CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission on Internet Governance

ourinternet.org

PAPER SERIES: NO. 38 — JULY 2016

One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation

Laura DeNardis

ONE INTERNET: AN EVIDENTIARY BASIS FOR POLICY MAKING ON INTERNET UNIVERSALITY AND FRAGMENTATION

Laura DeNardis

CHATHAM HOUSE
The Royal Institute of International Affairs

Published by the Centre for International Governance Innovation and Chatham House.

This work was carried out with the aid of a grant from the International Development Research Centre (IDRC), Ottawa, Canada.

The views expressed herein do not necessarily represent those of IDRC or its Board of Governors.

67 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

TABLE OF CONTENTS

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

Launched by two independent global think tanks, the Centre for International Governance Innovation (CIGI) and Chatham House, the Global Commission on Internet Governance will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

The Global Commission on Internet Governance will focus on four key themes:

- enhancing governance legitimacy — including regulatory approaches and standards;
- stimulating economic innovation and growth — including critical Internet resources, infrastructure and competition policy;
- ensuring human rights online — including establishing the principle of technological neutrality for human rights, privacy and free expression; and
- avoiding systemic risk — including establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence-building measures and disarmament issues.

The goal of the Global Commission on Internet Governance is two-fold. First, it will encourage globally inclusive public discussions on the future of Internet governance. Second, through its comprehensive policy-oriented report, and the subsequent promotion of this final report, the Global Commission on Internet Governance will communicate its findings with senior stakeholders at key Internet governance events.

www.ourinternet.org

ABOUT THE AUTHOR

Laura DeNardis, CIGI senior fellow, is a scholar of Internet architecture and governance and professor in the School of Communication at American University in Washington, DC. The author of *The Global War for Internet Governance* (Yale University Press, 2014) and several other books, her expertise has been featured in numerous publications. She serves as the director of research for the Global Commission on Internet Governance and is an affiliated fellow of the Yale Law School Information Society Project, where she previously served as executive director. Laura holds an A.B. in engineering science from Dartmouth College, a Master of Engineering from Cornell University, a Ph.D. in science and technology studies from Virginia Tech, and was awarded a postdoctoral fellowship from Yale Law School.

ACRONYMS

APIs	application programming interfaces
AS	autonomous systems
CDNs	content delivery networks
DNS	Domain Name System
GCIG	Global Commission on Internet Governance
IDNs	internationalized domain names
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITU	International Telecommunication Union
IXPs	Internet exchange points
MLAT	Mutual Legal Assistance Treaty
NAT	network address translation
OECD	Organisation for Economic Co-operation and Development
TCP/IP	Transmission Control Protocol/Internet Protocol
W3C	World Wide Web Consortium

EXECUTIVE SUMMARY

One twenty-first-century Internet policy debate concerns whether cyberspace will continue to expand into a universal network or fragment into disjointed segments based on geographical borders or proprietary ecosystems. Tensions between network universality and enclosure reflect conflicts among public-interest values in cyberspace, such as national security versus individual rights, and freedom of expression versus privacy. They also reflect increasing incongruity between the traditional governance roles of sovereign nation states and a global technological system that crosses national borders and is overseen by a distributed, private-sector-led multi-stakeholder governance framework. Under the mantle of cyber sovereignty, governments have attempted to overlay geopolitical borders on the Internet, such as implementing efficient systems of content censorship and filtering, or enacting privacy-related laws mandating restrictions on where and how companies may store customer data. New business models, such as zero-rating services designed to advance free Internet access in emerging markets, have raised questions about whether the next billion Internet users will have access to the global Internet or only a fraction of cyberspace available for free via walled gardens. This paper examines the extent to which the contemporary Internet can be viewed as a universal network now, explores the economic and social implications of emerging initiatives associated with the potential for Internet fragmentation, and presents a baseline proposal for the technological characteristics and policy frameworks necessary for affording the Internet with a sustained capacity for ongoing global growth and openness.

INTRODUCTION

Two forces are in tension as the Internet evolves. One pushes toward interconnected common platforms; the other pulls toward fragmentation and proprietary alternatives.

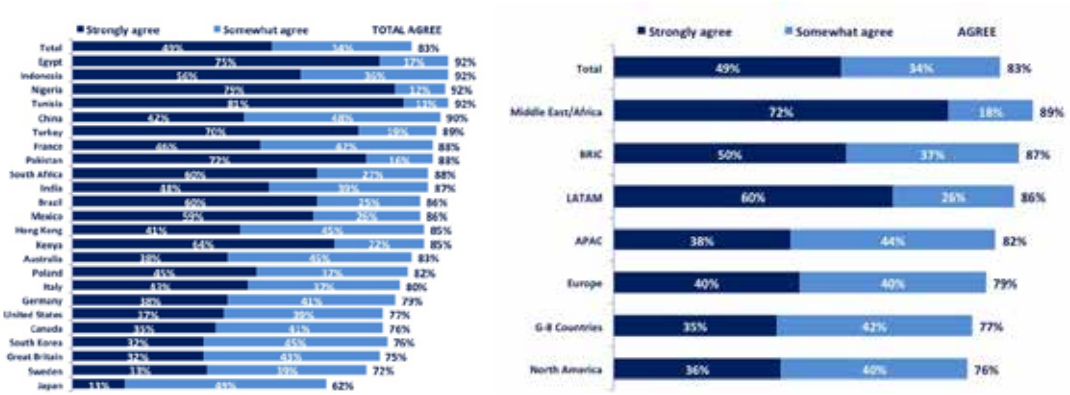
– Kevin Werbach (2008)

The economic and social promise of bringing the next billion people online usually assumes the ongoing growth and availability of a universal Internet. But the Internet of the future has many possible trajectories. One twenty-first-century Internet policy debate concerns whether cyberspace will continue to expand into a single, universal network, or fragment into disjointed segments based on geographical borders or proprietary ecosystems. How this choice resolves in the contemporary context will have considerable implications for the future of global economic development, national security and counterterrorism, and for the nature of free expression and access to knowledge online.

