the sensitivities on personal information, one could foresee an argument that such information can be separated from other data *objects*, such as industrial data. The argument is that trade agreements could at least liberalise industrial use of data for the time being. Nonetheless, over 75% of all data online is user-generated,[18] making the majority of data flows personal information by default; the 'industrial use of data' also involves personal data like delivery addresses, information on customers or personnel, as human operators are often logged in while collecting, processing or uploading machine data.

Given the very broad definition of personal data in recently enacted privacy laws, almost any industrial and business data could fall under its scope. All forms of data are also integrated and collated in a data object (say, a file): There are no technical or legal means to separate non-personal information (numbers in a spreadsheet) from non-personal information (author of the spreadsheet embedded in the code). This is the very much the purpose of regulatory fragmentation – to create discretionary powers for an executive to act as gatekeepers to the market by selectively enforcing burdensome rules. Fragmentation has now established "license to operate" regimes, where the executive sets up a positive list of commercial entities that are allowed on the market hinged on nationality or performance requirements.

4. Conclusions

With over 1300 barriers identified affecting the digital economy in a sample of just 65 countries, one could soon argue that we are a *fait accompli,* as there are too many barriers for international treaty negotiations to handle. Economic argument does not seem to sway 'hard' objectives, such as security or fundamental rights. Economic arguments are sometimes even

[18] Austin, Upton, Leading in the Age of Super-Transparency, *MIT Sloan Management Review*, Winter 2016

futile for economic objectives – a draconic online tax law is paid through loss of GDP, in other words corporate revenues and consumer welfare, while governments may actually see their tax base increase. Public choice dilemmas arise as there are different incentives between the public authorities and its subjects.

Third countries find it difficult to incentivise against fragmentation, as balkanisation are consequences of unique structural problems in the underlying economy or the political system. This is the case of the fragmentation caused by both the EU and China.

However, this note is not to provide a justification to fragmentation just because they are uncompromising – but to map why traditional economic diplomacy has so far failed.

In the new political dimension of trade negotiations post-TPP and TTIP, like-mindedness is no longer a recipe for ambitious EPA/FTA outcomes. In fact, similarity is an impediment to successful conclusion of FTAs: Homogeneity (the extent barriers are imposed in same areas) lead to weak outcomes in intra-EU cooperation such as DSM. Regulatory divergences amongst the signatories of TTIP and TISA were narrower than TPP where parties imposed high barriers in completely different regulatory areas.

With no effective cooperation instruments for global openness and rule of law, the global governance system is at a lose-lose situation. As the actors cannot offer credible incentives or threats, and they are left with very few policy options but to block their own economy on reciprocal basis, and thereby contribute to further fragmentation.

Trade Regulation, and Digital Trade

May, 2017

By Petros C. Mavroidis[i]

1. The WTO: Neither Transactional, Nor Policy-Oriented

In 1998, the WTO (World Trade Organization) established a Working Group on Electronic Commerce (e-commerce).[ii] Almost twenty years later, the group has nothing to show in terms of achievements, other than a few papers discussing the general, potential applicability of multilateral rules on some forms of digital trade. True, even the minutes reflecting the outcome of WTO Ministerial Conferences include a few lines on "e-commerce", but this is where the buck stops.[iii]

The WTO attitude is neither transactional, nor policy-oriented, as we explain in more detail later. It is haphazard. One cannot understand when going through all this mass of information regarding e-commerce, that the WTO has made publicly available, what the WTO-think on digital trade is. In the meantime, digital trade is progressing fast. According to data provided by the McKinsey Global Institute in 2016, the growth is explosive: international data flows are forty five times higher in 2014 than they were in 2005.[iv]

Under the circumstances, one might wonder whether international rules are necessary at all. Digital trade grows fast anyway. And yet, a number of issues arise that impede further progress, and that require solutions preferably at the multilateral level: data localization, geo-blocking are the latest in a series of examples on this front. The WTO Work Programme has not managed to address similar issues head on. It has not managed to integrate them in a wider thinking about digital trade either.

Some free trade areas (FTAs) have managed to fare better on this front. There are, of course, a number of reasons why this has been the case ranging from homogeneity of players involved (who share similar concerns) to negotiating costs. It is submitted that one reason why FTAs succeed where WTO has failed lies in that it is easier to bring together the trade and regulatory communities in a forum consisting of like-minded players. Digital trade is not about trade exclusively. There is an important regulatory dimension that covers issues such as privacy, security etc. This issue must be considered as well. The trading community will discuss how it applies to infra-firm flows for which there is no associated payment flow. We will end up thus, with a PPM (process and production method) analogue set of issues. Production

function matters in this discussion (e.g., is data secure? How ensure security? etc.). The regulatory community will be discussing this latter set of issues.

In Section 2, I briefly discuss where WTO stands now on digital trade. In Section 3, equally briefly I discuss some illustrative FTA-examples, and finally, in Section 4 I provide scaffolding for a more structured discussion on digital trade in the WTO.

2. Multilateral Regulation of Digital Trade

I divide this discussion in two parts: what is the coverage of digital trade at the WTO-level as rules now stand, followed by a brief discussion of he Work Programme. I kick off this Section with semantics.

2.1 What is Digital Trade

Official WTO documents use the term "e-commerce" (instead of digital trade), which is routinely defined as

Production, distribution, marketing, sale or delivery of goods and services by electronic means.

Thus expressed, the term covers not only end-to-end delivery of services, like internet and other telecoms, but also other services that can be transmitted in digitized form. The legal regime applicable to these transactions is that provided in the various national schedules of commitments under GATS (General Agreement on Trade in Services). Recall nonetheless, that in US-Gambling, the Appellate Body (AB) endorsed "technological neutrality", that is, the means of supply of a service does not matter. Digitally transmitted services are covered by commitments entered even when digital supply was not an option at the moment when the commitment had been entered.

