CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission on Internet Governance

ourinternet.org

PAPER SERIES: NO. 35 — MAY 2016

A Framework for Understanding Internet Openness

Jeremy West

A FRAMEWORK FOR UNDERSTANDING INTERNET OPENNESS

Jeremy West

CHATHAM HOUSE
The Royal Institute of International Affairs

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

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

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.

Disclaimer: This work draws on research conducted for the OECD Committee on Digital Economy Policy concerning the economic and social benefits of Internet openness. However, the opinions expressed and arguments employed herein are solely those of the author and do not necessarily reflect the official views of the OECD or of its member countries.

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

vi About the Global Commission on Internet Governance

vi About the Author

1 Acronyms

1 Executive Summary

1 Introduction

1 The Open Internet versus Internet Openness

2 Openness at a Glance

3 Technical Openness

5 Economic Openness

5 Social Openness

6 Other Facets of Openness

8 Conclusion

8 Works Cited

12 About CIGI

12 About Chatham House

12 CIGI Masthead

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

Jeremy West is a senior policy analyst in the Digital Economy Policy Division of the Directorate for Science, Technology and Innovation at the Organisation for Economic Co-operation and Development (OECD). He recently led a multidisciplinary project on intellectual property in the digital age and is currently researching the economic and social effects of Internet openness. Jeremy's background is in competition law and includes experience at a law firm in Washington, DC, at the United States Department of Justice and with the New Zealand Commerce Commission. Jeremy serves on the editorial boards of the *Antitrust Law Journal* and *Oxford Competition Law*, and is a member of the State Bar of California and the District of Columbia Bar. His OECD papers have been cited by the United States Antitrust Modernization Commission, the *Financial Times* and in scholarly journals.

ACRONYMS

CGN	carrier-grade NAT
DNS	domain name system
http	hypertext transfer protocol
IP	Internet Protocol
NAT	network address translator
OECD	Organisation for Economic Co-operation and Development
RTBF	right to be forgotten
SMTP	Simple Mail Transfer Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
URL	universal resource locator

EXECUTIVE SUMMARY

Over the past several years, observers have been aware that the Internet is becoming less "open." Yet, although organizations such as the Organisation for Economic Co-operation and Development (OECD) have concluded that a link exists between the Internet's origins as a system designed to be open by default and its ability to promote economic growth and social well-being, the pressures on the Internet to be more "closed" have persisted. This situation is ripe for analysis.

Achieving a better understanding of both how changes in openness affect economies and societies and how various stakeholder actions and inactions affect openness begins with a fundamental step: defining "Internet openness." That is the objective of this paper.

The term "open Internet" has been in circulation for several years, but it signifies different things to different people. It therefore causes confusion and is not well-suited for analysis. This paper concludes that there is no such thing as *the* open Internet. Instead, there is Internet openness, which exists in degrees along several dimensions. Those dimensions include not only technical considerations but also many others — such as market conditions, governance, legal environments and procedures, and human rights. Consequently, a large and diverse set of circumstances and stakeholder actions influence Internet openness.

INTRODUCTION

"As divergent forces tug at the internet, it is in danger of losing its universality and splintering into separate digital domains," *The Economist* (2010) stated. That was now more than five years ago. Although the OECD (2008; 2014), among other bodies, has recognized the link between a distributed, interconnected architecture designed to be open by default and the Internet's catalyst role for economic growth and social well-being, the splintering forces remain. These forces vary widely in nature and apply pressure at different levels of the Internet. They can be found in private sector actions as well as in public policies and governance.

A key question for policy makers is where they should aim to position their countries in the multidimensional Internet openness space. A number of important multi-stakeholder objectives — for example, sovereignty, public safety and economic development — call for actions that can lead to different degrees of openness. Because the Internet is a "network of networks," the probability that interventions will have unintended consequences is higher than it would otherwise be. Addressing the needs of some stakeholders could be politically expedient, for example, but it might also cause unintended harm to the more numerous but less visible masses. Setting and implementing sound policies related to openness can therefore be a challenging undertaking.

