Finding Common Ground

Challenges and Opportunities in Internet Governance and Internet-related Policy

A Briefing Book Prepared for
the Global Commission on Internet Governance

Finding Common Ground

Finding Common Ground

Challenges and Opportunities in Internet Governance and Internet-related Policy

A Briefing Book Prepared for the Global Commission on Internet Governance

Acknowledgement

The Centre for International Governance Innovation is grateful to CIGI Research Associate Samantha Bradshaw under the supervision of Mark Raymond and CIGI Senior Fellow, Professor Laura DeNardis, for her contributions to this briefing book.

CIGI

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

Table of Contents

Acronyms and Abbreviations

ACTA	Anti-Counterfeiting Trade Agreement
BRICS	Brazil, Russia, India, China and South Africa
ccTLD	country code top-level domain
CERT	Computer Emergency Response Team
CERT/CC	CERT Coordination Centre
CIRs	Critical Internet Resources
CMU	Carnegie Mellon University
CNI	Critical National Infrastructure
CRS	Computer Reservation Systems
CSTD	Commission on Science and Technology for Development (UN)
DNS	Domain Name System
DOC	Department of Commerce (US)
ECOSOC	Economic and Social Council (UN)
EFF	Electronic Frontier Foundation
ETNO	European Telecommunications Network Operators' Association
FDI	foreign direct investment
FOSS	Free and open-source software
FTC	Federal Trade Commission
GGE	Group of Governmental Experts
gTLD	general top-level domain
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IAB	Internet Architecture Board
ICT	Internet and communications technology
ICRC	International Committee of the Red Cross
IDNs	Internationalized Domain Names
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IP	Internet protocol
IPR	intellectual property rights
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6
ISOC	Internet Society
ISP	Internet service provider
ITRs	International Telecommunication Regulations
IXP	Internet Exchange Point
MNE	multinational enterprise
NATO	North American Treaty Organization
NPS	networked public sphere
NTIA	National Telecommunications and Information Administration
OCHA	Office for the Coordination of Humanitarian Affairs
OECD	Organisation for Economic Co-operation and Development
OHCHR	Office of the High Commissioner for Human Rights
PIPA	PROTECT IP Act
PPPs	public-private partnerships
RIRs	regional Internet registries
SOPA	Stop Online Piracy Act
TLDs	top-level domains
ToS	Terms of Service
TPP	Trans-Pacific Partnership
TTIP	Transatlantic Trade and Investment Partnership
UDHR	Universal Declaration of Human Rights
UDRP	Uniform Domain-Name Dispute Resolution Policy
UNCTAD	UN Conference on Trade and Development
UNDP	UN Development Programme
UNESCO	UN Educational, Scientific and Cultural Organization
UNGA	UN General Assembly
UNHRC	UN Human Rights Council
UNODC	UN Office on Drugs and Crime
VoIP	voice over Internet protocol
W3C	World Wide Web Consortium
WCIT	World Conference on International Telecommunications
WGEC	Working Group on Enhanced Cooperation
WTO	World Trade Organization

Speech by Former Foreign Minister Carl Bildt at the Seoul Conference on Cyberspace, 2013

Excellencies,
Ladies and Gentlemen,

It's truly a pleasure to come here to Seoul. Coming from the land of Ericsson — one of the global leaders in mobile networks — to the land of Samsung — one of the leaders in mobile devices. Our two countries are, in this world of connectivity, close neighbours and partners.

I was among the many people who attended the first cyber conference in London two years ago. It was a long time ago. Hundreds and hundreds of millions of people around the world have plugged into the internet since then. Mobile technologies have become much more abundant and even more capable. And we all know that we are only at the beginning of a truly revolutionary development.

Today, approximately 3 billion people are connected to the Internet. In some years, it is expected that there will be approximately 5 billion. But even more impressive is the explosion in mobile internet. Here, we see developing nations leapfrogging generations in the "developed world."

Africa is developing faster than any other continent. New technologies are creating vast new opportunities. In just five short years it is estimated that 60 percent of the world will be covered with LTE 4G networks with a capacity greater than what we have in most of Europe today.

There is still a digital divide. In some respects it might even be getting wider. Because increasingly it will become a divide less in terms of geography than of generations. A decade from now the vast majority of the teenagers of Indonesia, Sweden, Nigeria or Brazil will all be connected by their smart devices to a global mobile network far more capable than anything available to any of us today. The significance of this is crucial.

The World Bank estimates that an increase in broadband connectivity coverage by 10 per cent increases economic growth by 1 percent. If this is the case, then these technologies — in combination with open societies and open economies — represent the most powerful tool for economic development in modern times. We see it. Day by day. Across the world.

My own country — Sweden — is one of the leaders. It is said that the internet economy has contributed 8 per cent to our GDP. Perhaps. But I know for certain that there is today hardly any sector of our economy that moves forward without the internet.

We are becoming net-based economies. Net-based societies. And entering an even more net-based future. But since London two years ago — or even since the conference in Budapest last year — new challenges have also emerged.

Freedom on and off the net is even more under attack. Regimes afraid of change. Regimes afraid of the free flow of information and ideas. Trying to build their great walls to protect their great powers. The recent report from Freedom House on the issue was blunt: "Internet Freedom Deteriorates Worldwide, but Activists Push Back."

Last year we managed — as a broad coalition of countries — to get the UN Human Rights Council [UNHRC] to adopt the landmark resolution 20/8. Basically, it states that the protection of the freedom of speech and the freedom of information that the UN Universal Declaration of Human Rights [UDHR] seeks to protect in the offline world should apply equally in the online world. That is truly important. For all.

There are some limitations in most of our societies. Even in my own. Our cultures and traditions do differ. But limitations must always be based on the law, decided according to the law and subject to challenge under the law. That's fundamental. On this, we should never compromise.

Since London, as the dependence of our societies and economies on the net has grown, and our vulnerabilities accordingly, we have become more aware of all the issues of Internet security. Indeed, the security of the flows of information across the

world has probably become even more important to our societies and economies than the security of the air transport system or the flows of trade across our oceans.

The net is a mirror of our societies and of our world. Pirates are there. Terrorists are there. Criminals are there. Spies are there. And there are state sponsors of some or all of these activities all the time. We have a common duty to fight these evils, but to do it without endangering the values of freedom and an open world that are so central to us. Security and freedom. Freedom and security.

The two should go hand in hand. In our nations. In our world. Offline. And online.

Recently we have also found ourselves in a new debate about surveillance and privacy. Not a new debate for many of us. But certainly a debate with new dimensions. In my own country we have laws, extensively debated by our Parliament, on these issues. On access to "metadata" in our networks for law enforcement needs. On the foreign intelligence operations deemed important to our security. And I believe that these laws are in accordance with the highest standards.

In other countries it is different. Some countries operate vast surveillance systems without any laws of oversight whatsoever. Some are now having intense debates about these issues. And aggressive intelligence operations on the net are certainly not a rare occurrence. As a matter of fact, we see them every day, every hour, every minute, every second. I think we all do.

To these issues should be added the fact that nations seem to be preparing for what they call offensive operations on the net. Cyberwar is discussed as a new possible category of warfare. Taking all this together, I do believe that what we have seen during these few years makes it imperative to have a global dialogue on the global norms of behaviour on the net. And this global dialogue must also touch upon the basic issues of the governance of the net.

The present multi-stakeholder approach has undoubtedly served our world extremely well. It brings together technology innovators, government regulators, business representatives and civil society actors in a web of governance that has proved to be effective, dynamic and responsive. It's difficult to see that the rapid development of the internet that we have seen would have been possible had there been, for example, an exclusively state-centred governance structure. Thus, there is much that we should seek to preserve.But we cannot ignore that the legitimacy of this web of governance of the net is being challenged. A broad debate, also on this, is thus necessary. There are, of course, many rules and norms of importance of relevance for the net.

The [UDHR]. The UN Charter with its principles. The laws governing warfare. The principles of privacy. To name just some of obvious importance. These should not be changed. But their concrete application to our new world of hyperconnectivity needs to be clarified. And we should discuss the ways in which this can be done.