The ability to interconnect a projected 50 billion objects — from health devices to industrial control systems — depends even more so on the pervasive interoperability and global reach afforded by the Internet, and the diffusion and integration of the network, far beyond mobile phones and laptops, deep into the everyday objects and infrastructures that support life's day-to-day transactions. While the digital realm is still in its infancy, this *capacity* to connect ubiquitously to the Internet, regardless of location or access device, has become an implicit assumption of the twenty-first century.

Even in areas yet without Internet access, policy makers and entrepreneurs investing in information and communication technologies assume that building the necessary infrastructure is not only possible, but will empower citizens to participate in the global digital economy, access knowledge and engage in lawful communication with others, regardless of location or type of device. The more than 23,000 citizens polled in the 2014 CIGI-Ipsos Global Survey on Internet Security and Trust overwhelmingly view Internet access as a human right (see Figure 1), and vast majorities view the Internet as important for the future

Figure 1: "How much do you agree or disagree with the following statement? 'Affordable access to the Internet should be a basic human right.'"



Data Source: CIGI-Ipsos (2014).

of free speech, political expression, access to knowledge, and to their economic well-being (CIGI-Ipsos 2014).

Eighty-three percent of users believe affordable access to the Internet should be a basic human right when asked: "How much do you agree or disagree with the following statement? 'Affordable access to the Internet should be a basic human right.'"

In accord with these results, the United Nations Human Rights Council (2012) resolution on *The Promotion, Protection, and Enjoyment of Human Rights on the Internet* recognizes "the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms."

That the growth and rapid technological development of the Internet, and access to it, now approaches a basic human right is a remarkable development given just how recently cyberspace and associated digital technologies have evolved. As Leslie Daigle, chief technology officer emerita of the Internet Society, has said, "A sign of success of the Internet is the degree to which we take it for granted" (Daigle 2014).

Not taking for granted the Internet's interoperability and reach only requires recalling the computing environments that historically preceded it. Fragmentation was once patently the norm. Only a few decades ago, in 1981, IBM introduced its first personal computer. In the following decade, computer networks were disconnected isles of technology. Computers made by one company could be interconnected, but not with devices made by another. Digital networks were proprietary, based on closed technical specifications designed specifically *not* to connect with competitors' products. Companies using one type of network, such as IBM's Systems Network Architecture, could not communicate with a customer or business partner using a different environment, such as Digital Equipment Corporation's DECnet or Apple's AppleTalk network.

By design, there was no interoperability between systems. This architected lack of interconnectivity also characterized the popular, but proprietary, online consumer systems of the early 1990s, such as America Online, CompuServe and Prodigy, in which someone using one system could not communicate with someone using another. There was not yet interoperability — the ability to connect between devices, services and applications using standard protocols. The Internet, based on a family of protocols known as Transmission Control Protocol/Internet Protocol (TCP/IP), became the dominant open approach for enabling interconnectivity among diverse computing environments. The potential for universal reach and interoperability afforded by the Internet's technical design was a significant departure from the proprietary and disjointed communication approaches of predecessor computer networks.

Some contemporary trends have raised concerns about movements back toward fragmentation. The revolutionary capacity for universal access and the aspirational expectations for the Internet's accompanying economic and political benefits now stand in tension with geopolitical, technical and economic approaches poised to shift the Internet toward more of a segmented rather than universal system. Under the mantle of cyber sovereignty, governments have attempted to overlay geopolitical borders on the Internet, such as implementing efficient systems of content censorship and filtering, or enacting privacy-related laws mandating restrictions on where and how companies may store customer data. New business models, sometimes referred to as zero-rating services, designed to advance free access to the Internet in emerging markets, have raised questions about whether the next billion Internet users will have access to the global Internet or to only a fraction of cyberspace available for free via walled gardens. There are also concerns about a resurgence of proprietary systems designed specifically not to interoperate with other systems, particularly in the context of new Internet of Things (IoT) products and services, but also as part of broad market

trends away from general-purpose Internet access via browsers to mediation by platform-specific apps. These trends lead to the question of whether, over time, there will be a universal Internet or a fragmented Internet that varies based on country, region or proprietary ecosystem.

Conflicting values are always in tension in the realm of Internet architecture and governance — the broad ecosystem of administrative and design tasks necessary to keep the Internet operational — and the public-policy choices within this ecosystem. Tensions between network universality and enclosure indeed reflect conflicts regarding public-interest values in cyberspace, such as national security versus individual rights and freedom of expression versus privacy. They also reflect increasing incongruity between traditional Westphalian notions of sovereign nation states and a global technological system that crosses national borders and is overseen by a distributed, private-sector-led multi-stakeholder governance framework.

Objectives of national sovereignty and the global flow of information coexist tenuously. The coordination and technical design choices necessary to keep the Internet operational must constantly navigate diverging social values and interests. These alternatives are further complicated by the heterogeneous statutory, cultural and economic conditions that vary by region. To what extent should, or can, regional differences shape a distributed technical architecture that does not map neatly onto geographical borders?

Concern about Internet fragmentation emerged as a theme during the 2014 inception of the Global Commission on Internet Governance (GCIG). The commission viewed the Internet governance debate about fragmentation not as the single issue so often portrayed in policy discourses, but as a constellation of questions crossing many layers of Internet infrastructure, involving many stakeholders, and with potential impacts that are not only technical, but economic and political. So began a process of commissioning scholarly work to examine various dimensions of Internet universality and Internet fragmentation, whether political, economic, infrastructural, legal or content-based. The objective of this research collection is to provide an analysis of the nature and implications of various forms of Internet fragmentation, with the ultimate purpose of improving the evidentiary basis of policy making in this area.

The current paper helps to frame this research by, ironically, deconstructing (fragmenting) universal discussions about Internet fragmentation into a taxonomy of distinct topics that matches how the Internet works in practice and reflects the actual tangible policy choices at hand. Is there a universal Internet now? What are the various trends that could potentially move the Internet away from universality and toward fragmentation, and when is this desirable versus undesirable? What are the policy and design choices that can provide the capacity for a universal Internet but allow for institutional and individual freedom to not be completely interconnected? With these questions in mind, the following is divided into three sections:

- a consideration of the extent to which the contemporary Internet can be viewed as a universal network now;
- an exploration of the implications of emerging geopolitical and socio-economic initiatives associated with the potential for Internet fragmentation; and
- a baseline proposal for the technological characteristics and policy frameworks necessary for affording the Internet with a sustained capacity for ongoing global growth and openness.