And what about goods sold on the internet? Well, it all depends on their characterization as goods or services. A book sold say on Amazon will be subjected to the tariff concessions of the importing state. Panels have yet to decide whether a song sold on Amazon, if downloaded and saved, should be characterized as good or service.

Finally note that, n literature, the term "digital Trade" seems to be associated with a wider coverage than "e-commerce" as explained above. Branstetter (2016) for example, includes the following definition.

> *… the full range of electronic commerce issues, from online commercial transactions to the ancillary aspects of protection of intellectual property rights, privacy, and the protection of national interests.*

This wider understanding of the term is more in line with expressed business interests.

2.2 As Things Stand

WTO does not regulate head on e-commerce (or digital trade) but electronically transmitted services are covered by the GATS to the extent that commitments to liberalize the pertinent service sector have been made.[v] Indeed, WTO adjudicating bodies have resolved disputes dealing with electronically transmitted services.

In US-Gambling, the AB held that the US was violating its commitments regarding the supply of internet gambling. In China-Publications and Audiovisual Products, it was upheld that the electronic distribution of music was covered. In China-Electronic Payment Services, the AB held that the Chinese electronic payments regime was in violation of nondiscrimination. Finally, in Mexico-Telecoms, the Panel held that Mexico was violating its commitments on telecoms by imposing supra-competitive termination rates.

The TRIPs (Trade-related Intellectual Property Rights) Agreement as well, is relevant to this discussion. IP rights have typically a territorial dimension, and it is precisely this characteristic of IP rights that might obstruct supply of digitalized services. Since TRIPs embeds a minimum standard of protection of IP rights, WTO members remain free to enact higher standards of protection to the extent that they observe nondiscrimination. Nothing of course, stops WTO members from signing agreements to by-pass national idiosyncratic elements.

2.3 Work Programme

The Work Programme aims to bring e-commerce under the multilateral disciplines. At the moment of writing, it is clear that we are far away from even a modest agreement.

Since the end of the Uruguay round agreement, the ITA (Information Technology Agreement, I and II) have been concluded. This agreement has liberalized trade by eliminating duties in products such

as computers, semiconductors, or telecommunications equipment. Note that the number of the initial participants (29) grew significantly and reached 81, accounting for about 97% of world trade in IT goods.

3. FTAs and Digital Trade

Digital trade occupies space in the majority of free trade areas (FTAs) signed in the post-Uruguay round era.

3.1 Here, There and Everywhere

Take the European Union (EU) FTAs for example. Its agreement with Canada (CETA), Korea (KOREU), but also its agreements with more heterogeneous partners (like EU-Vietnam) all contain chapters dealing head on with digital trade (e-commerce).

The EU is not alone in this. US follows a similar path. The now (almost) defunct TPP, for example, contains provisions aiming to facilitate digital trade. There are some obvious starting points, like the provision to abolish duties on digital goods. There are also some more hotly debated issues that found their way into the text. The TPP, for example, takes a strong stance against data localization (not allowed to require the establishment of local computing facilities as a condition of doing business) .

TiSA (Trade in Services Agreement), the most ambitious plurilateral agreement[vi] negotiated between a few WTO members outside the confines of the WTO, when finalized, will include an Annex on E-Commerce, which would cover open networks, unsolicited commercial communication, interactive computing, and wider international cooperation in this area.

3.2 Advantage FTAs

FTAs go thus consistently further than the multilateral regime does when it comes to addressing digital trade.[vii] Issues like data localization for example, which have not entered the WTO jargon, are commonpce in the regulation of digital trade under the aegis of FTAs.

Why are trading partners prepared to do things bilaterally (or plurilaterally) and not multilaterally? After all, standard theory would suggest that deals should be easier when there is more to exchange. Regulation nevertheless, unlike tariffs cannot be dwindled down. To the extent that it exists for good reasons, it is nonnegotiable. The key is thus, to bring around the table regulators and the trading

community. To sensitize the former to the trade impact of their measures, and the latter to the well-founded of the intervention.

This is what a close-knit group of like-minded players can do. Examples abound: from the US-Regulatory Cooperation Council to the instruments for regulatory cooperation in CETA. [viii]

4. A Role for the WTO

WTO should change course. Mindful of its limits, it should approach this discussion in functional manner, working on its strengths rather than embarking on a Work Programme with no compass where to go.

4.1 Advantage FTAs

WTO should attempt to address three questions:

- What is being delivered?
- Who delivers electronically?

These two questions will help identify the relevance of the WTO on digital trade, both with respect to the GATT and the GATS.

4.2 Next Steps

The next question for WTO should be what can be done to further liberalize digital trade. In that, WTO should function originally as complement to FTAs, and substitute for their efforts when gains can be multilateralized.

4.2.1 Building Bridges to the Hothouses of Regulation

Cutting edge issues are easier discussed across like-minded players. Think of the discussion on consumer privacy encryption, which has been taking place in TPP, for example, but is not in the radar screen of the WTO Work Programme.

Think also of the data localization issue for example. TiSA negotiations almost collapsed because of this issue. The EU, because of legal constraints, could not subscribe to the recipe advanced.[ix] This issue is being discussed in various bilateral fora, and has yet to find its way into the WTO Work Programme.

And then there are issues, which have not been resolved even in more intense integration processes. Geo-blocking has been plaguing the EU quest for a unified digital market in the European continent. Recently, the Commission has proposed a regulation that will constitute the first step only towards eliminating obstacles to market integration.[x]

The WTO has a lot to learn from these discussions. How do that?