To help policy makers reach more informed decisions about Internet openness, the OECD has begun to develop a framework for analysis. It includes a definition of Internet openness, a broad description of the types of benefits — as well as some of the harms — that are associated with it, and a suite of relevant stakeholder objectives. The OECD is also looking at the way those objectives are translating into actions and conditions, with particular attention to how they affect openness at different layers of the Internet. The scope of the OECD's project includes gathering initial evidence of the economic and social benefits of Internet openness (and the impact of reducing openness), with a focus on international trade, innovation and entrepreneurship, macroeconomic performance and societal well-being. This paper, drawing on research conducted by the author for the OECD Committee on Digital Economy Policy, proposes a definition of "Internet openness."[1]

THE OPEN INTERNET VERSUS INTERNET OPENNESS

Although the term "open Internet" is used frequently, it has no universally accepted definition. It is a convenient phrase, like "level playing field," that glosses over complexities. It tends to be used on the assumption that everyone agrees on its meaning, but they do not. To some, it means technical openness (for example, global interoperability of transfer protocols). To others, it means openness in a human rights sense (such as freedom

1 This paper should be read in conjunction with GCIG Paper No. 36, *Internet Openness and Fragmentation: Toward Measuring Economic Effectiveness*, by Sarah Box.

from online censorship). Many use it interchangeably with other terms that do not have a universally adopted definition (for example, "net neutrality"), or it may be intended as shorthand for a particular characteristic such as geographically or demographically broad access to the Internet. As a result, the term causes confusion.

Furthermore, speaking about an open Internet suggests that Internet openness is binary — that it can only be fully open or fully closed. Even if one considers only the technical aspects of openness, the binary view does not correspond with how the Internet actually works. The Internet is a layered arrangement consisting of a physical access and transport infrastructure, an agreed set of packet and transport protocols, a domain name system (DNS), an Internet Protocol (IP) address system, applications and content. Together, the layers enable data flows that travel between user devices located at the edges of the network. Technical openness depends on the conditions at each of those layers. Some of the conditions increase openness, while others restrict it. Some even do both simultaneously. Certain conditions affect openness more strongly than others, and they can also affect different aspects of openness. But they do not simply turn openness "on" or "off."

For example, one condition that affects openness at the IP address layer is the shortage of IP addresses that has arisen due to the limitations of IP version four (IPv4), a protocol that identifies devices on a network. The shortage of available IP addresses makes it harder to connect more users and devices to the Internet (a closing effect). Therefore, a workaround solution — called a network address translator, or NAT — was created. A NAT allows multiple devices to share the same IP address. Many of the boxes that provide fixed broadband Internet access and Wi-Fi in homes have NATs built into them, enabling all of the Internet-connected devices within the home to use the same IP address. A carrier-grade NAT, or CGN, is a supersized NAT that allows many homes and other end sites to share small pools of IP addresses. CGNs increase openness by improving access to the Internet. However, they do not provide unlimited access, and in any event CGNs simultaneously reduce accountability by essentially hiding or anonymizing user activity — a closing effect. Consequently, CGNs neither fully open nor fully close the Internet, but they do affect its openness.

In fact, the Internet has rarely, if ever, been either fully open or fully closed. On the one hand, absolute openness — if such a state is even possible — would require the end of arrangements that are critical for economic and social reasons, such as having to pay for hardware and Internet access and enforcing child pornography laws. On the other hand, total closure would transform the Internet into nothing more than a series of isolated nodes, at which point it would cease to be a network at all.

The reality is that the Internet has degrees of both openness and "closedness" along many vectors. Therefore, the question to ask is not whether the Internet is open or closed, but how much openness or closedness it has, and in what dimensions. In fact, Internet openness is always in a state of flux, continuously becoming more open in some dimensions and more closed in others.

Accordingly, it is more helpful to study Internet openness with a multidimensional space in mind than with a basic open-or-closed perspective. That is why the oversimplifying term "open Internet" has been rejected in this paper in favour of "Internet openness."

In keeping with that choice, this paper adopts a broad view of Internet openness, one that goes well beyond a purely technical view and encompasses economic, social and other factors. On the one hand, technical openness increases when openly available protocols are used consistently to receive and send data flows across interoperable layers of the Internet, relying on an open and consistent IP address system and a uniform convention for domain names. Thus, for example, the more that devices connected to the Internet consistently use the Transmission Control Protocol/Internet Protocol (TCP/IP), the more technical openness there will be. On the other hand, the more that non-standard data flow control algorithms are used, the less technical openness there will be.

Economic openness varies with the ability of users to get online and to use the Internet to enhance their economic opportunities and to put them to productive uses. For instance, economic openness increases as broadband infrastructure grows, but it decreases when access providers lack competition and charge higher prices or provide poorer service as a result.

Social openness is positively related to the ability of individuals to use the Internet to broaden their non-pecuniary opportunities, such as keeping in touch more easily with family and friends, becoming more informed about topics of interest to them or expressing themselves. As an illustration, social openness increases when laws curtailing political expression are eased. It decreases when access to online educational material is eliminated because a government decides to block the entire platform through which the material is available.