These days the debate concerns the rules governing the right of states to conduct surveillance, primarily for reasons of security. Also here, I do believe that a discussion on the rules of behaviour would be most useful. To this objective, let me propose seven principles I believe should be observed.

First, legality. Surveillance needs to be based on laws. These laws must be adopted in a transparent manner through a democratic process. The implementation of these laws should be reviewed periodically to ensure that the expansion of surveillance capabilities due to, for instance, technological advances is properly debated.

Second, legitimate aim. Surveillance must be conducted on the basis of a legitimate and well-defined aim. Surveillance measures may never be carried out in a discriminatory or discretionary manner and only by specified state authorities.

Third, necessity and adequacy. The law should justify that surveillance is necessary and adequate to achieve the legitimate aim.

Fourth, proportionality. A sound proportionality judgment must be made, to carefully assess whether the benefits of surveillance outweigh its negative consequences.

Fifth, judicial authority. Decisions on the use of communications surveillance should be taken by a competent authority. As a general rule, an independent court should take such decisions.

Sixth, transparency. States should be as transparent as possible about how they carry out surveillance. They should provide information on how the surveillance legislation works in practice.

Seventh, public oversight of parliamentary or other credible institutions. We need to scrutinise how the laws work, to create transparency and build trust and legitimacy. Our obligation as governments is to provide security and to respect human rights — not either/or.

In trying to define principles such as the ones above, we want to continue to engage with civil society in a debate about reasonable limitations to state power, in line with our obligations. We now look forward to a deeper conversation with other governments, businesses and civil society on these issues. Our ultimate goal is a system that provides increased security, enjoys legitimacy and trust among people, and safeguards the freedom and rights of the individual.

And while we refine our own systems, we will continue the fight against the authoritarian regimes and forces that put bloggers in prison, censor social media as a tool for change, and shut down the internet when it suits them. In London two years ago, I said that the internet is the new frontline in the fight for freedom in the world. That is even more the case today. And it will be even more so in the coming years as our entire world, and our entire lives, go online.

Thank you.

Carl Bildt,
2013 Seoul Conference on Cyberspace

Section 1:
Managing Systemic Risk

1.1 Prospects for Establishing Norms Regarding State Conduct

Background

According to Nye (2014), it is unlikely that there will be "a single overarching regime for cyberspace anytime soon" and different sub-issues in the cyber regime are likely to develop norms at different rates. Unlike in the physical domain, the norms and rules that govern offensive state action in cyberspace are fairly incipient and still evolving. Two major initiatives have begun to set precedents for how international legal rules and norms will apply to cyberspace: the UN Group of Governmental Experts' (GGE's) report, which points to international consensus on the validity of applying existing international rules to cyberspace, and the Tallinn Manual, which expands on this idea and discusses how we can start thinking about applying existing laws to cyberspace challenges.

UN GGE

In July 2013, the GGE concluded that the law of armed conflict applies to cyberspace, and therefore that interaction between states in this domain should also be conducted within the framework of customary international law. The GGE was made up of experts from 15 countries, including China, Germany, Russia, the United Kingdom and the United States.

Tallinn Manual

The *Tallinn Manual on the International Law Applicable to Cyber Warfare* resulted from a three-year effort by international law and cyber security experts to create a legal framework applicable to cyberwar. The experts were brought together under the North Atlantic Treaty Organization's (NATO's) Cooperative Cyber Defence Centre of Excellence, based in Tallinn, Estonia. The manual considers how established international legal principles can be extended to cyberwarfare, in the same way that international law was extended after the invention of nuclear weapons. Particularly, the Tallinn Manual is concerned with *jus ad bellum* (the set of rules to be consulted before engaging in war) and *jus in bello* (the law of armed conflict or international humanitarian law) (Azzopardi 2013). Despite its nonbinding status, the manual is an important attempt to "delineate the threshold dividing cyber war from cybercrime and formalize international rules of engagement in cyber space" (Fleck 2013).

Contemporary Issues

Next Steps

Most efforts to establish norms regarding state conduct in cyberspace have pointed toward applying existing international legal frameworks to cyberwarfare, as were done in the nuclear era. However, there may be dangers in overextending this analogy (see Nye 2011). Are existing international laws enough, or do we need new laws to govern warfare in cyberspace, or at least some aspects of it? The rules that govern cyberwar are still being worked out: NATO's Cooperative Cyber Defence Centre of Excellence has undergone a second project, "Tallinn 2.0," to expand the scope of the Tallinn Manual, and the GGE conclusion on cyber attacks represents only a start for developing these norms. Going forward, policy makers need to decide the best route of action, and what exceptions and additions will have to be made (if any) to account for cyberwarfare.

Works Cited

Azzopardi, M. 2013. "The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Brief Introduction on Its treatment of Jus Ad Bellum Norms." *Elsa Malta Law Review* 3 (1): 174–84. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2335034.

Fleck, D. 2013. "Searching for International Rules Applicable to Cyber Warfare — A Critical First Assessment of the New Tallinn Manual." *Journal of Conflict and Security Law* 18 (2): 331–51.

Nye, J. 2011. "Nuclear Lessons for Cyber Security." *Strategic Studies Quarterly* 5 (4): 18–38.

———. 2014. *The Regime Complex for Managing Global Cyber Activities.* CIGI GCIG Papers No. 1. www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

Suggested Readings

Boyle, A. S. 2012. "Moving Towards Tallinn: Drafting the shape of Cyber Warfare." American Security Project. http://americansecurityproject.org/featured-items/2012/fact-sheet-moving-towards-tallinn-drafting-the-shape-of-cyber-warfare/.

UN General Assembly (UNGA). 2013. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." www.mofa.go.jp/files/000016407.pdf.

1.2 International Cyber Security Cooperation and Computer Emergency Response Teams

Background

With the increasing sophistication of cyber attacks and the global interconnection and interdependency of computer networks, international cyber security cooperation is needed to prevent and respond to cyber security emergencies (Madnick, Li and Choucri 2009). Computer Emergency Response Teams (CERTs) provide an important potential mechanism to facilitate and institutionalize such cooperation. The CERT program is "chartered to work with the Internet community in detecting and resolving computer security incidents, as well as taking steps to prevent future incidents" by: providing a single point of contact for emergencies; facilitating communication among experts who are working to solve security problems; serving as a central point for identifying and correcting computer system vulnerabilities; maintaining research ties to improve security; and initiating proactive measures to increase awareness and understanding of computer security to a variety of stakeholders (CERT 2011).

The first CERT was launched in 1988 at Carnegie Mellon University (CMU) in response to the Morris Worm — a computer virus that took down an estimated 10 percent of the Internet at the time (Madnick, Li and Choucri 2009). The CERT at CMU is now called the CERT Coordination Centre (CERT/CC), and it develops standards, best practices and policies for other CERTs (ibid.). CERT/CC has helped other countries develop their own CERTs, and has played a significant role in the creation of the US-CERT. At present, there are over 200 recognized CERTs, with different levels of organization, funding and expertise (Choucri, Madnick and Ferwerda 2013). In addition to CERT/CC, many CERT organizations also interact with other coordination networks, such as the Form of Incident Response and Security Teams, which was established to enhance information sharing between security groups (ibid.).

Contemporary Issues

Improving CERT Coordination and Leveraging CERTs

In general, CERTs share a common structure based on the standards and best practices set out by CERT/CC. However, individual CERTs differ in their areas of focus (academic, private, national, regional), expertise (phishing, viruses, information security) and ability to effectively perform their mandates, due to varying levels of funding and or technical expertise (ibid.). This loose network reduces the accountability for each CERT to individually perform, which may lead to insufficient coordination and information sharing among CERTs (ibid.). Furthermore, in most countries, national CERTs and CERT institutions do not exist, or are in their infancy (Raymond, Shull and Bradshaw, forthcoming). Going forward, policy makers can consider exploring options to improve coordination and information sharing among CERTs, and can consider leveraging their skills and expertise for a variety of cyber security issues. Policy makers can also explore the possibility of professionalizing various CERTs to improve international cyber security cooperation.