THE STATE OF INTERNET UNIVERSALITY

Discussions about fragmentation frequently begin with the assumption that fragmentation is a new or emerging development that threatens the global reach and generativity of the Internet. At the level of infrastructure, the Internet is inherently a heterogeneous assemblage of thousands of different networks, primarily owned and operated by the private sector and able to interconnect only because they adhere to a common set of protocols specifying how to format and exchange information. Because of this interconnection and the capacity, generally, to move information from one point to another, regardless of geographical location, people speak of *the Internet* and express concerns about whether it will fracture into *Internets*.

Examining the prospects and implications of Internet fragmentation first requires acknowledging that the contemporary Internet is not yet universal, geographically, materially or experientially. Divisions and barriers exist across the Internet ecosystem. Because of the complexity and heterogeneity of the global network, it can be useful to examine issues in layers, a conceptual framework that arose at least three decades ago around network protocols, such as the Open Systems Interconnection seven-layer protocol model (physical, data link, network, transport, session, presentation and application layers), or the more flexibly defined TCP/IP four-layer protocol suite (link, Internet, transport, application) (see, for example, Internet Engineering Task Force [IETF] 1989). This layered conceptual approach toward understanding protocols has given way to a norm of viewing the Internet as a layered system, even beyond protocols. In keeping with this tradition, which simply helps to conceptually organize the technological and administrative components of the Internet, this section will examine the state of Internet universality in four conceptual and overlapping categories:

- physical infrastructure (e.g., access, hardware, transmission systems);
- logical resources (e.g., IP addresses, protocols);
- the application and content layer (e.g., data and applications); and
- the legal layer (e.g., national policies and statutes, international treaties).

There is nothing fixed or natural about these categories, but they, or some variation of these categories, are frequently employed to discuss Internet architecture and policy, including discussions about fragmentation (Force Hill 2012; Drake, Cerf and Kleinwächter 2016). The layers also overlap with great complexity. For example, the legal (and policy) layer transcends the other three layers. Nevertheless, they are sufficient to help deconstruct the nuances of calling the Internet a universal network whose essential character may be threatened by fragmentation.

ASSESSING UNIVERSALITY AT THE PHYSICAL INFRASTRUCTURE LAYER

Viewed through the lens of physical infrastructure, the Internet is not yet a universal network. It must first be acknowledged that, by 2016, half of the world still does not have Internet access. According to International Telecommunication Union (ITU) indicators, 3.2 billion people had Internet access by 2015 (ITU 2015). Two billion of these users resided in developing countries, with many newer users accessing the network primarily from mobile phones. Although half the world still does not have Internet access, the growth rate has been exorbitant. As recently as the year 2000, only 400 million people could access the Internet. This number has grown by 700 percent over a 15-year period.

Yet among the half of the world using the Internet, access speeds vary considerably. For example, broadband access speeds in countries such as South Korea, France, Iceland and Denmark are much faster, generally, than the speeds in countries throughout Africa and Latin America. There is also not an even distribution of Internet exchange points (IXPs) around the world, and almost half of countries do not have an IXP within their borders, although the IXP penetration rate is rising rapidly. IXPs are shared interconnection sites at which network operators make agreements to interconnect, thereby serving as essential nodes interconnecting the Internet's backbone. While access, interconnection penetration and access speeds vary, and while a digital divide persists, the trajectory historically has been toward greater access saturation, interconnection growth and broadband connection rates, all indicators of movement toward Internet universality.

ASSESSING UNIVERSALITY AT THE LOGICAL LAYER

Much of what keeps the Internet operational can be described as logical (meaning non-physical, virtual, or software-defined) resources. While the distinctions in practice are much more nuanced, general examples of the Internet's logical layer include: domain names; the global Internet address space of IP version 4 (IPv4) and IP version 6 (IPv6) binary numbers; the Domain Name System (DNS) that translates names into IP addresses; the thousands of protocols that standardize how information should be formatted, addressed, compressed, stored, encrypted, error-checked and transmitted over a network; and even architectural design principles, such as the "end-to-end" principle (Saltzer, Reed and Clark 1984). The end-to-end principle of locating intelligence at network end points has long been associated with the capacity for Internet universality. This groundbreaking technical design principle is often used to describe the logical structure of the Internet, but it does not always apply to the contemporary Internet because of the preponderance of "middle of the network" intelligence mechanisms, such as network address translation (NAT) and security firewalls.

There have historically been examples of fragmentation across all of these logical categories. For example, the Internet does not now have a completely universal address space because of the ongoing transition from one IP address standard to another. To exchange information over the Internet, each device uses a globally unique binary number, either permanently or temporarily assigned for a session. The format of these IP addresses, under a long-standing protocol known as IPv4, assigns 32 bits to each binary address, a design choice that creates a global pool of 2^{32}, or roughly 4.3 billion Internet addresses. In the context of the internationalization and commercialization of the Internet, engineers anticipated that this would be an insufficient number to meet growth demands and designed a new standard, IPv6, to expand addresses to 128 bits long, providing an exponentially larger global address space of 2^{128}, or 340 undecillion addresses. For a variety of reasons related to political and economic incentives, as well as to technological complexities such as IPv6 being not natively backward-compatible with IPv4, IPv6 adoption has taken longer than anticipated (DeNardis 2009).

The Internet *had* a universal address space when the IPv4 address space was predominant, although even then some institutions used private address spaces on internal networks that connected to the global Internet through gateways. And it *would have* a universal address space if IPv6 adoption escalated to the point of deprecating IPv4. While the term "fragmentation" seems overstated, the Internet address space is not uniform in the contemporary context. This long-existing condition also produces, as

Jonah Force Hill aptly describes, "serious interoperability problems within the crucial East/West Internet relationship" because the rate of IPv6 adoption across Asia, a place with far fewer IPv4 addresses than in the West, is so much higher than in the United States and Europe (Force Hill 2012). There is also sometimes fragmentation around the DNS when it is used to block local queries to certain websites, usually for content-blocking purposes such as censorship or enforcement of intellectual property rights.