OPENNESS AT A GLANCE

Table 1 sets out the elements of openness that are discussed throughout this paper.

Table 1: Elements of Internet Openness

Technical	Economic	Social	Other
• End-to-end principle: – use of consistent standards – interoperable – open, consistent address space – uniform convention for domain names • Open protocols for core functions	• Cross-border supply and consumption • Economic accessibility • Regulatory transparency and certainty	• Respect for human rights: – freedom of expression – freedom to associate – privacy – freedom from discrimination – education	• Digital security: – availability – integrity – confidentiality – *but* with some vulnerability • Empowerment of users over data sent and received • Distributed control • Inclusive governance • Multilingualism

Source: Author.

TECHNICAL OPENNESS

A core feature of technical openness is the end-to-end principle (Saltzer, Reed and Clark 1981; Blumenthal and Clark 2001). The intended role of an open switched network that follows the end-to-end principle is limited to carrying individual data packets from source to destination. It does not alter or interfere with the packets; it just transports them, and it does so without favouring one stream of packets over another. All user access and all functions and services that populate the network are provided by devices that sit outside of the network itself. These devices communicate among themselves in a manner that is largely opaque to the network. In other words, the network should not replicate functions that can be performed by communicating end systems.

Like most elements of openness, the end-to-end principle is not an all-or-nothing absolute requirement, though. Rather, it is a principle that, in practice, may be followed to a greater or lesser degree in a network. The more it is followed, the more openness the network has. Stakeholders may thus prefer, or aspire to, an ideal of a fully end-to-end network, but just because a network might not be 100 percent end-to-end in practice does not mean that there is no openness in the network. Thus, the end-to-end principle is not to be confused with a set of network engineering constraints. Various services may operate in ways that are not precisely aligned to it. However, the extent to which particular network components can successfully operate while not adhering exactly to these broad precepts is bounded by the ability of other network components that operate according to these principles to successfully interoperate with them.

In an open switched network, the end-to-end principle requires the use of consistent technical standards. That means all active, packet-switching elements in the network use a uniform interpretation of the contents of each packet, supporting precisely the same protocol (in the case of the Internet, this is the IP specification). Consistency also means that all connected systems inside the network are able to communicate by using the same transport protocols. The Internet has commonly adopted two end-to-end transport protocols, the TCP and the User Datagram Protocol (UDP). While many other transport protocols have been defined, common convention in the Internet has settled on TCP and UDP as the two "universal" end-to-end transport protocols. The more consistently that connected systems around the world communicate by using these protocols, the more Internet openness increases.

Consistent technical standards contribute to another feature of technical openness: interoperability, that is, the ability to use any layer of the Internet without arbitrary, technical restriction. (Such use is not necessarily free of charge, however.) Furthermore, interoperability implies that there are no inherent or arbitrary technical restrictions interfering with anyone's ability to provide goods and services at any layer, whether it be transmission capacity, switching, domain names, applications or any of the other layers that make up the Internet. Interoperability leads to greater freedom of choice: the freer consumers are to choose the devices, applications and services they use, and the freer providers are to choose the types of devices, applications and services they offer, the more open the network is deemed to be.[2]

2 Note that "interoperability," as the term is used here, refers to interoperability with the network. It does not imply that devices sitting outside the network must be interoperable with each other, but only that the protocols used by the network should be available to device makers so that they can make their products compatible with the network. Thus, for example, iPhones and Android phones can both connect to the Internet, but they run on different operating systems.

The end-to-end principle also demands an open, consistent address space. This condition means every destination on the Internet is reachable from any other location on the Internet, which requires all destinations to have their own IP address that everyone else can reach. IP addresses must therefore be allocated and administered in such a way that each address is uniquely associated not only with a single network, but with a single device within that network. The network itself cannot resolve clashes where two or more devices are using the same address, so the responsibility for ensuring that all addresses are used in a manner that is unique is left to the bodies who administer address allocation and registration.[3]

The next requirement of the end-to-end principle is a uniform convention for domain names. The DNS is the combination of a common convention for creating names and a consistent methodology for transforming a universal resource locator (URL) from a format that is easy for humans to use into a format that is easy for machines to use (the "name resolution" function). In other words, the DNS allows people to use familiar symbols and terms, such as "www.oecd.org," when referring to service points connected to the Internet, instead of numeric IP addresses and transport protocol port numbers, such as "194.66.82.11." For the DNS to work properly, certain rules have to be followed when creating the names, and each name has to be tied to a single IP address.