Works Cited

CERT. 2011. "About Us." www.cert.org/meet_cert/.

Choucri, N., S. Madnick and J. Ferwerda. 2013. "Institutions for Cyber Security: International Response and Global Imperatives." In *Information Technology for Development*.http://ecir.mit.edu/images/stories/website%20photos/ECIR%20website%20staff%20pics/ECIR%20website%20staff%20pics/choucri%20madnick%20ferwerda_institutions%20for%20cyber%20security_published.pdf.

Madnick, S., A. Li and N. Choucri. 2009. "Experiences and Challenges with using CERT Data to Analyze." Massachusetts Institute of Technology Engineering Systems Division Working Paper Series. papers.ssrn.com/sol3/papers.cfm?abstract_id=1478206.

Raymond, Mark, Aaron Shull and Samantha Bradshaw. Forthcoming. "Rule-Making for State Conduct in the Attribution of Cyber-Attacks." In *Constructive Powers and Regional Security in East Asia.* www.academia.edu/9027635/Rule-Making_for_State_Conduct_in_the_Attribution_of_Cyber-Attacks.

1.3 Infrastructure Protection and Risk Management

Background

Critical National Infrastructure (CNI) is infrastructure that provides essential services, including water, banking, gas and communications (Cornish et al. 2011). In early 2008, a main Internet cable in the Mediterranean near Egypt was damaged, endangering access to the Internet across the Middle East. In 2007, similar incidents took place in Taiwan and Pakistan (Kurbalija 2012). Such outages have the potential to cause widespread disruption of daily life in wired societies and bolster the case for treating physical Internet infrastructure as part of CNI. As more CNI is connected to and dependent upon the Internet, the costs of such disruptions increase. CNI providers and operators may experience a wide variety of cyber attacks, ranging from malware to sophisticated surveillance techniques that attempt to steal insider information and trade secrets. According to a survey of various CNI organizations, these threats are proliferating. For example, one security software provider reported "a tenfold increase in malware attacks, rising from 6000 detections per day…in 2008 to 60,000 per day in 2009" (Cornish et al. 2011).

Contemporary Issues

A cyber attack on CNI is a black swan problem: the probability of an attack on CNI is low, however, if an attack were to occur its impact would be large. CNI organizations will manage cyber security in differing ways according to their vulnerabilities and resources. According to Cornish et al. (2011), "Although one might expect public and private organizations, particularly larger ones, to have a clear sense of best practices, continuity planning and risk management, this is not always the case." As a result there are a number of "inconsistencies, gaps and omissions (through ignorance or negligence)" in the way that organizations manage cyber security measures (ibid.). Going forward, policy makers will need to ask how organizations can better coordinate risk management and best practices to mitigate vulnerabilities in CNI.

Works Cited

Cornish, P., D. Livingstone, D. Clemente and C. Yorke. 2011. *Cyber Security and the UK's Critical National Infrastructure*. Chatham House Report.

Kurbalija, J. 2012. *An Introduction to Internet Governance*. Malta: DiploFoundation. www.diplomacy.edu/IGBook.

1.4 Problems of Attribution, Monitoring and Verification

Background

Attributing actions on the Internet is extremely difficult as identities can be easily concealed. Technical and non-technical measures can be used to identify the source of an attack. However, looking at the source alone is problematic, not only because Internet communications will pass through multiple routers in different states, but also because attackers often intentionally use proxies to mask their identities. Furthermore, relatively few governments have the technical expertise necessary to determine where cyber attacks originate. Most of this expertise is in the hands of private companies, and including private firms in the attribution of cyber attacks can be controversial because "it is not clear whether or not states will accept the findings of these companies, especially when the company is headquartered in the same state making the public attribution of the attack" (Raymond, Shull and Bradshaw, forthcoming).

When technical measures can identify the source of an attack, that fact alone does not indicate who, or which country, is responsible. For example, in 2009, when the Information Warfare Monitor uncovered "GhostNet" — an attack that emanated from computers in China and infiltrated government and commercial computer systems in over 100 countries — it could not be determined whether the plot was controlled by the Chinese government, by private "patriot hackers" acting in the Chinese interest but without government involvement, or by a criminal network in China. The possibility that another state used agents to launch the operation in China to mislead observers to the true operators of the GhostNet system could not be ruled out either (Goldsmith 2010).

Assuming that state-sponsored cyber attacks constitute internationally wrongful acts, and assuming technical measures can provide sufficient evidence that a certain actor is responsible for an attack, international laws that govern state responsibility can be applied to determine whether or not a certain state should be held responsible for a cyber attack (Raymond and Shull 2013). However, these laws are fragmented and do not clearly define what activities are attributable to a state.

Contemporary Issues

Getting Attribution Right

There are a number or risks associated with false attributions. Particularly, when accusations are made hastily, without convincing technical data or according to proper legal procedure, diplomatic relations can be damaged. Furthermore, such situations are prone to escalation: because cyber domain is offence-dominant, there may be a perceived necessity to respond with hasty attributions and tit-for-tat reprisals (ibid.).

However, over-attribution is only half the problem if policy makers want to deter bad conduct in cyberspace; there is also significant danger in widespread failure to attribute cyber attacks when technical and legal criteria have been satisfied (ibid.). If cyber attacks are not criticized and no efforts are made to hold bad actors accountable, we may see a cycle in which anonymity impedes the attribution of a cyber attack, while the lack of attribution means the bad actor will likely evade justice. This, in turn, decreases the level of cyber deterrence and increases the chance of developing permissive international norms.

Going forward, policy makers need to ask themselves what rules will govern when and how states publicly attribute cyber attacks. Currently, the international laws of state responsibility are fragmented. How should new norms and laws be framed to address issues of state responsibility and attribution of cyber attacks? Furthermore, policy makers need to ask themselves how they can find a middle ground that mitigates the risks associated with both widespread non-attributions with hasty attribution. With the risks associated with misattribution and the consequences that flow from it, what rules, norms and structures are needed to break escalatory spirals, even where attribution is properly made (ibid.)?

Works Cited

Goldsmith, J. 2010. "The New Vulnerability." New Republic, June 7. www.newrepublic.com/article/books-and-arts/75262/the-new-vulnerability.

Raymond, Mark, Aaron Shull and Samantha Bradshaw. Forthcoming. "Rule-Making for State Conduct in the Attribution of Cyber-Attacks." In *Constructive Powers and Regional Security in East Asia.* www.academia.edu/9027635/Rule-Making_for_State_Conduct_in_the_Attribution_of_Cyber-Attacks.

1.5 Proliferation and Disarmament Issues

Background

As a result of the proliferation of cyber incidents and recent media attention, cyber security issues have been at the top of the agenda for governments around the world. US President Barack Obama's recent *Cyberspace Policy Review* declared that "cyber security risks pose some of the most serious economic and national security challenge of the 21st century" (Government of the United States 2009). Governments have been updating their legislation on cyber security and international conferences have been highlighting the strategic-military aspects of cyber security.

In the current state of technology, the cyber domain is largely offence-dominant (Nye 2013). This is because attack tools are fairly cheap and widely available: websites in China and Ukraine sell daily, weekly, monthly or even lifetime rentals of botnets with 24/7 technical support (Diebert and Rohozinski 2011). Furthermore, attackers can mount their assaults with "lightning speed from anywhere on the planet to anywhere else, disguising their origins and masking responsibility" (Deibert 2013).

As a result, the world is also seeing what cyber security scholars refer to as the "rise of a new cyber military industrial complex," as major defense corporations, such as Boeing and Northrop Grumman, are now repositioning themselves to service the cyber security market (Deibert and Rohozinski 2011). Furthermore, new products and services, such as Deep Packet Inspection or Big Data Analytics, developed mainly by western firms, are finding their way into regimes with

questionable human rights records. These tools are being used to limit freedom of speech, access to information and to infiltrate the computers of dissidents and activists (Deibert 2013).