4.2.2 Complements and Substitutes

WTO could complement these efforts by designing an osmosis mechanism. Issues that for example, have found similar or identical solutions in various FTAs could be debated as potential multilateral regulation. In doing that, WTO could become the multilateral substitute for regulation at the FTA-level.

In the meantime, it can provide an information-exchange regime, where good ideas and regulatory solutions agreed at the FTA-level could find a forum to be discussed by potentially interested players. Those keen could mimic the best regulatory examples. Others would have additional food for thinking their next regulatory interventions.

Reference

1. Bollyky, Tom, and Petros C. Mavroidis. 2017. Trade, Social Preferences and Regulatory Cooperation, the New WTO Think, Journal of International Economic Law, 20: 1-30
2. Branstetter, Lee. 2016. TPP and Digital Trade, pp. 72-81 in Jeffrey J. Schott and Cathleen Cimino-Isaacs (eds.), Assessing the Trans-Pacific Partnership, vol. 2, Innovations in Trading Rules, Peterson Institute of International Economics: Washington DC.
3. Hoekman, Bernard M., and Petros C. Mavroidis. 2015. WTO 'à la carte' or WTO 'menu du jour'? Assessing the Case for Plurilateral Agreements, European Journal of International Law, 26: 319-343.
4. Mishra, Neha. 2017. The Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance, Journal of International Economic Law, forthcoming.

---

[i] Edwin B. Parker Professor of Law at CLS, New York City, and Professor of Law at the University of Neuchâtel (Switzerland). For helpful discussions, I am indebted to Bernard M. Hoekman, and Robert Wolfe.

[ii] WTO Doc. WT/MIN(98)/DEC/2 of 25 May 1998.

[iii] One can find all these documents (both members' proposals, as well as WTO Secretariat background papers) in the WTO webpage https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm

[iv] See also Information Economy Report (2015), Unblocking the Potential of E-Commerce for Developing Countries, UNCTAD: Geneva, Switzerland.

[v] In light of our discussion above, there is no need to elaborate any further on the regime regarding trade in goods.

[vi] Hoekman and Mavroidis (2015) discuss the workings of plurilateral agreements.

[vii] Mishra (2017) for example discusses TPP

[viii] Bollyky and Mavroidis (2017) discuss this issue in more detail.

[ix] In C-362/14 (Max Schrems v. Facebook), the Court held that a Commission decision to allow for free flow of data cannot undermine the powers of national supervisory authorities to review whether transfer of data complies with the requirements of the EU directive regulating this issue (and essentially discuss the consistency of transfer with protection of fundamental rights). Eventually, in February 2016 the EU and US reached an agreement, the implementation status of which is still uncertain. Branstetter (2016) refers to CGE studies quantifying the negative impact on investment resulting from data localization requirements.

[x] COM (2016) 289.

The Future of Global Cyber Trust:

Fragmentation v. Universality Tradeoffs[i]

May, 2017

By Dr. Laura DeNardis[ii]

1. Introduction

Commerce, speech, social life, and every imaginable industrial sector are now digitally mediated and therefore contingent upon the security and integrity of Internet infrastructure. Emerging technological advances such as cyber physical systems, cryptocurrencies, and artificial intelligence raise the stakes of network stability significantly. What are the implications of these trust dependencies on modern society and the Internet itself? Until societies experience economic or social upheaval, the role of trust in maintaining societal stability exists as a taken for granted background context of daily life. Individuals trust that financial institutions will secure their bank accounts, cars will not malfunction, airplanes will stay in the sky, and medical test results remain confidential. Democracies depend upon the integrity of voting systems and commercial transactions rely upon trust between buyers and sellers. What has changed in recent decades is that all of these trust dependencies now also depend upon the integrity and security of underlying digital infrastructure.

Even while societal dependencies on digital infrastructure mount, there is evidence of some loss of trust in this very infrastructure and its governing institutions. Some of this loss of trust stems from actions in the political realm, whereby governments establish policies, such as data localization laws or national cybersecurity measures, to enhance national sovereignty or address privacy concerns about foreign intelligence gathering practices. Loss of trust among Internet users arises from rising awareness of government surveillance and private sector data gathering practices, as well as high-profile cybersecurity breaches, including the massive data breaches at Yahoo!, Target, and the US Office of Personnel Management (OPM).

The 2017 CIGI-Ipsos Survey on Internet Security and Trust, polling more than 24,000 users in 24 countries, found that a majority of respondents were more concerned about privacy than they had been in the previous year, partly related to cybercrime but, increasingly, also due to concerns about their own

governments (CIGI-Ipsos 2017). The poll indicated that only half of respondents trust their governments to act responsibly online.

Trust has always been a requirement for keeping the Internet operational, but society is approaching a tipping point in which significant improvements in digital trust are necessary to sustain a global digital economy and public sphere. Indeed, many of the most contentious global policy issues in the cyber arena involve struggles over trust: in the stability of infrastructure, voting systems, digitally mediated news, the security and privacy of user data, the authenticity of information and users, and commercial transactions. Not surprisingly, considerable policy and scholarly attention has focused on these issues, and especially, the close association between cybersecurity technologies and trust policies (Schneider 1998, Singer & Friedman 2014, Hampson & Jardine 2016).

Constructions of trust in cyberspace will affect whether the Internet continues to expand into a universal network or fragment into segments enclosed by geopolitical borders or proprietary market ecosystems. A great deal of policy and scholarly attention has examined tensions between Internet universality and fragmentation (Werbach 2008, Force Hill 2010, DeNardis 2016, Drake et al., 2016, Mueller 2017). What has been addressed less is the more narrow policy intersection between cyber trust and fragmentation. Can digital trust and Internet universality co-exist in the long term in light of technological and geopolitical changes facing the Internet? There is a moment of opportunity to examine intersections between digital trust and fragmentation and explore which future solutions – public policy, market approaches, civil society interventions, and technical design – can foster the trust necessary for the stability and security of digital systems while also enabling a universal Internet supporting digital trade, freedom of expression, and access to knowledge.