Whenever data is sent from one Internet-connected device to another, there is a DNS query. The query asks the DNS what the correct IP address is for the desired recipient of the data flow. Regardless of where and how a DNS query is generated, the response should reflect the current state of the authentic information published in the DNS. The implication here is that the DNS uses the name space derived from a single and unique root zone, with all name resolvers answering name queries by searching within that uniquely rooted name space. If that does not occur, then, when a user types, for example,"www.yahoo.fr" he or she might wind up looking at the home page for, say, *El País*, thereby introducing an element of chaos that would severely undermine the Internet's utility.

The more closely and consistently the end-to-end principle is followed, the greater the likelihood that no matter where data originates and what path it takes as it travels across the Internet, it will arrive intact at the intended destination, and only that destination.

Finally, technical openness also increases with the adoption of open protocols, at least for a number of core Internet functions. Open protocols are openly available, meaning they are not encumbered by restrictive claims of control or ownership. A number of open, commonly defined application-level protocols have already been adopted for core services. For example, applications that pass email messages are expected to use the Simple Mail Transfer Protocol (SMTP) and browsers are expected to use the hypertext transfer protocol (http). Other network-wide functions, including data transfer, instant messaging and presence notification, are also supported by open protocols.

However, proprietary protocols do exist, even for core functions such as sending data across the Internet. Some companies have incentives for using proprietary transit protocols. Their motive, at least in some instances, is to try to use a disproportionate share of the available bandwidth for their own communications without experiencing packet loss (which occurs when packets of data travelling across the Internet do not reach their destination). See Box 1 for more details.

The open nature of the technical foundation of the Internet is critical to the Internet's "identity." It is what it is today largely because of its technical openness. Policy actions and inactions that restrict technical openness have the capability to weaken the Internet's security, flexibility and stability.

ECONOMIC OPENNESS

The Internet's economic openness corresponds to the ability of people, businesses and organizations to get online and use the Internet to increase their economic opportunities and capitalize on them. Increasing one's economic opportunities via the Internet naturally depends on access to the Internet. Having economic access means that the requisite infrastructure for connecting to the Internet is available, and at a competitive price. The better the markets for Internet service, computers, smartphones and other connecting devices function, the more open and inclusive the digital economy will be. Economic access requires investment in electricity and broadband infrastructure as well as sound competition policy (OECD 2014, 7, 19-20).

Consider the case of telecommunications market liberalization in Kenya. When Telkom Kenya's monopoly on the Internet backbone ended and two new firms entered the scene, they brought competition into the country's market for Internet access for the first time. As a result of that and other pro-competitive policies, bandwidth availability increased and service costs to operators

3 Address allocation and registration has been an evolutionary process. The original address administration and registry function was managed through US research agencies. The evolution of that model led to the creation of five regional Internet registries, each of which serves the address allocation and registry function needs of regional communities. The practices relating to access of address space through allocation and assignment are based on policies developed by the respective address communities in each region. The general theme of these policies is one of "demonstrated need," where addresses are available to applicants who can demonstrate their need for these addresses within their intended service infrastructure.

Box 1: Non-Standard Flow Control Algorithms

The end-to-end principle assumes that TCP is the predominant protocol used by hosts connected to the Internet. In particular, it assumes that the data flow control algorithm used by all TCP implementations behaves in very similar ways across the Internet. That algorithm relies on the aggregate outcome of the TCP flow control protocols to provide a fair-share allocation of common network resources, so that an approximately equal proportion of those resources is devoted to each active flow. In other words, no one flow is more important than any other.

Specifically, each TCP session will both impose pressure on and respond to pressure from other concurrent sessions in trying to reach a point where the network's bandwidth is shared equally across the concurrent active flows. Packet loss occurs when there is too much pressure, so a flow will gradually increase its sending rate until the onset of packet loss, at which point it will immediately halve its sending rate. It will then gradually probe with increased rates until the next packet loss event. TCP implementations that use a different flow control algorithm normally fare worse, as their efforts to put more pressure on other flows often result in packet loss in their own flow.

However, there has been a significant body of research into flow control algorithms and some have emerged that appear to be able to secure a greater relative share of network resources without the self-damage problem. These algorithms are capable of exerting "unfair" pressure on other concurrent TCP flows, consuming a disproportionate share of network resources. Examples include Akamai's FastDNS, Google's QUIC and some Linux distributions using CUBIC.

Source: Geoff Huston, consultant to the OECD.

declined. In fact, their rates dropped by some 90 percent and those savings were passed along to consumers, who also benefited from wider geographic access. The number of Internet users in Kenya more than doubled during the year after liberalization. "Today, thanks largely to a liberal market approach complemented by proactive and effective policymaking, Kenya is a regional hub for tech and Internet start-ups and has attracted substantial investment from employers like IBM and Microsoft" (Dalberg 2014, 18).