Contemporary Issues

Offence-Dominant Domain

In an offence-dominant environment, the pressure is "to keep up or be left behind" (Diebert and Rohozinski 2011). However, like all arms races before it, the growing tensions in cyberspace and "the proliferation of tools and services that feed it create a climate of fear and insecurity where threats lurk behind every corner and rash decisions can lead to unexpected outcomes and chaos" (Deibert 2013). While most countries publicly declare that they have no wish to be caught up in a digital arms race, the threat of a sudden devastating attack may create significant pressures, especially when combined with major firms looking to exploit a lucrative new market.

Works Cited

Diebert, R. 2013. "Canada and the Challenges of Cyberspace Governance and Security." *SPP Communique* 5 (3).

Diebert, R. and R. Rohozinski. 2011. "The New Cyber Military-Industrial Complex." *The Globe and Mail*, March 28. www.theglobeandmail.com/globe-debate/the-new-cyber-military-industrial-complex/article573990/.

Government of the United States. 2009. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

Nye, J. 2011. "Nuclear Lessons for Cyber Security." *Strategic Studies Quarterly* 5 (4): 18–38.

Suggested Readings

Dunn Cavelty, M. 2012. "The Militarization of Cyberspace: Why Less May Be Better." Paper presented at the 4th International Conference on Cyber Conflict. www.ccdcoe.org/publications/2012proceedings/2_6_Dunn%20Cavelty_TheMilitarisationOfCyberspace.pdf.

1.6 Cybercrime

Background

Though it is difficult to quantify how much cybercrime is occurring, a recent analysis by the Center for Strategic and International Studies (2014) estimates that cybercrime costs the global economy more than USD $400 billion. Individual cybercrime victimization is significantly higher than conventional forms of crime. For example, "victimization rates for online credit card fraud, identity theft, responding to a phishing attempt and experiencing unauthorized access to an email account, vary between 1 and 17 percent of the online population from 21 countries around the world, compared with typical burglary, robbery and car theft rates of under 5 percent for those same countries" (UN Office on Drugs and Crime [UNODC] 2013). Private actors report similar victimization rates. For example, victimization rates for data breaches due to intrusion or phishing are between two and 16 percent (ibid.).

Laws play a key role in the prevention and prosecution of cybercrime; at the national level, cybercrime laws often concern criminalization. However, countries are increasingly recognizing a need to expand their legislation into other areas, such as investigative measures, jurisdiction, electronic evidence and international coordination (ibid.). International legal coordination measures are important when it comes to investigating and prosecuting cybercrime because of its transnational nature. Often, the perpetrator and victim are located in different countries, posing difficulties for law enforcement agencies in investigating and prosecuting cybercrimes (Schreier, Weeks and Winkler 2014). Without cooperation, issues of state sovereignty can impede criminal investigation and prosecution. In many countries, the principle of "dual criminality," which requires that the offence in question be punishable in both jurisdictions, must be in place for legal cooperation (ibid.). If countries have different or diverging laws, effective deterrence, enforcement and prosecution by law enforcement agencies can be undermined. Furthermore, "the speed at which cyber criminals can inflict harm and move on to evade detection also puts enforcement agencies under heavy time pressures, making effective international cooperation even more vital" (ibid.). Despite the need for international cooperation on cybercrime, no global multilateral treaty exists to deal with these issues.

The Council of Europe's Convention on Cybercrime is the only major multilateral convention that addresses cybercrime coordination issues. The Convention on Cybercrime lists a number of crimes that signatories are required to codify in their domestic law. These crimes include hacking, child pornography offences and offences related to intellectual property violations. The convention also sets out a number of procedural mechanisms that signatories must establish domestically, such as granting law enforcement authorities the power to compel Internet service providers (ISPs) to monitor a person's online activities.

The convention calls upon signatories to cooperate to the widest extent possible in investigation and prosecution of cybercrime offences. Four non-European states (Canada, Japan, the United States and South Africa) participated in the negotiations of the treaty and signed it. The United States has also ratified the convention. The convention is considered more than a regional convention because countries that did not participate in its drafting are still able to sign it, but it is not considered a global convention because only one non-member has ratified it.

Contemporary Issues

Addressing Fragmentation

There is international legal fragmentation when it comes to addressing cybercrime, and there are divergent views regarding the appropriate procedural mechanisms to develop global standards for investigating, enforcing and prosecuting crimes online (see The Register 2010). The Convention on Cybercrime could be a starting place for global cooperation. However, critics have argued that making the convention global would be difficult because it was drafted by mainly Western democracies. Another option would be to draft a new convention on cybercrime cooperation with more participation from the developing world. There is no clear consensus on the best path forward.

Defining the Scope of Cybercrime

Not all acts of cybercrime are committed for the same purpose. A great deal is intended to fund the activities of pre-existing organized criminal enterprises, while another subset involves the exploitation of children or other vulnerable individuals. However, some cybercrime involves elements of protest and political dissent or even simple mischief. Policy makers may wish to consider whether it is prudent or appropriate to make distinctions between criminal acts involving the use of information and communications technology (ICT) on the basis of their purpose, at least for sentencing purposes. Such measures might be useful in minimizing the social costs associated with the prosecution and incarceration of offenders accused of more minor offences.

Works Cited

Center for Strategic and International Studies. 2014. *Net Losses: Estimating the Global Cost of Cybercrime: Economic Impact of Cybercrime II.* www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf.

Schreier, F., B.Weeks and T. H. Winkler. 2014. "Cyber Security: The Road Ahead." DCAF: Centre for Security, Development and the Rule of Law Working Paper Series No. 4. www.dcaf.ch/content/download/35863/526943/file/Cyber2.pdf.

The Register. 2010. "UN Split on Cybercrime Conventions: Follow Euro Model or go for Something New?" www.theregister.co.uk/2010/04/19/un_cybercrime_conventions/.

UNODC. 2013. "Comprehensive Study on Cybercrime." www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

Suggested Readings

Council of Europe. 2001. "Convention on Cybercrime." http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

1.7 Surveillance

Background

In the wake of recent disclosures about cyber espionage, the discussion surrounding online surveillance continues to capture global headlines. New technological developments over the past decade allow governments and other organizations to collect, store and analyze information relatively cheaply and efficiently. With the integration of the Internet into our daily lives, this technology can assemble a picture of an individual's entire personal and professional life with a few computer commands.

Intelligence gathering is an established government function, but like many things, online

surveillance has created a grey area in the rules of the game. The United States has claimed that it uses online surveillance methods to protect its citizens against terrorism, improving state security. US Secretary of State John Kerry stated that no "innocent people" were being abused and that surveillance by several countries had prevented many terrorist plots (*The Guardian* 2013). Whether or not these statements are true, the online factor has complicated our traditional notions and methods of surveillance and understanding of what constitutes acceptable levels of surveillance in the international realm.

In response, Brazil and Germany have spearheaded efforts at the United Nations to protect the privacy of electronic communications. In the fall of 2013, they drafted a "Resolution on The Right to Privacy in the Digital Age," emphasizing that "unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data" are "highly intrusive acts" that "violate the rights to privacy and freedom of expression and may contradict the tenets of a democratic society" (UNGA 2013a). And in 2014 Brazil hosted the NETmundial meeting to elaborate principles of Internet governance and propose a roadmap for the future development of the ecosystem (NETMundial 2014).

Revelations about US surveillance strategies have also been felt by the private sector, as some leaked documents revealed that the agency had intercepted data transmitted on the cables that link the worldwide data centres belonging to Google and Yahoo (see Gellman and Soltani 2013). In an open letter to the United States, Google and Yahoo, along with several other technology giants, raised their concerns regarding US national law and data transparency (see Reform Government Surveillance 2013). Overall, the revelations have been toxic for the legitimacy of Internet governance and diplomatic processes, as they have shed light on a number of serious privacy and transparency issues.