2. Digital Trust Points as a Precursor to Internet Universality

The Internet is not a single network but an interconnected collection of mostly privately owned networks able to interoperate because they adhere to common sets of standards for formatting and exchanging information. Trust between network operators has always been a requirement for this interconnection, just like trust between trading partners is necessary for the global digital economy to function. Each autonomous system advertises the routes (i.e. collections of Internet Protocol addresses) reachable through that network using Border Gateway Protocol (BGP). Historically, network operators have trusted adjacent networks to advertise accurate routes, although security breaches certainly occur

at these borders. The ability to access information on a website from anywhere in the world similarly depends upon trust in the Internet's Domain Name System (DNS), the globally distributed system that translates domain names into corresponding Internet addresses locating information online. Trust in the DNS is a necessary precursor for the Internet to globally operate. Technical infrastructure trust mechanisms such as public key cryptography authentication are increasingly engineered into these systems.

Even though the digital economy has experienced tremendous growth – the Internet has more than 3 billion Internet users and contributes more than $4 trillion USD to the global economy – the Internet is not yet universal. Viewed through the lens of physical infrastructure and bandwidth, nearly half the world still does not have access and, among those who do, access speeds vary considerably (ITU 2015). At the logical, software-defined layer of the Internet, there is also fragmentation, such as the use of the DNS to carry out censorship and other content controls. At the application and content layer, the Internet is not yet universal because of language differences, including barriers to universal accommodation of internationalized domain names (IDNs) that incorporate non-Latin characters such as those used in Arabic, Chinese, and Cyrillic text. Regional policies block content locally, such as the Right to be Forgotten in the European Union, the geo-IP restriction of Netflix in Canada, and systems of censorship and blocking in China and elsewhere. Fragmentation of networks for security reasons, via firewalls and virtual private networks, is of course the norm for most corporate networks. This choice to create fragmentation for security reasons is quite distinct from fragmentation that is not a user choice. Overall, the Internet has continued to expand globally because of trust among networks, between websites and browsers, and in common technical standards and systems of routing and addressing.

3. Geopolitical Trust Tensions Are Creating Fragmentation

Despite the historical growth trajectory of the Internet, several geopolitical trust problems are creating digital fragmentation. Values of privacy, security, and national sovereignty increasingly conflict with values of universality and the free flow of information across borders. Some of these conflicts arise from problems of jurisdiction, as well as incongruities between technological and nation-state boundaries. The virtual architecture of the Internet and the cross-border nature of data flows are often incommensurable with political borders. While routers make decisions about the flow of information based on engineering optimization rather than geography, what counts as privacy, hate speech,

indecency, and freedom of expression, differs greatly across geopolitical borders. Legal authority over citizens and institutions within borders does not comport well with the cross-border and distributed nature of cyberspace. Interoperability and harmonization of Internet policies across borders can prevent Internet fragmentation, but cultivating cultural and political agreement on many Internet policy issues can be an intractable problem, even in areas such as intellectual property rights enforcement and cybercrime. The jurisdictionally complex task of enforcing laws often falls to private intermediaries, creating a privatization of governance unprecedented in the contemporary era.

A trust-related example of attempts to harmonize national borders with virtual borders involves the introduction of data localization laws placing constraints on how private companies (e.g. banks, retail, or technology companies) handle customer data, including requirements that data be stored on servers within a nation's borders (Chander and Le 2015). The rationales for these policies often cite concern about customer privacy in the context of foreign surveillance, even though concentrating data in a fixed location can facilitate efficient surveillance and create a host of technical complexities and economic costs (Bauer, et al. 2016).

Governments increasingly view control of Internet infrastructure as a proxy for state power, whether motivated by national security, cyber war concerns, censorship, or economic objectives. China and other countries seeking greater control over information flows have advocated for top-down, bordered, government-centric cyber sovereignty approaches that supplant traditional private sector led governance approaches in the name of cyber order (DeNardis, Goldstein and Gross 2016). Some of these efforts to assert cyber sovereignty arise from lack of trust in the institutions that govern the Internet and raise the possibility of fragmentation not only of digital networks but of the global governance structures tasked with keeping networks operational.

4. Emerging Trust Terrains: IOT, Currency, and AI

Emerging technological innovations raise the stakes of digital trust and also challenge some prevailing assumptions that the goal of a universal Internet is always in the public interest. Internet of Things (IOT) projections envision the ability to interconnect an estimated 50 billion objects to the global Internet. The diffusion of the Internet into material objects - remote sensor devices, health monitoring devices, home appliances, traffic systems, and networked vehicles – raises the stakes for digital trust. For example, a disruption of a network-connected cardiac implant threatens human safety rather than simply

the ability to communicate. Digitally dependent and digital-only cryptographic currencies also continue to gain traction, often outside of traditional regulatory frameworks. What trust mechanisms are necessary to preserve confidence, integrity, and security in financial systems? As decisions about how information is organized and how data is analyzed move to machine learning and artificial intelligence systems, new systems of accountability and human safety will be necessary to instill trust in digital environments.

5. Framing Questions for the Panel

Fragmentation as a Context-Dependent Value. Given threats from cyberattacks, cybercrime, and geopolitically motivated Internet conflict, and considering that the cyber realm now includes industrial control systems, medical devices, vehicles and other human safety-related contexts, is fragmentation necessarily something that should be minimized? Conversely, in highly trust dependent areas, under what conditions is fragmentation actually desirable?

The Tension between Privacy/Security and Universality. Can values of privacy and security, and the trust solutions necessary to sustain these values co-exist with norms of Internet universality?