ASSESSING UNIVERSALITY AT THE APPLICATION AND CONTENT LAYER

For those who do have access, the experience of Internet use varies considerably, often based on cultural and human-rights differences, such as what information is available in which language, level of digital literacy and what information is blocked or censored in a region. The spectrum of digital information available natively in English is much larger than the content available in other languages, so the experience of the Internet obviously varies based on language. Domain names, because they include content, have historically created language fragmentation. For most of the Internet's history, primarily because of its origin in the United States, domain names were only able to use the Latin alphabet, meaning that any languages using Arabic, Chinese, Cyrillic or other non-Latin characters were excluded from domain names. The standards community has developed the means to include non-Latin scripts via internationalized domain names (IDNs), but there are still barriers to the universal accommodation of these IDNs.

Fragmentation at the content level exists in part because of censorship. Information available online in China, in light of China's extensive system of filtering and blocking digital content, is quite distinct from the information available over the Internet in Sweden, for example. Fragmentation at the content level also arises from policies such as the "Right to be Forgotten" law in the European Union, which deletes content locally, or, in another example, geo-IP-restricted Netflix in Canada. The content available in one region is not necessarily the same as that content available in another region. With these differences in mind, the experience of the Internet at the content level is, of course, not universal.

There is also balkanization at the application level. Related to the diminishment of the end-to-end principle, most applications do not have the commensurable interoperability that existed with historically dominant Internet applications, such as email and the World Wide Web. With email, the expectation, and revolutionary innovation, was that anyone using an email client provided by one company could send emails to someone using a different email client. Similarly, someone could reach a website regardless of the browser or search engine used. Some contemporary Internet applications, ranging from Internet voice applications to social media to video games and messaging systems, do not have this interoperability, so are more fragmented. In the mobile environment, "apps" are tied directly to the platform provider and, often, the operating system and require platform mediation and curation. Some applications do not need to interoperate, or are designed not to interoperate for security reasons. For example, financial services applications often rely upon private networks or virtual private networks largely disconnected from the public Internet to achieve requisite performance metrics and security (Yoo 2016). But for general applications, taking the choice away from consumers to interoperate using common application types is a shift in norms. For example, there is no technical reason why making a voice call or sending a message over the Internet would require a proprietary system or gatekeeping function. It is a market technique. There is not necessarily interoperability among the apps used on different mobile platforms, either. Especially given the large number of users accessing the Internet via apps from mobile phones, this variation of fragmentation is significant.

Universal accessibility, however, has continuously improved for people with disabilities, such as those with sight or hearing impairments, largely because of the availability of Web accessibility standards established by the World Wide Web Consortium (W3C). Yet, despite gains, there are many opportunities for greater implementation of universal accessibility standards into applications.

ASSESSING UNIVERSALITY AT THE LEGAL LAYER

Although Internet governance is often viewed as one policy area, it is more accurately described as a broad ecosystem of tasks necessary to keep Internet technologies operational and the enactment of public policies around these technologies. The tasks are carried out by relatively new global institutions, such as the Internet Corporation for Assigned Names and Numbers and the IETF; the policies enacted by private Internet companies; international agreements; and national statutory and administrative frameworks. It is across this latter jurisdictional area of Internet governance that some of the greatest conflicts have historically arisen. The Internet is designed to be inherently cross-border, whereas national laws are bordered and vary significantly by jurisdiction in areas such as hate speech, privacy norms and approaches to intellectual property rights. Nation-state laws conflict with each other but especially stand in tension with the Internet's virtual, cross-border data flows and distributed character. Nations have jurisdictional oversight of the citizens and companies within their borders, but these borders do not comport well with the Internet's distributed and virtual nature.

Bertrand de La Chapelle and Paul Fehlinger (2016) warn about the implications of this disjuncture in their paper *Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation*. They argue that intergovernmental efforts

fail to adequately address cross-border online challenges. Lacking is effective transnational cooperation, and national governments have undertaken legal and technical efforts to expand their jurisdiction in cyberspace. These efforts not only create international tensions, but also pose challenges to the stability of Internet infrastructure and human rights online. The authors recommend the creation of "issue-based governance networks" that facilitate transnational cooperation among actors based on shared principles which allow them to address issues such as requests for content removal.

In *Legal Interoperablity as a Tool for Combatting Fragmentation*, Rolf H. Weber (2014) views legal interoperability as a means to prevent increasing Internet fragmentation and promote growth and expression online. Legal interoperability refers to the "process of making legal rules cooperate across jurisdictions" (ibid., 6). The extent to which legal mechanisms are balanced can be understood on a continuum, with complete assimilation and a fragmented legal landscape constituting the binary opposites. According to Weber, legal approaches need to be tailored to respective issues and contexts. A bottom-up approach is most effective in identifying legal solutions as it allows multiple stakeholders to come together to formulate solutions.

In the contemporary system, there is no harmonization of policy approaches across borders. In many cases, this is preferable because legal harmonization toward repressive information policies would be problematic. In other cases, such as fighting cybercrime, greater cooperation would be desirable. The obvious challenge underpinning the question of legal harmonization is the question of jurisdiction — in other words, determining applicable laws in cross-border conflicts. Territoriality itself is difficult to assess because of complexities over whether jurisdiction is based on server location, user location, registrar location, or where a relevant intermediary is incorporated. While there are some legal treaties, such as the Council of Europe Convention on Cybercrime (also known as the Budapest Convention), there is still a great deal of diversity in legal approaches to the Internet, often shaped by political conceptions of what counts as freedom of expression and privacy and what is the appropriate role of the private sector. As such, cross-border requests have typically involved direct interactions between governments and private intermediaries, whether they entail user data requests, content blocking or another purpose. This approach presents challenges to information intermediaries, who have to navigate relevant and widely diverging laws in all the jurisdictions in which they operate, often under varying statutes regarding intermediary liability. Considering all of these factors, it cannot be said that there is a great deal of universality at the legal layer.