Contemporary Issues

National Privacy Standards

Privacy laws and standards have poorly adapted to this changing technological environment. In many states, legal standards are "either non-existent or inadequate to deal with the modern communications surveillance environment" (UNGA 2013b). In many states, "vague and broadly conceived legal provisions are being invoked to legitimize and sanction the use of seriously intrusive techniques (ibid.). When information can be tracked back to a particular individual or group of individuals, it can put these people at risk of being exposed to violations of their human rights, including the right to privacy and the right to freedom of expression. For example, restrictions in anonymity in communication can have a chilling effect on victims of all forms of abuse. Without anonymity, victims may become more reluctant to report in fear of double victimization (ibid.). Furthermore, information that identifies individuals who report on acts of violence or human right violations could be used by governments or armed groups for retribution. This was the case when the Egyptian government used mobile call logs to track down dissent in the aftermath of anti-government food protests in 2008 (Ahmed et al. 2009); when the Taliban threatened to target foreign aid workers responding to the floods in Pakistan in 2010 (Office for the Coordination of Humanitarian Affairs [OCHA] 2013); or when the Ukrainian government used mobile and GPS technology to text message protestors: "Dear Subscriber, you are registered as a participant in a mass riot" in 2014 (The Guardian 2014).

Extra-Territorial Application of National Surveillance Laws

With the proliferation of cloud computing technologies and the increased flow of data across borders, a number of states have begun to adopt laws that's authorize them to conduct extra-territorial surveillance or to intercept communications in foreign jurisdictions (UNGA 2013b). South Africa, the Netherlands, Pakistan and the United States are just a few examples (see ibid. for a detailed list). This suggests trends towards the extension of surveillance powers beyond national borders. Policy makers need to ask, what limits, if any, need to be placed on a state's ability to conduct surveillance in foreign jurisdictions.

Transparency Part One: Balancing Secrecy, Security and Privacy

When undergoing surveillance for the purpose of national security, states must strike a fine balance between secrecy, security and privacy. Some degree of secrecy is a requirement of legitimate intelligence operations; however, there need to be robust mechanisms to ensure that such agencies do not act inappropriately. Establishing new laws with no formal mechanisms of oversight will not

guarantee that states will play by the rules. Unlike nuclear tests, Internet surveillance cannot always be reliably detected. Policy makers will need to ask what the appropriate balance between secrecy, privacy and security should look like and what kinds of mechanisms will guarantee states adhere to these standards.

Transparency Part Two: Judicial Oversight

Traditionally, to undergo communication surveillance, states or law enforcement agencies would have to have judicial authorizations. In many cases, this requirement is being weakened or removed (see UNGA 2013b). Frank La Rue, the UN's Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression reports that "progressively, communication surveillance is being authorized on a broad and indiscriminate basis, without the need for law enforcement authorities to establish a factual basis for the surveillance on a case-by-case basis" (ibid.). Furthermore, in many states, network operators are being compelled to modify existing infrastructure to enable surveillance by state agents, eliminating the opportunity for judicial oversight. These types of arrangements take surveillance out of the realm of judicial authorization and allow for unregulated surveillance to occur in secrecy, removing any transparency and accountability on the part of the state (ibid.).

Works Cited

Ahmed, M. H., J. Penney, S. Ikki, A. Salami, T. L. Bath, M. Abad Allah and S. Mansour. 2009. "Threats to Mobile Phone Users' Privacy." www.engr.mun.ca/~mhahmed/privacy/mobile_phone_privacy_report.pdf.

Gellman, B. and A. Soltani. 2013. "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say." *The Washington Post*, October 30. www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

NETMundial. 2014. "NETmundial: The Beginning of a Process." http://netmundial.br/about/.

OCHA. 2013. "Humanitarianism in a Network Age." https://docs.unocha.org/sites/dms/Documents/WEB%20Humanitarianism%20in%20the%20Network%20Age%20vF%20single.pdf.

Reform Government Surveillance. 2013. "Global Government Surveillance Reform." www.reformgovernmentsurveillance.com/.

The Guardian. 2013. "US Surveillance Has Gone too Far, John Kerry Admits." *The Guardian*, November 1. www.theguardian.com/world/2013/oct/31/john-kerry-some-surveillance-gone-too-far.

———. 2014. "Text Messages Warn Ukraine Protestors They Are 'Participants in Mass Riot.'" *The Guardian*, January 21. www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot.

UNGA. 2013a. "The Right to Privacy in the Digital Age." www.auswaertigesamt.de/cae/servlet/contentblob/660692/publicationFile/186838/131127_Right2Privacy_EN.pdf.

———. 2013b. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

1.8 Technical Risk

Managing systemic risk is not simply a matter of diplomacy and international politics; it also entails effective governance aimed at ensuring the continued security and stability of critical Internet resources, as well as the development and adoption of high-quality Internet standards. The section that follows examines these technical dimensions of systemic risk.

1.8a Authority over the Root

Background

The Internet is often referred to as a "network of networks" because it is not a single physical entity, but rather "hundreds of thousands of interconnected networks linking hundreds of millions of computers around the world" (Kruger 2013). Every device that connects to the Internet has a unique Internet Protocol (IP) address, such as

216.191.141.45. IP addresses designate the virtual location of a device that connects to the Internet, allowing devices to send and receive information from other devices connected to the network. One function of the Domain Name System (DNS) is to translate between the numerical IP address to the text-based domain names that people use.

The DNS is sometimes described as the Internet's address book. At the top of the DNS are root servers that distribute the contents of the root zone file to servers across the Internet. The root zone file contains the numeric IP addresses and the corresponding domain names of the DNS servers for all top-level domains (TLDs). Across the world there are 13 "logical" root servers that are managed by academic institutions, private corporations and government institutions. Ten of these logical servers are located in the United States, one is in Sweden, one in the Netherlands and one in Japan (Kurbalija 2012). These 13 logical root servers are replicated across hundreds of servers around the world.

While there are no formal statutory authorities or international agreements governing the DNS, several entities play key roles. Because the Internet evolved from a network infrastructure funded by the US Department of Defense, the US government originally owned and operated the key components of network architecture that enabled the DNS to function (Kruger 2013). In 1998, a memorandum of understanding between the Internet Corporation for Assigned Names and Numbers (ICANN) and the US Department of Commerce (DOC) initiated a process that transitioned technical DNS coordination and management functions to ICANN, while retaining accountability to the US government. In 2006, this agreement was superseded by a joint project agreement, which expired in 2009, and was replaced by an affirmation of commitments. This affirmation formally limited US oversight by providing review panels, which are independent from ICANN board and staff, to periodically assess the activities and processes of ICANN (ibid.).

However, another contract between the DOC and ICANN authorized the Internet Assigned Numbers Authority (IANA), a subsidiary body of ICANN, to perform various technical functions under the DOC's authority, including editing the root zone file. Once the DOC approves content, it is entered into the master root server, operated by VeriSign — a private company under contract with the DOC (Kurbalija 2012, 57-58). The file in the master root server is then automatically replicated on all the other root servers. The US-delegated control over the root zone file through its contract with IANA has long placed the question of US authority at the centre of concern for various governments and stakeholders. As a result, the National Telecommunications and Information Administration (NTIA) — an agency of the DOC that is responsible for advising on telecommunication and information policy issues — issued a statement in 2011 that sought public comment on the upcoming award of a new IANA functions contract. In July 2012, the NTIA announced the award of the new IANA contract to ICANN for up to seven years.

In October 2013, ICANN and other Internet standard-setting institutions — the Internet Activities Board, Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), Internet Society (ISOC) and five regional Internet registries (RIRs) — issued the Montevideo Statement on the Future of Internet Cooperation that called for a globalization of the IANA function, which is currently being performed under ICANN with the US government (ICANN 2013). In the wake of the mass surveillance revelations, some stakeholders have questioned the exclusive US status as a counterpart to the IANA contract and control over the root zone file (Corwin 2013). In March 2014, the NTIA announced that the United States would transition oversight to the multi-stakeholder community by 2015. However, no consensus proposal for replacing the current model exists.

Contemporary Issues

What Will Authority Over The Root Look Like?

Going forward, policy makers will need to consider if the current governance model for authority over the root is sufficient, or if an additional proposal, such as further internationalization of ICANN, should be adopted. The further internationalization of ICANN would mean that it would be characterized by an international legal personality that is not a formal intergovernmental organization.