Trust as a Precursor for Universality. Where Internet universality has positive economic and social effects (e.g. freedom of expression, global commerce), what are the most pressing trust dependencies necessary for the growth of the global digital economy and digital public sphere?

Trust Solutions. What solutions - in technical architecture, market approaches, government policies, and international agreements – hold the most promise to create trust conditions necessary for an appropriate balance between Internet universality and fragmentation?

Emerging Trust Dependencies. What policy solutions of today can address emerging technological phenomena such as artificial intelligence, cryptographic currencies, and cyber physical systems?

Reference

1. Bauer, Matthias, Martina Ferracane and Erik van der Marel (2016). "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization," *Global Commission on Internet Governance Papers Series* No. 30, May. Accessed at https://ourinternet-files.s3.amazonaws.com/publications/ gcig_no30web.pdf.
2. Chander, Anupam and Uyen Le (2015). "Data Nationalism," *Emory Law Journal*, Vol. 64, No. 3.
3. CIGI-Ipsos Global Survey on Internet Security and Trust, April 2017. Accessed at https://www.cigionline.org/internet-survey.
4. DeNardis, Laura (2016). One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation, Global Commission on Internet Governance, GCIG Paper No. 38, July 19. Accessed at https://www.cigionline.org/publications/one-internet-evidentiary-basis-policy-making-internet-universality-and-fragmentation.
5. DeNardis, Laura, Gordon Goldstein, and David A. Gross (2016), "The Rising Geopolitics of Internet Governance: Cyber Sovereignty v. Distributed Governance," Columbia SIPA Working Paper, November 30.
6. Drake, William J., Vinton G. Cerf and Wolfgang Kleinwächter (2016) "Internet Fragmentation: An Overview." World Economic Forum Future of the Internet Initiative White Paper, January. Accessed at www3.weforum.org/docs/WEF_FII_ Internet_Fragmentation_An_Overview_2016.pdf.
7. Force Hill, Jonah (2012). "Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers," Belfer Center for Science and International Affairs, Harvard Kennedy School. Accessed at http://belfercenter.ksg.harvard.edu/files/ internet_fragmentation_jonah_hill.pdf.
8. Hampson, Fen Osler and Eric Jardine (2016). Looks Who's Watching: Surveillance, Treachery and Trust Online, Center for International Governance Innovation (CIGI) Press.
9. ITU (2015). International Telecommunication Union (ITU), "ICT Facts and Figures – The World in 2015," 2015. Accessed at http://www.itu.int/en/ITU-D/Statistics.
10. Mueller, Milton (2017). *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*, Polity Press.
11. Schneider, Fred B., ed. (1998). *Trust in Cyberspace*, National Academy of Science Press.

12. Singer, P.W. and Allan Freidman (2014). *Cybersecurity and Cyber War: What Everyone Needs to Know*, Oxford University Press.
13. Werbach, Kevin (2008). "The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing it Apart," *University of California Davis Law Review*.

[i] Background Thought Piece - Digital Futures Policy Forum Panel: Developing Trust and Assurance

[ii] Adjunct Senior Research Scholar, Columbia SIPA, Professor, American University

COLUMBIA|SIPA
School of International and Public Affairs

accessnow

HUMAN RIGHTS PRINCIPLES FOR CONNECTIVITY AND DEVELOPMENT

Internet connectivity is essential for economic, social, cultural, political, and civic participation in the digital age. For the benefits of information and communications technologies to spread equitably and freely, connectivity must occur within a human rights framework.

Our goal in developing the Principles is to prevent, mitigate, and remedy human rights harms that arise in development projects to build internet infrastructure, connect the world to the internet, and achieve the Sustainable Development Goals (SDGs) using information and communications technologies (ICTs).[1] Since more than four billion people lack access to the internet, the largest stakeholder group in these efforts remains unconnected, likely marginalized, rarely consulted, and dangerously at risk of being left behind in the digital age. Our process is open to input and innovation to support the broadest possible participation.

The Principles advanced in this draft are grounded in international human rights law and norms; are consistent with the SDGs as well as development best practices; and are designed to help guide initiatives to increase connectivity to the global internet. We use the term "connectivity" here in recognition of the many programs that aim to spur infrastructure investment and bring all people online by 2020, such as the Global Connect Initiative,[2] Connect the World,[3] and Connect 2020.[4] We intend the term to encompass efforts to provide affordable access to infrastructure, including public access points, as well as policy initiatives and capacity-building programs to enable development and the free and safe exercise of human rights online.

These Principles do not aim to supplant, but rather to build on and adapt, such foundational documents as the Internet Rights and Principles Coalition (IRPC) Charter of Human Rights and Principles for the Internet,[5] the Association for Progressive Communications (APC) Internet Rights Charter,[6] the UN Guiding Principles on Business & Human Rights,[7] and the Council of Europe Guide to Human Rights for Internet Users.[8] They are intended to inform financial institution safeguards like the Overseas Private Investment Corporation's Environmental and Social Policy Statement.[9]

1. http://www.globalgoals.org/#the-goals
2. https://share.america.gov/globalconnect
3. http://connecttheworld.one.org
4. http://www.itu.int/en/connect2020/Pages/default.aspx
5. http://internetrightsandprinciples.org/site
6. https://www.apc.org/node/5677#1
7. https://business-humanrights.org/en/un-guiding-principles
8. https://www.coe.int/en/web/internet-users-rights/guide
9. https://www.opic.gov/sites/default/files/consolidated_esps.pdf

These Principles guide stakeholders on building protections for human rights into development programs, by design:

1 Assessments of connectivity investments must include an evaluation of the impact on human rights. Connectivity, development, and human rights are interdependent, and should not be considered in isolation. Those evaluating connectivity investments for development must consider the impact on political, economic, social, and cultural rights.