The access aspect of economic openness goes beyond merely being able to connect to the Internet. It also refers to the degree to which entrepreneurs — from individuals to global companies — can capitalize on the economic opportunities enabled by the Internet without interference from over-inclusive or anticompetitive regulations (for example, unnecessarily broad content-based filtering or blocking policies). Private sector conduct, such as making it unreasonably difficult to sell an application in a platform's app store, can have a restrictive effect on economic openness, too. Conversely, the easier it is to legally use and sell applications, products, content and services on the Internet, the wider the economic opportunities will be.

Economic openness also refers to the ability to consume and supply services over the Internet on a cross-border basis. The fewer unjustifiable barriers there are that prevent users from accessing, generating and selling the lawful content, applications and services of their choice, regardless of the jurisdiction they are coming from or going to, the more economically open the Internet is considered to be (OECD 2014, 7). Examples of justifiable barriers to cross-border data (content) flows include well-tailored measures that protect public safety or preserve culture and national values. Note that privacy- and security-enhancing measures are not deemed to be barriers to openness when they balance fundamental rights, freedoms and principles and comply with the OECD's guidelines on privacy (OECD 2013) and security (OECD 2015). Indeed, such measures (discussed below) are considered to enhance openness.

Economic openness also depends on regulatory transparency and certainty. The clearer the laws, rights and regulations concerning the Internet, and the fairer the process for enforcing them, the greater the regulatory transparency and certainty (OECD 2014, 10). Regulatory transparency and certainty increase economic openness by reducing one of the risks of doing business as either a buyer or a seller in the digital economy: the risk of violating applicable laws or of being unable to defend one's rights adequately.

SOCIAL OPENNESS

The Internet's social openness corresponds to the ability of individuals to use the Internet to broaden their non-pecuniary opportunities. Such opportunities could include their meeting new people and exchanging knowledge and ideas with them, keeping in touch more easily with family and friends, expressing themselves to a potentially wider audience than they would otherwise be able to reach, becoming more informed about topics that are personally meaningful, gaining a better understanding of what their elected representatives in government are doing and becoming more active in their communities. The social aspects of Internet openness can reverberate and have a positive effect on economic openness. In particular, enhancing elements such as freedom of expression promotes more than human rights; it promotes innovation, as well. Innovation depends greatly on knowledge

sharing and collaboration, and restrictions on freedom of expression online can inhibit sharing and collaboration.

The protection, promotion and enjoyment of all human rights is closely connected to the Internet's social openness. Consecutive resolutions of the United Nations Human Rights Council affirm that all human rights apply online just as they do off-line. Human rights include, for example, freedom of opinion and expression, freedom to associate, privacy, and education (United Nations [UN] 1948, articles 12, 19, 20, 23, 26; UN 2012). To see how human rights can bear on social openness, consider freedom from discrimination (UN 1948, article 2), which is particularly relevant in the context of access. If individuals are being denied access to lawful content and services online on the basis of their race, colour, sex, language, religion, political or other opinion, national or social origin, and so on, there is an obvious negative effect on social openness. Conversely, then, the more access that individuals have to lawful content and services online without interference based on those factors, the more socially open the Internet is. (Interestingly, the relationship between human rights and Internet openness is mutually reinforcing. Not only does respect for human rights generally enhance openness, but openness facilitates human rights [OECD 2014, 20].)

Although the concept of Internet openness incorporates consideration of the respect accorded these rights, making human rights ever stronger will not necessarily always result in more openness. Eventually, some of these rights would become so strong that they would impinge on each other and, as a result, on openness. For example, if freedom of expression were limitless, it would be legal to post child pornography on the Internet. See Box 2 for another example.

Box 2: The Right to Be Forgotten

If extended far enough, some human or fundamental rights might eventually conflict with one another. For example, in 2014 the Court of Justice of the European Union ruled that under certain conditions individuals have the right to ask search engines to remove links with personal information about them. The right applies when the information is inaccurate, irrelevant, inadequate or excessive for the purposes of the data processing (Google Spain SL v Agencia Española de Protección de Datos, C-131/12, May 13, 2014, para. 93). The Court of Justice acknowledged that the "right to be forgotten" (RTBF) is not absolute and that it will therefore need to be balanced with other fundamental rights, such as freedom of expression (ibid., para. 85).

The RTBF also illustrates the tension that can arise between privacy and openness. The RTBF increases privacy and therefore may increase trust, resulting in an opening effect. At the same time, the RTBF takes information off-line, which arguably has a closing effect. Each country must decide for itself how to manage the relationship between privacy and openness. Indeed, jurisdictions such as the European Union and the United States differ on the RTBF, as the right is protected in the European Union but not in the United States. Which jurisdiction has a more open Internet policy as a result is a subjective question.