If ICANN were to adopt this model, what would its governance structure look like? The International Committee of the Red Cross (ICRC) is an independent, impartial and neutral organization with an exclusively humanitarian mission to protect the lives and dignity of victims of armed

conflict and provide them with assistance. In this sense, the ICRC has international legal personality but is not a formal intergovernmental organization. One option is to make authority over the root look more like the ICRC's neutral, independent and impartial governance model. The ICRC is governed by an assembly, an assembly council, the directorate and the presidency. The governing bodies of the ICRC have overall responsibility for ICRC "policy, strategy and decisions related to the development of International Humanitarian Law" (ICRC 2014). In addition, they oversee all activities of the organization, including "field and headquartered operations and approval of objectives and budgets" (ibid.). The members of the assembly are all elected members of Swiss nationality. These members are responsible for electing the directorate, which sits for a four-year term, the president and the vice president.

Works Cited

Corwin, P. S. 2013. "ICANN@15: Born in the USA — But Will it Stay?" www.circleid.com/posts/20131115_icann15_born_in_the_usa_but_will_it_stay_api1/.

ICANN. 2013. "Montevideo Statement on the Future of Internet Cooperation." www.icann.org/en/news/announcements/announcement-07oct13-en.htm.

ICRC. 2014. "ICRC Decision Making Structures." www.icrc.org/eng/resources/documents/misc/icrc-decision-making-structures-030706.htm.

Kruger, L. 2013. "Internet Domain Names: Background and Policy Issues." Congressional Research Service. www.fas.org/sgp/crs/misc/97-868.pdf.

Kurbalija, J. 2012. *An Introduction to Internet Governance*. Malta: DiploFoundation. www.diplomacy.edu/IGBook.

1.8b Standards Development

Background

A central function keeping the Internet operational is the development and implementation of Internet technical protocols. These are the standards that enable interoperability across the Internet, such as TCP/IP, Wi-Fi, MP3 and HTTP. While these standards are more commonly recognized, the majority of Internet standards are not visible to end-users. Private, non-state and non-profit institutions, as well as some public-private institutions, are responsible for developing the majority of Internet standards Although standards-setting organizations are largely non-political institutions, the "technical design decisions" that go into standards development can have significant economic or political implications (DeNardis 2009a). If a particular given set of standards are not adopted by the global Internet community, as well as states and businesses that use or create this technology, the technical risk is that the Internet will become fragmented. The key standards-setting organizations, their roles and membership policies are outlined below.

IETF

The IETF has developed the majority of core Internet standards, including IP and other networking standards for the Internet. The IETF was formally founded in 1986, but is a derivative of the core Internet engineering community tracing back to the 1970s. More recently, the IETF was placed under the umbrella of the ISOC, and was tasked with keeping the Internet "operational, open and transparent" (DeNardis 2013). As an institution it is unincorporated, has no formal membership or membership requirements, and makes decisions based on rough consensus and working code. This is best demonstrated by the IETF's Request for Comments process where "the basic ground rules [are] that anyone [can] say anything and that nothing [is] official" (DeNardis and Raymond 2013). This is representative of the "horizontal, distributed and voluntaristic rule making procedures" reflective of the Internet technical community (ibid.).

The W3C

The W3C is an important non-state entity that sets application-layer standards for the Web, such as HTML. It was founded in 1994 by Web inventor Tim Berners-Lee in order "to ensure interoperability among different emerging Web products developed by different companies" (DeNardis 2013). Membership in the W3C is typically held by organizations, including companies, NGOs and units of government. The W3C, like the IETF, adopts standards according to public commentary processes that are open to participation.

Recent Developments

Montevideo Statement on the Future of Internet Cooperation

For the last few years, several technical Internet organizations (ISOC, ICANN, the Internet

Architecture Board [IAB], IETF, IANA, RIRs and W3C) have met to promote better coordination among themselves. In October 2013, these organizations released the Montevideo Statement, recognizing that there is a clear need to strengthen and evolve global multi-stakeholder Internet cooperation. The statement pointed to a few key issues, such as national fragmentation, pervasive surveillance and a need to strengthen the multi-stakeholder model for Internet governance. The statement also called for a need to accelerate the globalization of ICANN and IANA functions, and the transition to Internet Protocol version 6 (IPv6) (ISOC 2013). The Montevideo Statement regarding the globalization of ICANN and the IANA functions was met with some contention from a variety of stakeholders (see the previous section for more details).

IETF and New Security Standards to Combat Surveillance

Following the 2013 revelations about online surveillance, the balance between security and human rights has become increasingly urgent in the eyes of many stakeholders, including the technical standards-setting community. In November 2013, 1,200 engineers and technical specialists gathered at the IETF meeting in Vancouver, Canada to work on improving various aspects of Internet technology. They reached broad consensus that Internet security has to be improved to protect citizens against unwarranted mass surveillance. Discussions addressed how various standards could be improved to protect against security breaches and how to meet the challenges of changing technology security in the long term. The IETF urged Web developers to support a move that would encrypt a large percentage of Internet traffic. Although this would not stop mass surveillance, the adoption of this standard would make it more expensive for governments and other actors to conduct surveillance.

Works Cited

DeNardis, L. 2009a. "Open Standards and Global Politics." *International Journal of Communications Law & Policy* 13 (1): 168–84. www.ijclp.net/files/ijclp_web-doc_9-13-2009.pdf.

DeNardis, L. 2013. *Internet Points of Control as Global Governance.* CIGI Internet Governance Papers No. 2. Waterloo: CIGI. www.cigionline.org/sites/default/files/no2_3.pdf.

DeNardis, L. and M. Raymond. 2013. "Thinking Clearly about Multistakeholder Internet Governance." Paper presented at the Eighth Annual Conference of the Global Internet Governance Academic Network (GigaNet), Bali, Indonesia, October 21. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2354377.

ISOC. 2013. "Montevideo Statement on the Future of Internet Cooperation." www.internetsociety.org/news/montevideo-statement-future-internet-cooperation.

Suggested Readings

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

1.8b-i Standards Development Principles

Background

As the Internet continues to grow, the standards that allow it to function with speed, efficiency and interoperability continue to evolve. The standards development process varies between organizations; however, many of them share particular values. Last year, the Institute of Electrical and Electronics Engineers, IAB, IETF, ISOC and the W3C affirmed a set of principles called "OpenStand" that define the characteristics of the modern standards paradigm. Although formalized in 2012, the OpenStand principles represent the standards development paradigm that has shaped the Internet since its inception. These principles are outlined below.

1. **Cooperation:** Respectful cooperation between standards organizations, whereby each respects the autonomy, integrity, processes, and intellectual property rules of the others.
2. **Adherence to principles**:
   - **Due process**. Decisions are made with equity and fairness among participants. No one party dominates or guides standards development. Standards processes are transparent and opportunities exist to appeal decisions. Processes for periodic standards review and updating are well defined.
   - **Broad consensus**. Processes allow for all views to be considered and addressed, such that agreement can be found across a range of interests.
   - **Transparency**. Standards organizations

provide advance public notice of proposed standards development activities, the scope of work to be undertaken and conditions for participation. Easily accessible records of decisions and the materials used in reaching those decisions are provided. Public comment periods are provided before final standards approval and adoption.

- **Balance**. Standards activities are not exclusively dominated by any particular person, company or interest group.
- **Openness**. Standards processes are open to all interested and informed parties.

3. **Collective empowerment**: Commitment by affirming standards organizations and their participants to collective empowerment by striving for standards that:
   - are chosen and defined based on technical merit, as judged by the contributed expertise of each participant;
   - provide global interoperability, scalability, stability, and resiliency;
   - enable global competition;
   - serve as building blocks for further innovation; and
   - contribute to the creation of global communities, benefiting humanity.
4. **Availability**: Standards specifications are made accessible to all for implementation and deployment. Affirming standards organizations have defined procedures to develop specifications that can be implemented under fair terms. Given market diversity, fair terms may vary from royalty-free to fair, reasonable and non-discriminatory terms.
5. **Voluntary adoption**: Standards are voluntarily adopted and success is determined by the market. (OpenStand 2013)

The OpenStand principles represent a "shared commitment to producing standards through open processes and consensus based decision making, with transparency and balance" (Daigle 2013). As the Internet continues to grow, policy makers need to recognize this unique approach that has contributed to the Internet's success over the past 20 years.