2 Investment in infrastructure should be deployed hand-in-hand with human rights-based capacity building, public access points, and skills development. To bridge the gender digital divide and other persistent inequalities will require more than simply extending infrastructure; inclusive partnerships are vital for unlocking the full benefits of connectivity for a population.

3 Investors should support connectivity for development that respects human rights. Human rights apply online just as they do offline. Participation in connectivity initiatives should be conditioned on demonstrated respect for human rights, applicable before, during, and after completion of the project. To ensure sustainability of connectivity projects and avoid partial execution of investments, conditions should be reached through cooperative strategies.

4 Investors should promote affordable and open access to the whole internet. The internet is a global resource that must remain open and affordable. Affordability should be set based on local needs and realities. Public, aid, and development-targeted funding should not enable private actors to create walled gardens or employ business models that fail to offer users affordable access to the global internet.

5 Investors should seek to facilitate freedom of expression through resilient and robust networks that reach marginalized and vulnerable communities. The law should promote wide access to content, stable and resilient networks, and sustainable systems.

6 Connectivity investments for development must respect privacy, which is essential for the internet economy. Privacy impact evaluations and technical, legal, and policy due diligence should be carried out on connectivity initiatives before deployment.

7 Projects for connectivity should be undertaken using open, transparent, and inclusive processes. Corruption is an obstacle to human rights and development. All public and private institutions involved in connectivity projects must enable access to information, build trust with stakeholders, and ensure accountability for funding.

8 Connectivity initiatives should remain open to civil society and community participation throughout the life of the project. Ensuring safe and secure access requires international collaboration, as well as local organizing, based on a multistakeholder model.

9 Connectivity initiatives must meaningfully extend access remedy to through robust and rights-respecting oversight and grievance processes. Establish points of contact to hear grievances and predictable, transparent procedures to appeal determinations. Participation in a remedial process should never preclude access to courts.

To foster an enabling environment for digital economies, governments must commit to not block, throttle, or shutdown communications tools and networks, in violation of international human rights. Positively, governments should implement strong network neutrality and data protection regulation, supporting both the economic interests and human rights of local communities.

For more information:

Peter Micek
General Counsel
Access Now
accessnow.org
peter@accessnow.org

Panel Discussion:

Cyber Conflict and Democratic Institutions

By Sean Kanuck

1. Introduction

This year's Global Digital Futures Policy Forum focuses on the tension between fragmentation of the Internet and globalization. While fragmentation, splintering, or "Balkanization" of the Internet has been a prominent topic of discussion for several years now, globalization has recently received a resurgence of attention in popular debate[i]. Globalization – long revered as a teleological objective of the Western liberal order – is increasingly being questioned by electorates in North America and Europe. Rising nationalist tendencies among certain political parties and candidates seek to re-assert domestic advantage and the self-interest of their constituents as their primary political goals. That trend, coupled with the legal debates about privacy and data localization in multiple jurisdictions, has reinvigorated interest in studying fragmented futures for the Internet.

This Panel will address cyber conflict as it pertains to the manipulation and/or compromise of democratic institutions – both directly and indirectly. Direct intervention in a democratic election could comprise either public efforts to personally obstruct voters or else clandestine alteration of actual vote tabulations; indirect intervention could consist of using proxy voices or inducing political, economic, or media events with secondary impacts on voter turnout and election results. Manipulative actions that do not directly alter the voting process or results are to be considered "influence operations", while actual changes to registered voters (including threats of violence or other means to physically deter eligible voters from attending the polls) or the ballots that are cast are typically deemed illegal "voter fraud", even when perpetrated by the state apparatus itself. (Figure 1 below reflects the fact that both direct intervention and indirect influence in democratic elections can be either overt or covert.)

Information communication technologies (ICT) present many new vectors for potentially interfering with democratic institutions. Foreign competitors, traditionally offset by geography, can now impose themselves on domestic political systems anywhere in the world. Social media platforms enable

individuals or special interest groups to broadcast their policy positions at little or no cost and even to strategically misrepresent broader support for those positions. Internet-connected ICT networks are highly susceptible to unauthorized access, thereby rendering sensitive data vulnerable to theft and public release. In essence, the digital future – and liberal democratic processes that will rely upon it – is susceptible to interference and disruption. This Panel will consider ways to safeguard democracies and the international order from corruptive influences (or at least to minimize their impacts) in the future.

Figure 1: Examples of Methodologies for Manipulation of Democratic Elections

	DIRECT INTERVENTION	**INDIRECT INFLUENCE**
OVERT	Intimidating or deliberately misinforming voters in order to deter turn out. For example, unofficial "robocalls" used during the 2011 Canadian federal election to falsely claim changes to polling station locations.[ii]	Public campaign donations and/or speeches by non-candidates in support of specific ballot choices. For example, President Obama's 2016 speech in London opposing "Brexit" before that referendum.[iii]
COVERT	Secretly altering the election results in order to favor a specific candidate. For example, the historical allegations regarding Lucien Bonaparte's inflation of voting results in the French constitutional plebiscite of 1800.[iv]	Clandestine, third-party activity intended to increase or decrease support for specific candidates. For example, reputed Russian espionage and publicization of materials during the 2016 U.S. presidential campaign.[v]

2. Historical Precedent

When evaluating the impact of cyber modalities (i.e. ICT) on democratic institutions, one must first consider what is genuinely new in either the objectives or possible impacts. Regardless of which quadrant of Figure 1 is of concern, there is ample historical precedent from geo-politics. Thucydides recounted Athenian efforts to lobby the magistrates of Melos to capitulate without battle (i.e. indirect and overt influence). Similarly, Radio Free Europe and Voice of America were designed to provide the electorates of foreign polities with information that was otherwise unavailable and/or forbidden. Nor is history want for allegations of ballot-box stuffing (i.e. direct and covert intervention) or voter intimidation (i.e. direct and overt intervention). Digital manifestations of those forms of fraud are certainly illegal and deserving of policy attention, but they are not the focus of recent debate. What seems to capture the current imagination – and concern – is the heightened opportunity for indirect, covert influence through

cyber means. Careful analysis is required, however, to properly assess the nature and foundation of that concern.