THE IMPLICATIONS OF EXOGENOUS TRENDS TOWARD FRAGMENTATION

While the preceding section indicates that various forms of fragmentation already exist throughout the Internet ecosystem, it also suggests that, especially at the infrastructure and logical layers, the Internet has continuously moved toward universality. Access rates continue to increase, IPv6 growth continues, new IXPs are built, IDNs are adopted. Policy and scholarly concerns about rising forms of Internet fragmentation have arisen from two exogenous trends around the Internet: market-driven fragmentation and geopolitically driven fragmentation. While it is also possible to create a separate discussion on purely technically driven fragmentation, the following section folds these technological issues into the discussions of economic and political contexts shaping Internet fragmentation, and then discusses the projected costs of fragmentation.

MARKET-DRIVEN FRAGMENTATION AND GEOPOLITICALLY DRIVEN FRAGMENTATION

Technological innovations such as the IoT and the rise in cloud-computing approaches create new spaces for the question of fragmentation versus universality. British computer scientist Dame Wendy Hall has said, "The Internet of Things is not yet an Internet."[1] This is a prescient statement because IoT implementations have not demonstrated, or aspired to, the same degree of interoperability and use of competition-enabling open standards as other areas of Internet applications. In *Market-Driven Challenges to Open Internet Standards*, Internet engineer Patrik Fältström (2016) explains how market forces often oppose interoperability and competition in favour of locking users into proprietary services that are unable to interact with competitors' services. This is particularly the case in emerging IoT markets. Fältström uses IP-based lighting-control systems as an example of both an IoT application and an emerging area in which manufacturers take non-interoperable, siloed approaches in which devices they manufacture speak to each other but not with devices made by other companies. These types of proprietary approaches that eschew interoperability and openness are the norm in consumer electronics, and, as Fältström explains, "each company imagines that its proprietary approach will become widely adopted as the 'de facto' standard, with respect to which it will have an obvious competitive advantage over other companies pursuing the same 'maybe it will be me' strategy" (ibid., 7). Another trend is the preponderance of cloud services in which users interact with the service via application programming interfaces (APIs) and are subject to the proprietary service's terms and conditions rather than communicating based on standard protocols.

1 Personal communication to author.

The question of market-driven fragmentation around technological disruption is part of a broader tension that has often arisen in the Internet space around private actors seeking market advantage through digital enclosure and proprietary approaches. In their white paper on Internet fragmentation produced for the World Economic Forum's Future of the Internet Initiative, William Drake, Vinton Cerf and Wolfgang Kleinwächter (2016) provide an extensive taxonomy of the types of commercially driven fragmentation that occur, including peering and interconnection, certain types of net-neutrality violations, walled gardens and geo-blocking of content.

Rising geopolitical challenges around the Internet similarly raise concerns about the prospects for a universal Internet. Jurisdictional conflicts that have always accompanied Internet globalization are complicated by emerging economic, political and technical factors. The economic stakes of digital commerce are high, political contention over content control is rising, and technological structures — such as cloud computing and content distribution networks — are increasingly distributed. More than ever, technologies do not reside neatly within borders, and therefore jurisdictions. Where data is stored (often in more than one place via replication and caching), where a domain name is registered, where employees reside and where a company is incorporated no longer have natural relationships.

In this context of blurred lines between technological and national borders, some governmental policies are seeking to reassert geographical sovereignty in cyberspace, often in specific policy areas. Data localization laws are a prime example. These laws place constraints on how and where private companies store customer data, such as requiring customer data to be stored on servers within a nation's borders or placing various restrictions on the nature of and extent to which customer information is shared across borders (Chander and Le 2015). The impetus for some of these policies concerns customer privacy in the context of foreign surveillance. Accordingly, some arose in the contentious aftermath of disclosures about the expansiveness of the surveillance program of America's National Security Agency. In other cases, the motivation is to create market advantages for indigenous rather than foreign companies.

Data localization laws raise many questions about potential effects on engineering efficiency, the cost of doing business, the ability to innovate and human rights. Concentrating data in a fixed location can actually facilitate efficient surveillance, either from the host country or via foreign surveillance. From an engineering perspective, factors that affect how information is stored and transmitted include the goals of reducing latency, providing redundancy and replication to distribute data closer to its destination, and other basic traffic-engineering and traffic-optimization goals that can conflict with data localization requirements.

Politically driven infrastructure prescriptions also heighten concerns about legal fragmentation. In *A Primer on Globally Harmonizing Internet Jurisdiction and Regulations*, Michael Chertoff and Paul Rosenzweig (2015, 1) warn about the potential legal fracturing of the Internet due to geopolitical trends such as data-localization policies: "We stand on the cusp of a defining moment for the Internet. Existing trends, left unaddressed, might very well lead to the fracturing of the World Wide Web."

Their paper extends the question of which nations' laws jurisdictionally apply in different contexts. In other words, who has power over what? As an alternative to the jurisdictional concerns raised in data localization laws, Chertoff and Rosenzweig propose and evaluate a choice-of-law rule based on four models for clarifying jurisdiction: citizenship of data creator, citizenship of data subject, location of "harm" that has taken place, or citizenship of data custodian. They also provide recommendations about streamlining the Mutual Legal Assistance Treaty (MLAT) structure, which could help minimize incentives for unilateral approaches such as data localization rules.

THE ECONOMIC EFFECTS OF OPENNESS AND FRAGMENTATION

Discussions about the effects of infrastructure prescriptions such as data localization laws often centre on large content intermediaries like Google. What is often overlooked is that these laws also have significant effects on other economic sectors. From financial services to retail, every sector of the economy relies upon digital technologies to store and transmit information about customers or engage in routine business practices such as billing or the delivery of services. Similar to the tech sector, many of these companies in other industries have customers, stores and offices throughout the world, and are not concentrated in any particular country.