Works Cited

Daigle, L. 2013. "The Internet and OpenStand: The Internet Didn't Happen by Accident." *CircleID* (blog). www.circleid.com/posts/20131014_internet_and_openstand_the_internet_didnt_happen_by_accident/ .

OpenStand. 2013. "About Open Stand: A Global Community for Open Innovation." http://open-stand.org/about-us/.

1.8b-ii Enhancing Opportunities for Effective Developing World Participation in Standards Development

Background

As the Internet has become more complex, the number of standards required to use the Internet has increased. At the same time, there are a growing number of standards-setting organizations that work to make the Internet functional and interoperable. These institutions all have distinct policies and practices when it comes to developing standards and encouraging participation within their organization. As we have learned from the OpenStand principles, the legitimacy of Internet standards development has historically been derived from its open and voluntary institutional approach. However, despite this open and inclusive paradigm, stakeholders from developing countries — governments, private sector, civil society and technical community — are underrepresented in the Internet standards-setting community.

Contemporary Issues

Addressing Barriers to Entry

The degree of openness in the standards-setting process varies considerably by institution. Even in some of the most open organizations, "barriers of money, access, culture and knowledge can impede meaningful participation by developing countries" (DeNardis 2009). In the developed world, most participants in standards-setting organizations receive salaries from the organizations they work for. However, in developing countries, smaller companies, organizations or individual citizens may not have the resources to cover travel expenses for meetings that occur in the

developed world. Furthermore, compared to the developed world, the developing world is just beginning to connect online and participate in standards governance. The "esoteric knowledge and technological expertise required to participate in working groups also creates some inherent barriers to involvement for those joining the process as late entrants" (ibid.).

Access and cultural barriers also exist in standards work. For example, individuals from some cultures may experience language barriers or be unaccustomed to the informal culture of some of the Internet standards communities. Access, ranging from adequate electronic access to physical access to industry access, or even access to key decision makers in standards processes, is another key barrier to meaningful participation (ibid.).

It is important for policy makers to consider the role that developing countries play in the standards-setting process. If developing countries are not involved in standards development because of barriers to entry, their interests are not directly reflected in policy making (ibid.). In addition, involvement in standards development will increase commitment to voluntary adoption of those same standards in developing countries. Widespread adoption of key standards is critical to maintaining universal interoperability. Over the next few years, the majority of Internet growth will be coming from countries in the developing world. It is important that these countries are given a voice in shaping the future of the Internet.

Works Cited

DeNardis, L. 2009. "Open Standards and Global Politics." *International Journal of Communications Law and Policy* 13 (Special Internet Governance Edition). www.ijclp.net/files/ijclp_web-doc_9-13-2009.pdf.

Section 2:
Preserving Innovation

2.1 Internet Access and Interconnection

2.1a The Economics of Interconnection

Background

The Internet is composed of thousands of independently owned and managed networks that interconnect with each other, either bilaterally or at shared Internet Exchange Points (IXPs). When a packet is routed across networks to reach its destination, information from one service provider's network will flow seamlessly through another provider's network via high-speed fibre optic cables connected at high-speed switches. Although there are many types of private interconnection arrangements made between networks in practice, generally speaking, network operators agree to exchange traffic with one another through mutual peering agreements in which no money changes hands or via paid transit agreements in which one network operator pays the other for transport to the Internet. Network operators will employ a combination of peering and transit agreements to engineer the most cost-effective and efficient solution for routing information (ISOC 2013). These agreements are generally private in nature and typically involve little or no regulatory oversight.

Internet interconnection has evolved independently from the historical traditions of interconnection among voice telecommunication providers. The ongoing transition from traditional landline, cellphone and SMS networks to Voice over IP (VoIP) networks for telecommunications services poses a major threat to the business models of incumbent telecommunications operators. Throughout the developing world and to some extent in Europe, national telecom incumbents are key sources of government revenue and are seen as symbolic national corporate champions. Accordingly, many states, as well as the incumbents within them, are motivated to preserve their business models by increasing the costs of VoIP, or by finding a way to capture revenue from interconnection.

This revenue model concern led to new proposals in advance of the World Conference on International Telecommunications (WCIT) in 2012. The European Telecommunications Network Operators' Association (ETNO) made a proposal that suggested three global policy alterations pertinent to Internet interconnection: expansion of International Telecommunication Regulations (ITRs) to include Internet connectivity; involvement of nation-states in "facilitating" interconnection; and the prospect of compensation between providers based on "sending party network pays" (DeNardis 2012). Sending party pays is imported from the telephone model of "calling party pays" (ISOC 2013). Sending party pays is a direct adoption of the international telephone regime, where the caller incurs the cost of placing the call. This proposal is a fundamental challenge to the current model of transit and peering agreements that accomplish Internet interconnection and, as a result, has been met with concern.

Contemporary Issues

Is State Oversight and Regulation Needed?

Some stakeholders have argued that there is a need for state regulation, or at least facilitation, of Internet interconnections. There has been a long history of calls for direct governmental regulation or funding of this interconnection, particularly over the following concerns.

- **Interconnection in emerging markets**: In many parts of the world, countries do not have a single shared IXP within their borders. Shared interconnection sites play "a critical role in emerging markets by bringing content closer to users, promoting local peering connectivity among regional network operators, reducing interconnection costs, and enabling sovereign nation state autonomy in areas such as critical infrastructure protection" (DeNardis 2012). Some stakeholders have argued that state regulation would improve the expansion of IXPs into the developing world. Others have argued that state regulation would actually impede the expansion of IXPs into the developing world by creating disincentives for network operators to expand into complex regulatory systems. (ibid.).
- **Anti-competitive practices**: Unlike traditional telecommunication services, there has been little regulatory oversight of how Internet interconnection occurs, beyond antitrust concerns. While on one hand, market forces and antitrust regulations can effectively discourage anti-competitive behaviour in peering and transit agreements, there are rational concerns about lack of competition in Internet backbones and incumbent network peering policies that limit additional connectivity other than paid transit by smaller providers.

- **Censorship and filtering**: Because interconnection points concentrate the flow of traffic between network operators, they are potential points of government filtering and censorship. Having greater transparency and insight into the agreements and configurations at these sites of potential government intervention is important and is an area in need of additional attention.

Compensation through "Sender Pays"

Many stakeholders have taken the view that despite the fact that there is little oversight, Internet interconnection works. In general, these stakeholders argue that state regulation is not needed for the following reasons:

- **Complication**: The "sending party network pays" principle would greatly complicate interconnection, since carriers would be required to build and maintain accounting mechanisms in order to determine who will pay for traffic that flows between networks. Furthermore, "protecting against manipulation of the payment system would entail further complexity and cost" (Center for Democracy and Technology 2012).
- **Higher costs**: Sender pays would result in higher costs that would be incurred by network accounting systems and subsequently passed on to Internet users. Sending party pays is a direct adoption of the international telephone regime, where callers pay high fees for long distance phone calls. Forcing IP interconnections to reflect the telephone regime could make Internet access more like long distance calling with higher costs passed on to customers.
- **Limits on developing countries**: If sending networks have to pay fees to reach local telecom operators that serve users in developing countries, large corporations may decide that certain countries are "not big or commercially important enough to justify the cost of routing traffic there" (ibid.). As carriers decline or limit interconnection with destinations deemed not worth the cost of termination fees, certain countries may find themselves on a worsening side of the digital divide. Citizens in those countries could face reduced ability or increased costs to access important content outside of their countries borders.