OTHER FACETS OF OPENNESS

Certain elements of openness do not fit neatly within the categories of technical, economic or social openness. They might cut across some or all of the categories, or they might just have different natures altogether. One such element is the empowerment of individuals to understand and control how their private data is used online, as well as to control the information they receive online (OECD 2014, 12). Empowerment corresponds with the degree to which Internet users are provided with useful, comprehensible information about the privacy ramifications of their online activities as well as the degree to which they can control those ramifications. Are there laws, regulations or industry codes of conduct in place that require online services to inform users about what personal data is being retained and how it will be used? To what extent do users have control over how their data is used? Note that in this context more openness for some stakeholders might imply less for others. For example, more openness for business in the form of greater freedom to use the personal data of its customers might imply less openness in the form of lower transparency, awareness or control for individuals. Conversely, more openness for individuals in the form of greater empowerment over their personal data might imply less openness for businesses.

The level of empowerment also depends on how much control users have over the amount and type of information they receive via the Internet. Are their email accounts flooded with spam? Are they able to block mail from certain accounts? Can they protect their children from content they consider to be harmful?

Empowerment is relevant to openness because it fosters trust in the Internet. The OECD's *Principles for Internet Policy Making* (2014, 25) envision a cooperative effort on empowerment, in which governments, the private sector, the Internet technical community and civil society "work together to provide the capacity for appropriate and effective individual control over the receipt of information and disclosure of personal data." The inclusion of the word "appropriate" reflects that a measured amount of control over one's personal data is called for.

Thus there can be too much or too little empowerment, but the right amount promotes openness. For example, great strides in medical research can be made with data that is collected via the Internet. If the data is suitably de-identified, the danger to personal privacy presented by its collection and use could be low while the benefits for human health could be high. However, if users were able to invoke a blanket refusal that prevented any of their personal data from being used in any manner, no matter how many measures were taken to strip out its personally identifying tags, the result could well be considered a net loss for society.

Although Internet openness catalyzes a host of economic and social benefits, it can also expose users to online intrusions, fraud, extortion, ransomware, intellectual property theft, denial-of-service attacks and a variety of other dangers. Those cyber activities threaten economic and social well-being by exposing personal and private data, harming financial and public infrastructure, threatening public safety, subverting human rights and depriving businesses of the fruits of their innovation and investment. What is needed to combat these threats and to preserve the Internet's ability to carry global data flows safely is digital security. Security is, therefore, another element of openness. Security cuts across all of the dimensions — technical, economic and social — of openness, and has three main components.

Confidentiality

The greater the availability to end-users of robust and uncompromised protection from third-party eavesdropping and unauthorized access to data, the more confidentiality they will have when they send and store data on the Internet (where "data" means any content that flows over the Internet, such as credit card numbers, bank account information, trade secrets, private conversations, photographs and so on).

Integrity

The better able end-users are to verify the identity of whomever they are communicating with and to ensure that received communications are genuine and precise copies of what was sent, the more integrity their communications will have.

Availability

The greater a network's ability to withstand a cyber attack or hacking attempt without any interruption of service to users, the more availability that network has.

All else being equal, the more effective a network's digital security measures are, the more users will trust and rely on the network. In short, any notion that digital security must be viewed as a closing element is incorrect, because it is critical for building trust in the Internet. If trust declines enough, people will be less likely to use the Internet than they would otherwise be and data flows will shrink. Consequently, a better way to look at digital security is to recognize it as an element that contributes to openness, provided it balances fundamental rights, freedoms and principles and complies with the OECD's (2015) security guidelines.

This is not to say that absolutely airtight digital security would always be optimal (even if it existed, which it does not). Some degree of intrusion could be justified on grounds such as national security or law enforcement needs. In addition, stronger security comes at a financial cost, so it will be efficient for individuals and businesses to opt for a lower level of security for some or all of their activities.

Furthermore, any degree of Internet openness necessarily implies a certain amount of vulnerability. Internet security risks cannot be eradicated as long as the component networks remain interoperable and have any ability to communicate with one another. Ultimate security would require cutting oneself off from the Internet altogether, which would have an obvious closing effect. Accordingly, the OECD's *Principles for Internet Policy Making* (2014, 11) recognize that "strong" privacy protection rather than "absolute" privacy protection "is critical to ensuring that the Internet fulfils its social and economic potential."