James Kaplan and Kayvaun Rowshankish (2015) of McKinsey & Company address the economic implications of data localization laws on the financial services sector in their paper *Addressing the Impact of Data Location Regulation in Financial Services.* Their survey of chief executives in the financial-services sector suggests that data localization laws place significant burdens on private industry, including the complexity costs of navigating and interpreting different regulations across jurisdictions, and of either making technological modifications to comply with new regulations or pulling out of certain markets entirely. For example, to comply with some laws, financial-services companies must locate human resources and technical infrastructure in places where they otherwise would not have a physical presence. As they explain, "Data location regulations make some countries economically unattractive, causing institutions to exit, and limiting their global footprint" (Kaplan and Rowshankish 2015, 3).

The Organisation for Economic Co-operation and Development (OECD) has been doing work to measure global data flows and quantitatively assess the effects of Internet openness. In her paper *Internet Openness and Fragmentation: Toward Measuring the Economic Effects*, OECD senior policy analyst Sarah Box (2016) presents some of the initial results and, in particular, OECD efforts to aggregate and analyze cross-border data flows among the world's countries using corporate data from Google searches and YouTube views. A universally accessible Internet that enables free flows of information across borders is widely understood to have positive effects on trade, whether by improving supply-chain efficiency, expanding customer and market reach, or bettering payment and delivery systems. The knowledge shared freely across borders also stimulates innovation and entrepreneurship. Box's paper addresses the difficulty of establishing empirical evidence of these connections, describes some of the existing studies quantifying the effects of Internet openness, and presents some of the OECD's initial findings, including a "uniform trend of users increasingly accessing content outside their countries," as well as establishing that data flows, while not predictable, often have international dimensions (ibid., 6).

Laws that limit the free flow of information across borders have detrimental effects on the wider economy beyond implications to industry. Researchers Matthias Bauer, Martina Ferracane and Erik van der Marel (2016) quantitatively present the broad costs of data localization laws in their study *Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization*. They developed an index that serves as a proxy for data regulation across various OECD and emerging economies, and then assess the impact of regulations on downstream sectors that make use of data. Their study examines specific laws in 60 jurisdictions, and quantitatively models how data localization laws would engender losses to GDP, decreases in domestic investments and welfare losses to citizens. They conclude, "Accordingly, tight regulations on the free flow of data tend to cause an economy's production structure to shift (back) towards less innovative and relatively volatile sectors such as agriculture, raw materials and natural resources" (ibid., 18).

Another dimension of analysis is that bordered Internet policies rarely correspond to how Internet infrastructure works in practice. Although physical infrastructure such as fibre-optic cable, switching centres, routers and radiofrequency antennas reside within physical borders, neither the logical architecture nor the realities of how information flows over the Internet comport neatly with national borders. This is especially the case in interconnection issues. Routers make decisions about how to forward packets based on issues of network efficiency and resource reachability rather than on where the next hop physically resides. The actual "bordered" areas of the Internet are autonomous systems (AS). The Internet is described as a network of networks but it is more technically accurate to describe it as an interconnected network of virtual AS. Autonomous systems are routing domains, which manage a set of IP addresses either residing in the domain or accessible through that domain to an entity that pays a transit fee to connect to the global Internet through that system. Most understand that handoffs between network operators also require physical interconnections, such as those that occur at shared IXPs. But even these interconnection points do not correspond to a geopolitically bordered view of the Internet, because an exchange of information originating and terminating between two telecommunication companies within a single country can potentially be routed through an IXP located in another country, before being routed back to the originating region.

How company business models, across all sectors of the economy, also use the Internet does not correspond to national borders. Companies can register a domain name in one country; locate servers in another; establish customer service centres in yet another country; and hire content delivery networks (CDNs) or cloud-computing providers to replicate, store or cache information all over the world. Geopolitically driven policies that seek to place borders around dimensions of Internet data flows should also consider the intractability of aligning these policies with the material and virtual reality of how the Internet actually works.

A TECHNICAL DESIGN AND POLICY VISION FOR A UNIVERSAL INTERNET

Internet governance is not static any more than the Internet's technical architecture is static. Contemporary policy choices will affect not only a spectrum of public-interest issues but also the stability and character of the Internet itself, in the same way that architecture reciprocally shapes policy choices. Although various forms of fragmentation already permeate the Internet ecosystem, the generative and open qualities of the network have nevertheless enabled its rapid geographical expansion, and have also created conditions that generally promote an open playing field for entrepreneurs to introduce new systems and applications that could be assured to interoperate with other systems globally. There has been diversity in the types of devices, services and applications enabled largely by conformance to open technical protocols that allow these diverse environments to exchange information with each other.

Given that technological change has been constant in the Internet environment, what fundamental principles or other design characteristics have enabled this growth and innovation? Internet engineer Leslie Daigle (2015), in her paper *On the Nature of the Internet*, acknowledges the constant and rapid transformations in the Internet's underlying technical architecture and suggests that it may be preferable to define the Internet based on its core underlying principles,

or "Internet invariants," as the Internet Society (2012) has described these characteristics. These principles include: global reach/integrity; general purpose; supporting innovation without requiring permission; accessibility; interoperability and mutual agreement; collaboration; reusable (technical) building blocks; and no permanent favourites (Daigle 2015).

All of these principles speak in some way to the Internet's inherent potential for universality. For example, the principle of *global reach* is designed to allow any two devices connected to the Internet to connect with each other, regardless of location or network. The diversity principle of *general purpose* expands this goal to allowing for any application or service to run over the Internet. The principle of *permissionless innovation*, the ability for anyone to set up a new service without requiring anyone else's permission, is linked closely to the universality and openness of the Internet because it creates the capacity and potentiality of innovation to arise from anywhere in the world, and without having to pass through gatekeeping constraints. A closely related principle is *no permanent favourites*. Because the Internet's underlying technical infrastructure enables anyone to connect and introduce new innovation, new entrants are always possible and, in a continuous cycle of disruption and innovation, the entrepreneurs of today are potentially the dominant business people of tomorrow. Perhaps most salient to the potential of a universal Internet is the principle of *interoperability and mutual agreement*.