Framing Question 1: What is so new and inherently objectionable about digital influence campaigns?

If one reasonably acknowledges that foreign efforts to influence elections are as old as elections themselves, then one is left with either (i) a theoretical objection that is so counterfactual to historical practice that it is relegated to pure academic consideration, or (ii) a practical objection that employing a new technological means to an old political end is somehow unacceptable. It is worth recalling that public international law does not outlaw espionage – which is merely accepted as a feature of international relations. Nor is the publication and dissemination of political opinions generally deemed objectionable in liberal democracies. So what is really at issue here?

By way of example, several former U.S. intelligence officials have stated that they considered the theft of Office of Personnel Management records to be a "legitimate" foreign intelligence target.[vi] But even so, U.S. government officials have said that the scale and import of that espionage crossed a line that was unacceptable. So, it would seem that the objection stems from the quantitative scope of the activity in question (i.e. the sheer number of records compromised, the gross imbalance between the cost of conducting the activity versus its harm to the victim, the possible stand-off distance from which such an operation can be conducted without personal risk, etc.), rather than the qualitative nature of the activity itself (i.e. the theft of private information, the type of data targeted, etc.). Chivalric objections to the crossbow and guerilla warfare tactics should immediately come to mind, for new methods of conflict are often too efficacious for the establishment to accept at first outset.

Framing Question 2: When does a quantitative improvement in espionage constitute an unacceptable qualitative change? Do recent offensive cyber advances constitute a qualitative threat to democracy?

<u>Protected Infrastructure</u>

The U.S. Department of Homeland Security did not officially designate election systems as a critical infrastructure until January 2017.[vii] Yet, almost four years earlier in March 2013, the U.S. Director of National Intelligence (DNI) had identified an important incongruity related to how different nation states view online media and their political systems:

> *"Online information control is a key issue among the United States and other actors. However, some countries, including Russia, China, and Iran, focus on 'cyber influence' and the risk that Internet content might contribute to political instability and regime change. The United States focuses on cyber security and the risks to the reliability and integrity of our networks and systems. This is a fundamental difference in how we define cyber threats."*[viii]

That fundamental difference (i.e. the underlying distinction between infrastructure and content) is also germane to the question of which ICT deserve protection as "democratic institutions". Most everyone would likely agree that public authorities must guaranty the security of polling stations, voting machines, and official election returns. In other words, they are expected to prevent direct intervention that is contrary to the rule of law. This is represented by the United States' "infrastructure-centric" view of cyber security that was highlighted by the DNI. Content poses a much more complicated challenge.

Framing Question 3: Is the national government responsible for ensuring the confidentiality, availability, and integrity of all media resources that can influence a democratic electorate? Why not?

The discussion about where to draw the line regarding indirect influence quickly becomes muddied, as we regularly see with proposals for campaign finance reform. Managing the impact of informational content pits two democratic values against one another, namely freedom and equality. How much leverage should freedom of expression permit wealthy individuals and companies to exert on democratic processes? Is every mass media outlet or social media platform to receive a critical infrastructure designation because they can be utilized to influence public opinion? Which entities are "entitled" to special protections and/or restrictions? Each of those questions is a public policy dilemma.

Figure 2: Examples of Civilian Infrastructures that Impact Democratic Elections

	VOTING SYSTEMS	INFORMATION RESOURCES

PUBLIC	Government administered polling stations and officially monitored vote tabulation. Susceptible to corruption by ruling party.	National television, radio, print, and online media outlets. Subject to selective coverage and preferential treatment by ruling party.
PRIVATE	Hardware and software for voting systems and registration databases developed by commercial companies. Susceptible to supply chain and/or remote penetrations.	Independent mass media and online social media platforms. Subject to censorship by government as well as disruption and/or manipulation by third parties.

The status of political parties and their proprietary resources also raises very difficult legal and policy questions. If the compromise of an entity like the Democratic National Committee or the Republican National Committee in the United States is deemed a national security concern, then what level of governmental oversight and regulation of (i.e. access to) that party's ICT networks is appropriate in the national interest? Does that level change depending on whether that party is currently in power? Should smaller political parties be exempt from such regulation if they are not likely targets for foreign intervention? Once again, these cyber challenges are pitting core democratic values against one another (e.g. privacy versus national security) and policy trade-offs are inevitable.

Framing Question 4: Can private data be treated as a national asset against the will of its owner?

Social media represents a uniquely influential and vulnerable feature of modern politics. Its impact during the Arab Spring was noted by governments and demonstrators alike around the world. Since then, the use and manipulation (e.g. "astroturfing" to generate the semblance of broader support) of social media has become an instrumental part of political campaigns, opposition movements, and foreign influence operations. It is possible, at least to a certain degree, to reveal such social media manipulation (e.g. by technically determining the provenance of posted information, detecting automated programs for "re-tweeting" and "liking" posted information, and identifying patterns of coordinated "trolling"), but that requires analysis of large tranches of proprietary data, including both content and technical meta-data. In democratic societies, private ICT companies have no *ex ante* obligation to make their databases available to government authorities for speculative research.