Another cross-cutting facet of openness is multilingualism. If the Internet cannot accommodate a language, people who can communicate only in that language will not be able to enjoy the social and economic benefits that people who speak other languages have. Furthermore, the online contributions that could have been made by people who are linguistically blocked will be unavailable to everyone.

One of the most important characteristics of openness is inclusive governance. This means that decisions about shared principles, norms, rules, procedures and programs that shape the ways in which the Internet is used and evolves are made not just by one group, but by governments, the private sector, the technical community and civil society working collaboratively.

Finally, Internet openness involves distributed control. The Internet is not centrally managed. It depends on the voluntary participation and collaboration of many people and organizations to oversee its independent components and make the Internet work. While the various participants need to follow the Internet's widely adopted technical protocols and standards, the distributed control arrangement allows them to organize and operate their particular parts of the Internet largely in the manner of their choosing.

From a practical standpoint, openness corresponds with the individual's ability to use the Internet to do more things online, whether it is starting an e-business, expressing opinions, sharing knowledge and ideas, or using a map on a mobile device. Certain factors such as personal privacy, the security of commercial data, national security and fundamental values must be given due regard in determining the degree of openness that a society wishes to have. It is not the purpose of this paper, however, to reach conclusions about how much openness or closedness there should be.

CONCLUSION

This paper has proposed a broad definition of Internet openness. It is well known that certain technical elements of the Internet's architecture, such as publicly available and commonly adopted data transport protocols, have had profound effects on economies and societies by virtue of their contribution to openness. By including economic, social and other elements in the definition, this paper recognizes that Internet openness also depends on an array of non-technical factors such as affordable access, privacy rights and transparent regulations. If the implications of this definition of Internet openness can be distilled into one phrase, it is that Internet openness leads to the global free flow of data across the network.

With a working definition of Internet openness in hand, it is possible to take additional steps toward better understanding how — and how much — changes in openness are affecting economic and social outcomes. The OECD is now taking those steps with the aim of helping policy makers to take evidence-based approaches to decisions about Internet openness.

Acknowledgement

The author wishes to thank Geoff Huston, a consultant to the OECD, whose work (which can be found at www.potaroo.net/ispcol/2015-10/open.pdf) provided a basis for the more technical aspects of this paper.

WORKS CITED

Blumenthal, M. and D. Clark. 2001. "Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World." *ACM Transactions on Internet Technology* 1 (1): 70–109.

Box, Sarah. 2016. *Internet Openness and Fragmentation: Toward Measuring the Economic Effects*. Global Commission on Internet Governance Paper Series No. 36. Waterloo, ON: CIGI.

Dalberg. 2014. *Open for Business? The Economic Impact of Internet Openness*. Dalberg Global Development Advisors, March. www.dalberg.com/documents/Open_for_Business_Dalberg.pdf.

OECD. 2008. *The Seoul Declaration for the Future of the Internet Economy*. Paris, France: OECD Publishing. www.oecd.org/sti/40839436.pdf.

———. 2013. *The OECD Privacy Framework*. Paris, France: OECD Publishing. www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

———. 2014. *Principles for Internet Policy Making*. Paris, France: OECD Publishing. www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf.

———. 2015. *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*. Paris, France: OECD Publishing. http://dx.doi.org/10.1787/9789264245471-en.

Saltzer, J., D. Reed and D. Clark. 1981. "End-to-End Arguments in System Design." In *Proceedings of the Second International Conference on Distributed Computing Systems* [Paris, April 8–10]. Washington, DC: IEEE Computer Society.

The Economist. 2010. "The Web's New Walls: How the threats to the internet's openness can be averted." *The Economist*, September 2. www.economist.com/node/16943579.

UN. 1948. General Assembly resolution 217 A, *Universal Declaration of Human Rights*, A/RES/217 (111) (December 10). www.un.org/en/universal-declaration-human-rights/.

———. 2012. General Assembly resolution 20.8, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/20.8 (July 16). http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement.

CIGI PUBLICATIONS
ADVANCING POLICY IDEAS AND DEBATE

Global Commission on Internet Governance

The Global Commission on Internet Governance (GCIG) 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 and Chatham House, the GCIG 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.

GLOBAL COMMISSION ON INTERNET GOVERNANCE PAPER SERIES

The Regime Complex for Managing Global Cyber Activities
GCIG Paper Series No. 1
Joseph S. Nye, Jr.

Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate
GCIG Paper Series No. 2
Tim Maurer and Robert Morgus

Legal Mechanisms for Governing the Transition of Key Domain Name Functions to the Global Multi-stakeholder Community
GCIG Paper Series No. 3
Aaron Shull, Paul Twomey and Christopher S. Yoo

Legal Interoperability as a Tool for Combatting Fragmentation
GCIG Paper Series No. 4
Rolf H. Weber

Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem
GCIG Paper Series No. 5
Stefaan G. Verhulst, Beth S. Noveck, Jillian Raines and Antony Declercq

The Impact of the Dark Web on Internet Governance and Cyber Security
GCIG Paper Series No. 6
Tobby Simon and Michael Chertoff

On the Nature of the Internet
GCIG Paper Series No. 7
Leslie Daigle

Understanding Digital Intelligence and the Norms That Might Govern It
GCIG Paper Series No. 8
David Omand

ICANN: Bridging the Trust Gap
GCIG Paper Series No. 9
Emily Taylor

A Primer on Globally Harmonizing Internet Jurisdiction and Regulations
GCIG Paper Series No. 10
Michael Chertoff and Paul Rosenzweig

Connected Choices: How the Internet is Challenging Sovereign Decisions
GCIG Paper Series No. 11
Melissa E. Hathaway

Solving the International Internet Policy Coordination Problem
GCIG Paper Series No. 12
Nick Ashton-Hart

Net Neutrality: Reflections on the Current Debate
GCIG Paper Series No. 13
Pablo Bello and Juan Jung

Addressing the Impact of Data Location Regulation in Financial Services
GCIG Paper Series No. 14
James M. Kaplan and Kayvaun Rowshankish

Cyber Security and Cyber Resilience in East Africa
GCIG Paper Series No. 15
Iginio Gagliardone and Nanjira Sambuli

Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime
GCIG Paper Series No. 16
Eric Jardine

CIGI PUBLICATIONS
ADVANCING POLICY IDEAS AND DEBATE

The Emergence of Contention in Global Internet Governance
GCIG Paper Series No. 17
Samantha Bradshaw, Laura DeNardis, Fen Osler Hampson, Eric Jardine and Mark Raymond

Landmark EU and US Net Neutrality Decisions: How Might Pending Decisions Impact Internet Fragmentation?
GCIG Paper Series No. 18
Ben Scott, Stefan Heumann and Jan-Peter Kleinhans

The Strengths and Weaknesses of the Brazilian Internet Bill of Rights: Examining a Human Rights Framework for the Internet
GCIG Paper Series No. 19
Carolina Rossini, Francisco Brito Cruz and Danilo Doneda

The Tor Dark Net
GCIG Paper Series No. 20
Gareth Owen and Nick Savage

The Dark Web Dilemma: Tor, Anonymity and Online Policing
GCIG Paper Series No. 21
Eric Jardine

One in Three: Internet Governance and Children's Rights
GCIG Paper Series No. 22
Sonia Livingstone, John Carr and Jasmina Byrne

Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity
GCIG Paper Series No. 23
Samantha Bradshaw

The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality
GCIG Paper Series No. 24
Emily Taylor

The Digital Trade Imbalance and Its Implications for Internet Governance
GCIG Paper Series No. 25
Susan Ariel Aaronson

A Pragmatic Approach to the Right to be Forgotten
GCIG Paper Series No. 26
Wendy Hall, Kieron O'Hara and Nigel Shadbolt

Education 3.0 and Internet Governance: A New Global Alliance for Children and Young People's Sustainable Digital Development
GCIG Paper Series No. 27
Divina Frau-Meigs and Lee Hibbard

Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation
GCIG Paper Series No. 28
Bertrand de La Chapelle and Paul Fehlinger

Patents and Internet Standards
GCIG Paper Series No. 29
Jorge L. Contreras

Tracing the Economic Impact of Regulations on the Free Flow of Data Localization
GCIG Paper Series No. 30
Matthias Bauer, Martina F. Ferracane and Erik van der Marel

Looking Back on the First Round of New gTLD Applications: Implications for the Future of Domain Name Regulation
GCIG Paper Series No. 31
Jacqueline D. Lipton

Governance of International Trade and the Internet: Existing and Evolving Regulatory Systems
GCIG Paper Series No. 32
Harsha Vardhana Singh, Ahmed Abdel-Latif and L. Lee Tuthill

Market-driven Challenges to Open Internet Standards
GCIG Paper Series No. 33
Patrik Fälström

How to Connect the Other Half: Evidence and Policy Insights from Household Surveys in Latin America
GCIG Paper Series No. 34
Hernan Galperin

Available for free download at www.cigionline.org/publications

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 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

Managing Editor, Publications	Carol Bonnett
Senior Publications Editor	Jennifer Goyder
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Publications Editor	Kristen Scott Ndiaye
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