What has operationalized many of the principles leading to the capacity for Internet universality are the open technical standards that are developed collaboratively in standards-setting institutions such as the IETF and the W3C, as noted, and made publicly available so that others can develop products with the assurance of compatibility with heterogeneous services, devices and applications on the Internet. Internet standards serve as the blueprints developers can use to ensure that their products are interoperable with other products in the marketplace. These standards serve a primary technical purpose, but they also carry political implications and economic externalities. Politically, these institutions sometimes make public-interest decisions, such as on the extent of user privacy or accessibility for the disabled. Economically, technical standards, and the extent to which they have embedded intellectual-property restrictions, are closely linked to innovation because they provide a platform upon which innovation and competition can occur (DeNardis 2011).

Open standards are therefore linked to the question of Internet universality versus fragmentation in three ways. If technical standards sometimes establish public policy, procedural norms of participatory openness, as well as open publication of the standard, are necessary to establish policy-making legitimacy; technically, they provide the interoperability among applications, networks, and services that is necessary for the possibility of global accessibility and reach; and economically, open standards are the primary enabler of market competition and the operationalization of the innovation principle of no permanent favourites.

At the same time, network fragmentation does not always produce detrimental effects. Many of the core technologies necessary for cyber security and basic business operations, such as firewalls and virtual private networks, are designed precisely to "fragment" the Internet. A network with sensitive health records or financial data should not be universally accessible or interoperable. In his paper *Are Two Networks Better Than One? Toward a Theory of Optimal Fragmentation in the Internet*, Christopher S. Yoo (2016) references Metcalfe's law concerning the value of connectivity based on the network-effect insight that, as a network grows, accretion in the number of connections exceeds the growth in the number of nodes. After a point, there can be diminishing marginal returns with additional resources on a network. Yoo also notes that concern about fragmentation must take into account not just optimization of the network as a whole, but also incentives for individual actors.

Lack of interconnection, interoperability and universality are sometimes beneficial, and are indeed carefully designed into systems for the purpose of securing private communication systems or carefully controlling access to and from the global public Internet. But this is an example of a design choice applied to a private network that private entities should be allowed to make, in the same way they should be allowed to choose to connect their private networks to the global public network. Choosing to limit connectivity in certain ways does not foreclose the possibility of connecting in the future or under different circumstances. The potential choice of openness is indeed part of openness.

Many contemporary forces are in tension with traditions of openness: market-driven approaches that seek enclosure and proprietary advantage; geopolitically driven policies that seek to place borders on the Internet; lack of adoption of technologies that address digital resource constraints; and various types of content fragmentation, ranging from censorship to infrastructure-based, intellectual-property-rights enforcement. It is also clear that forces seeking to move the Internet toward greater fragmentation come from both government and the private sector, all complicated by technological disruptions. Furthermore, user choices, to some extent, are also selecting approaches that are arguably more fragmented, such as widespread adoption of proprietary and non-interoperable social-media applications and messaging systems. A great question is whether these tensions will have long-term detrimental effects on the character of the open Internet.

Of course, it has become a mantra to express that the Internet should remain "free and open." But defining "free" and "open" is difficult in practice. Open-source-software communities often make the distinction between "free beer" and "free speech." So too, openness in the context of

Internet governance is contextual and can refer to technical openness (open standards), civil-liberties openness (freedom of expression and association), and openness of digital markets (permissionless innovation and a level playing field for competition). When the term "Internet openness" is used, it can take on any or all of these meanings.

In *A Framework for Understanding Internet Openness*, OECD senior policy analyst Jeremy West (2016) seeks to answer the enigmatic question of what Internet openness is. West posits that there is "no such thing as *the* open Internet," but rather, "Internet openness, which exists in various degrees along several dimensions" (2016, 1) and that "the essence of Internet openness is the global free flow of data across the network" (ibid., 8). The OECD's ongoing work on Internet openness has helped advance an understanding that accounts for network and social heterogeneity while defining openness at three levels: technical, economic and social. Technical openness refers primarily to features of interoperability and universality, such as a universal address space, open protocols and inclusive technology governance. Economic openness refers to features such as infrastructure access at a competitive cost, the capacity for cross-border digital exchange, and regulatory transparency and certainty. Social openness invokes a collection of human rights online, such as the right to privacy, the right to education, and rights of freedom of expression and association.

This collection of GCIG research papers, taken as a whole, advances research and informs policy making in several ways. It suggests that, while the Internet has not yet achieved universality, its aspirational capacity for global reach and interoperability is being challenged by a number of exogenous pressures, both market-driven and geopolitical. Systems of Internet infrastructure and governance are increasingly recognized as critical points of control for achieving market advantage or carrying out geopolitical or global economic objectives. Many efforts to gain political and economic advantage bring the network toward fragmentation and away from universality, and this movement is not without costs to national economies, human rights, and the stability and security of the Internet. Preserving one Internet requires policies (see Table 1) that: incentivize infrastructure advancements such as the adoption of IPv6, growth in broadband access, and the global distribution of IXPs and undersea cables; promote trust by providing strong cyber security and a universal framework of basic human rights online; promote conditions for open innovation models geared toward permissionless innovation and access to knowledge rather than proprietary advantage and information enclosure; and preserve the inclusive and participatory multi-stakeholder model of Internet governance over emerging efforts geared toward cyber sovereignty, multilateralism and state control. As Internet technological disruption rapidly evolves toward the IoT and other emerging cyber systems pervading every corner of social and economic life, the enclosure or openness of these new market innovations will help determine whether the digital sphere is constituted by non-interoperable fragments or a universal Internet.

Table 1: Baseline Characteristics of Internet Universality

Layer	Internet Governance Characteristic
Physical Infrastructure	• Investments in broadband access penetration • Policies that promote the development of IXPs and other interconnection and transmission systems in emerging markets • Human capacity building
Logical Resources	• A universal IP address space • A universally consistent and stable DNS • Adoption of IPv6 • Open technical standards that are open in participation and implementation, and engender multiple competing products that are interoperable • Human capacity building in standards setting and critical logical resources
Application and Content Layer	• Promotion of global access to knowledge rather than censorship of lawful content • Universal support of IDNs • Applications that adopt standards of accessibility for the disabled • Promotion of digital literacy • Promotion of interoperability norms in emerging contexts such as IoT
Legal Layer	• Rejection of government policies that restrict the flow of data across borders and have detrimental effects on trade, economic growth and freedom of expression • Agreements among governments to not tamper with the core infrastructure of the Internet, such as the DNS and systems of routing and interconnection • Promotion of the private-sector-led multi-stakeholder governance system

Source: Author.