Figure 3: Examples of Information Propagation to Induce Political or Economic Behavior

	INTENTIONAL MESSAGING	UNWITTING EXPLOITATION
INFORM	The 2007 airborne delivery of leaflets over Afghanistan by the U.S. military in order to deter insurgent activity by the Taliban.[ix]	In 2016, Twitter suspended thousands of suspected terrorist accounts that promoted violence and/or spread propaganda.[x]
DECEIVE	Adoption of the title "Bolshevik" (i.e. "one of the majority") by a party faction that was numerically inferior.[xi] The ironic naming of "Greenland" by Erik the Red to encourage emigration to a new colony that was less temperate.[xii]	The Syrian Electronic Army's false "tweet" disseminated from the Associated Press's Twitter account, which led to temporary fluctuations in U.S. stock markets in 2013.[xiii] False news items posted on Facebook during the 2016 U.S. presidential campaign.[xiv]

Data Integrity

As Figure 3 illustrates, many forms of media have been used to spread both information and disinformation for political effect. History is certainly replete with examples of interest groups "marketing" their views to the public – such as the U.S. founding fathers' ascription of the moniker "Anti-Federalists" to their opponents in order to impute a negative connotation – but social media platforms present a new challenge whereby they host content that is neither of their own creation nor necessarily attributable to physically identifiable third-parties. Accordingly, they become enablers for all sorts of online activities that can foster or undermine democratic institutions. That schizophrenia is perhaps best characterized by the hacker consortium Anonymous, which has both thwarted sovereign governments and also publicized child pornographers and corporate fraud.[xv]

Framing Question 5: Is the "common carrier" model the right legal analogy for social media outlets?

All of the themes aforementioned in this paper (e.g. espionage, influence operations, quantitative change, qualitative distinctions, public versus private infrastructure, freedom of expression, national security, etc.) coalesce around the key issue of data integrity. Because democracies rely on the ability of their populaces to make informed decisions, increased dependence on insecure ICT poses considerable threats. How can the public ever differentiate truth from falsehood with certainty?

In fact, international humanitarian law (aka the law or armed conflict) struggles with a similar

of war (i.e. permissible deceptions not based on garnering false status).[xvi] Interestingly, though, "misinformation" is listed as a ruse vice perfidy; moreover, the relevant treaty distinctions explicitly do not "affect the existing generally recognized rules of international law applicable to espionage."[xvii] Thus, cyber operations premised on exerting indirect influence are particularly problematic – especially when they only reveal true information.

Framing Question 6: Can two "rights" make a "wrong" … that is, should espionage (which is accepted in international relations) that exposes the truth (a core democratic value) be prohibited?

Ultimately, the most nefarious threat to democratic institutions is the corruption of the integrity of information. The pervasive introduction of false data into mainstream media could erode public confidence and destabilize society. That is, of course, exactly what authoritarian regimes are (i) highly concerned about happening to themselves, and (ii) well-practiced in perpetrating against their adversaries. Yet, democracies pride themselves on permitting their citizens to hold and publicize contrarian (or even counterfactual) opinions, and modern ICT permit foreign voices to participate in domestic dialogues.

It seems then that the most conceptually disturbing challenge for democratic institutions regards digital, highly efficient, indirect, foreign, misinformation campaigns that can neither be prevented nor easily identified. Furthermore, it is unclear what kind of governmental institutions (domestic or international) and/or private sector initiatives could resolve that difficulty, for this seemingly new cyber concern tautologically reduces to the well-known game theory paradox of "who guards the guardians"?

---

iSee http://www.atlanticcouncil.org/images/files/publication_pdfs/403/121311_ACUS_FiveCyberFutures.pdf ; See generally, David Kennedy, A WORLD OF STRUGGLE: HOW POWER, LAW, AND EXPERTISE SHAPE GLOBAL POLITICAL ECONOMY, Princeton University Press (2016).

ii See http://news.nationalpost.com/news/canada/canadian-politics/electoral-fraud-did-take-place-in-2011- federal-vote-but-it-didnt-affect-outcome-judge-rules

iii See https://www.theguardian.com/politics/2016/apr/22/barack-obama-brexit-uk-back-of-queue-for-trade-talks

iv See e.g., https://en.wikipedia.org/wiki/French_constitutional_referendum,_1800

vi See http://www.defensenews.com/story/defense/policy-budget/cyber/2015/06/27/opm-attack-hack-china- cybersecurity-personal-data-suspect-espionage-verifiable-/29341789/; See https://www.the-american- interest.com/2015/06/16/former-cia-head-opm-hack-was-honorable-espionage-work/

vii See https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure- critical

viii James R. Clapper, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence, March 12, 2013

ix See http://www.af.mil/News/Article-Display/Article/127729/operation-achilles-leaflet-airdrop-delivers-message- to-taliban/

x See https://www.wired.com/2016/08/twitter-says-suspended-360000-suspected-terrorist-accounts-year/

xi See https://www.britannica.com/topic/Bolshevik; See http://www.historytoday.com/richard-cavendish/bolshevik-menshevik-split

xii See http://news.nationalgeographic.com/2016/06/iceland-greenland-name-swap/; See also, https://www.scientificamerican.com/article/proof-on-ice-southern-greenland-green-earth-warmer/

xiii See https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that- tipped-stock-market-by-136-billion-is-it-terrorism/?utm_term=.f575e36dfcd2

xiv See http://www.reuters.com/article/us-usa-election-facebook-idUSKBN1380TH

xv See https://sg.finance.yahoo.com/news/Anonymous-exposes-visitors-afpsg-2809071407.html; See http://asia.nikkei.com/Business/Trends/Hackers-turn-stock-advisers-as-Anonymous-targets-China-Inc?page=1

xvi See Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (hereinafter Protocol 1), Article 37, June 8, 1977; See also, Protocol 1, Article 39

xvii Protocol 1, Article 39(3); See Protocol 1, Article 37(2)


COLUMBIA | SIPA
School of International and Public Affairs