WORKS CITED

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.* GCIG Papers Series No. 30. Waterloo, ON: CIGI. www.cigionline.org/publications/tracing-economic-impact-of-regulations-free-flow-of-data-and-data-localization.

Box, Sarah. 2016. *Internet Openness and Fragmentation: Toward Measuring the Economic Effects*. GCIG Papers Series No. 36. Waterloo, ON: CIGI. www.cigionline.org/publications/internet-openness-and-fragmentation-toward-measuring-economic-effects.

Chander, Anupam and Uyen Le. 2015. "Data Nationalism." *Emory Law Journal* 64 (3): 677–739.

Chertoff, Michael and Paul Rosenzweig. 2015. *A Primer on Globally Harmonizing Internet Jurisdiction and Regulations.* GCIG Paper Series No. 10. Waterloo, ON: CIGI. ourinternet.org/publication/a-primer-on-globally-harmonizing-internet-jurisdiction-and-regulations.

CIGI-Ipsos. 2014. CIGI-Ipsos Survey on Global Security and Trust. www.cigionline.org/internet-survey.

Daigle, Leslie. 2014. "Permissionless Innovation — Openness, Not Anarchy." *Internet Society Tech Matters* (blog), April 22. www.internetsociety.org/blog/tech-matters/2014/04/permissionless-innovation-openness-not-anarchy.

———. 2015. *On the Nature of the Internet*. GCIG Paper Series No. 7. Waterloo, ON: CIGI. www.ourinternet.org/publication/on-the-nature-of-the-internet.

de La Chapelle, Bertrand and Paul Fehlinger. 2016. *Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation*. GCIG Paper Series No. 28. Waterloo, ON: CIGI. www.ourinternet.org/publication/jurisdiction-on-the-internet.

DeNardis, Laura. 2009. *Protocol Politics: The Globalization of Internet Governance.* Cambridge, MA: MIT Press.

———, ed. 2011. *Opening Standards: The Global Politics of Interoperability*. Cambridge, MA: MIT Press.

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. www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

Fältström, Patrik. 2016. *Market-Driven Challenges to Open Internet Standards.* GCIG Papers Series No. 33. Waterloo, ON: CIGI. www.cigionline.org/publications/market-driven-challenges-open-internet-standards.

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, John F. Kennedy School of Government, Harvard University. http://belfercenter.hks.harvard.edu/files/internet_fragmentation_jonah_hill.pdf.

IETF. 1989. "Request for Comments 1122: Requirements for Internet Hosts — Communication Layers." Edited by Robert Braden, October. www.tools.ietf.org/html/rfc1122.

Internet Society. 2012. "Internet Invariants: What Really Matters." www.internetsociety.org/internet-invariants-what-really-matters.

ITU. 2015. "ICT Facts and Figures — The World in 2015." www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

Kaplan, James and Kayvaun Rowshankish. 2015. *Addressing the Impact of Data Location Regulation in Financial Services*. GCIG Paper Series No. 14. Waterloo, ON: CIGI. www.ourinternet.org/publication/addressing-the-impact-of-data-location-regulation-in-financial-services.

Saltzer, Jerome, David Reed and David Clark. 1984. "End-to-End Arguments in System Design." *ACM Transactions on Computer Systems 2* (4): 277–88.

United Nations Human Rights Council. 2012. *Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet*. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx.

Weber, Rolf H. 2014. *Legal Interoperablity as a Tool for Combatting Fragmentation.* GCIG Papers Series No. 4. Waterloo, ON: CIGI. www.ourinternet.org/publication/legal-interoperability-as-a-tool-for-combatting-fragmentation.

Werbach, Kevin. 2008. "The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing it Apart." *University of California Davis Law Review* 42: 343–412.

West, Jeremy. 2016. *A Framework for Understanding Internet Openness*. GCIG Papers Series No. 35. Waterloo, ON: CIGI. www.cigionline.org/publications/framework-understanding-internet-openness.

Yoo, Christopher S. 2016. *When Are Two Networks Better than One? Towards a Theory of Optimal Fragmentation in the Internet*. GCIG Papers Series No. 37. Waterloo, ON: CIGI. www.cigionline.org/publications/when-are-two-networks-better-one-toward-theory-of-optimal-fragmentation.

ABOUT CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on three themes: the global economy; global security & politics; and international law.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

For more information, please visit www.cigionline.org.

ABOUT CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is based in London. Chatham House's mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all. The institute: engages governments, the private sector, civil society and its members in open debates and confidential discussions about significant developments in international affairs; produces independent and rigorous analysis of critical global, regional and country-specific challenges and opportunities; and offers new ideas to decision-makers and -shapers on how these could best be tackled from the near- to the long-term. For more information, please visit: www.chathamhouse.org.

CIGI MASTHEAD

Executive

President	Rohinton P. Medhora
Director of Finance	Shelley Boettger
Director of the International Law Research Program	Oonagh Fitzgerald
Director of the Global Security & Politics Program	Fen Osler Hampson
Director of Human Resources	Susan Hirst
Director of the Global Economy Program	Domenico Lombardi
Chief of Staff and General Counsel	Aaron Shull
Director of Communications and Digital Media	Spencer Tripp

Publications

Publisher	Carol Bonnett
Senior Publications Editor	Jennifer Goyder
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Publications Editor	Lynn Schellenberg
Graphic Designer	Sara Moore
Graphic Designer	Melodie Wakefield

Communications

For media enquiries, please contact communications@cigionline.org.

CIGI
67 Erb Street West
Waterloo, Ontario N2L 6C2
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs
10 St James's Square
London, England SW1Y 4LE, United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org