The "sender pays" proposal could be used as a development model. For example, some stakeholders may argue that the ETNO proposal, or something like it, would help generate revenue that could be used for infrastructure deployment in less developed countries. Furthermore, because the proposal does not specify any particular use for such funds, countries could extract a levy from the network operator and use it to improve the overall welfare of the state. However, these ideas have also been met with criticism. While the sender pays model may generate additional revenue for some carriers, it will most likely come at the cost of the citizens, who may already suffer from access issues due to high costs. Furthermore, if the sender pays model is used to help improve development, it would be highly uneven due to geography and the attractiveness of setting up interconnection points in certain countries over others.

Works Cited

Center for Democracy and Technology. 2012. "ETNO Proposal Threatens to Impair Access to Open, Global Internet." www.cdt.org/files/pdfs/CDT_Analysis_ETNO_Proposal.pdf.

DeNardis, L. 2012. "Governance at the Internet's Core: The Geopolitics of Interconnection and Internet Exchange Points (IXPs) in Emerging Markets." Paper presented at the Telecommunications Policy Research Conference, the 40th Research Conference on Communication, Information and Internet Policy, Arlington, VA. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2029715.

ISOC. 2013. "Internet Interconnections: Proposals for New Interconnection Model Comes up Short." www.internetsociety.org/sites/default/files/Internet%20Interconnections%20Proposals%20For%20New%20Interconnection%20Model%20Comes%20Up%20Short.pdf.

Suggested Readings

WCIT. 2012. *Russian Federation: Proposals for the Work of the Conference.* http://files.wcitleaks.org/public/S12-WCIT12-C-0027!R1!MSW-E.pdf.

2.1b Localization and Possible Fragmentation

Background

When information is transmitted over the Internet, it is divided up into small segments called packets that are transmitted across networks via routers over the fastest path to their destination. Each packet is comprised of a payload (the actual content of the information), along with administrative information such as IP addresses. In order for a packet to reach its destination along the fastest route, it may travel over several networks that cross the borders of various states. Because routing algorithms "help routers optimize routes to minimize the latency or delay in transmitting information" from one place to another, and because network operators will exchange this information between one another, users have little control over or knowledge about where their data travels (DeNardis 2013). With the proliferation of Internet applications that rely on cloud computing technology, this phenomenon is exacerbated as suppliers optimize their capacity by moving and storing data on different servers that could be located outside of a user's home country (National Board of Trade 2012). The border-blind nature of Internet routing raises important questions regarding the security and privacy of data in transit, as well as over determining who has legal jurisdiction over such data.

Contemporary Issues

Localization and Uncertainty Regarding Applicable Legal Systems

The NSA surveillance disclosures have become a major concern for countries in the European Union, Brazil and elsewhere. In addition to thinking about creating national servers to store national data, Brazil has been working to create a "BRICS cable" (Brazil, Russia, India, China and South Africa) that will create "an independent link" between BRICS countries in order to "bypass NSA cables and avoid spying" (RT 2013). This points to important concerns regarding the movement of data across foreign jurisdictions. When public data is routed or stored in a server in a foreign country, a number of serious issues arise, such as the potential consequences of this information being exposed to another country's legal system and regulatory apparatus. While the majority of countries have some form of data protection and confidentiality legislation, it is common for limitations on the treatment of foreign data to exist. Furthermore, in many other countries, substantial data protection laws are often lacking. Would routing data through (or cloud storage of data in) a country be sufficient to establish legal jurisdiction over that data?

Works Cited

DeNardis, L. 2013. *Internet Points of Control as Global Governance*. CIGI Internet Governance Papers No. 2. www.cigionline.org/sites/default/files/no2_3.pdf.

National Board of Trade. 2012. *How Borderless is the Cloud? An Introduction to Cloud Computing and International Trade*. Sweden: National Board of Trade.

RT. 2013. "Brazil to Press for Local Internet Data Storage after NSA Spying." RT.com. http://rt.com/news/brazil-brics-internet-nsa-895/.

2.1c Net Neutrality

Background

A founding design principle of the Internet was the desire for an open system in which packets are delivered across a network equally without regard to their content or other characteristics. The basic contemporary question of "net neutrality" is whether ISPs should be legally prohibited from discriminating against certain types of Internet traffic versus other types. As a principle, net neutrality requires that ISPs route all traffic in a neutral manner, without blocking or throttling back packets based on content, traffic type, protocol, application or destination. Over the past few years, censorship by Internet intermediaries has been increasing in scale and scope. While ISP blocking is currently widespread in controlling spam email and, in some countries, blocking sexually explicit or illegal images, over the past few years various network operators have received criticism for blocking content and throttling smaller ISPs that piggyback on their network infrastructure for anti-competitive purposes, as well as for engaging in general traffic management purposes (Belli and De Filippi 2008). At the same time, the net neutrality debate has been further fuelled when a US appeals court threw out federal rules requiring broadband providers to treat all Internet traffic equally (Nagesh and Sharma and 2014).

To block and/or throttle content, ISPs employ "Internet traffic management techniques" that

inspect, prioritize or deprioritize Internet content in a tiered fashion. Internet traffic management techniques can take on different forms for various reasons: "needs basis discrimination" takes place when there is network congestion; "active discrimination" takes place when carriers inspect all data packets regardless of congestion; and "blocking" takes place when carriers discard data traffic from a particular source (Verhulst 2011). The main questions that policy makers must address are: when and under what conditions may ISPs be prohibited from discriminating or using Internet traffic management techniques for various purposes; and who will provide oversight to ensure open access and prevent anti-competitive behaviour?

Contemporary Issues

Appropriate versus Inappropriate Discrimination

New technologies such as deep packet inspection now allow ISPs to look inside a data packet to see its content. ISPs can tell how much email a customer is sending or receiving, whether they are using peer-to-peer software, specific applications such as Skype or if they are using their connection for online gaming. Because different applications consume different amounts of bandwidth, some ISPs argue that customers who use high-bandwidth applications slow down everyone's connection. Critics of ISP discrimination often argue that if ISPs discriminate between different types of traffic, ISPs could limit applications that threaten their own businesses. For example, Skype would compete with phone services offered by many ISPs and therefore threaten existing profit streams. Critics also suggest that if ISPs discriminate and provide tiered services, bigger companies that can afford to pay ISPs for faster speeds will enjoy an unfair advantage over smaller firms and individuals. It is important to note that packet inspection and similar technologies are not always harmful, and can be used to prevent viruses, denial of service attacks and other malicious activity. Policy makers will need to confront serious questions, including: what is appropriate and inappropriate discrimination? What kind of policy or set of laws should governments adopt in order to ensure fair access to Internet content? How to conduct proper oversight regarding Internet management techniques and ISP discrimination?

Preserving Openness and Universal Access

Proponents of net neutrality suggest that an "open and fair" network is important for empowering users and fostering creativity and innovation. They suggest that the adoption of invasive techniques can have consequences for a user's fundamental rights to expression and privacy, which are guaranteed by international human right standards. Policy makers will need to ask what kinds of limitations (if any) should be placed on differential packet treatment.

Works Cited

Belli, L. and P. De Filippi. 2008. The value of network Neutrality for the Internet of Tomorrow. http://nebula.wsimg.com/c65488b3edff49adc2dba84e344591bd?AccessKeyId=B45063449B96D27B8F85&disposition=0.

Nagesh, Gautham and Amol Sharma. 2014. "Court Tosses Rules of Road for Internet." *Wall street Journal*. http://online.wsj.com/articles/SB10001424052702304049704579320500441593462.

Verhulst, S. G. 2011. "Mapping Digital Media: Net Neutrality and the Media." www.opensocietyfoundations.org/sites/default/files/mapping-digital-media-net-neutrality-20110808.pdf.

Suggested Readings

CBC. 2009. "FAQ: Net Neutrality and Internet Traffic Management." CBC News, July 2. www.cbc.ca/news/technology/faq-net-neutrality-and-internet-traffic-management-1.789869.

2.2 Critical Internet Resources: Balancing Adequacy, Accessibility, Security and Stability

Critical Internet Resources (CIRs) refer to Internet-specific logical resources; they are unique binary and alphanumeric identifiers related to the Internet's addressing system and the DNS. A common characteristic of CIRs is the technical design requirement that they serve as globally unique identifiers, a feature necessitating centralized coordination. The need for some centralized coordination has often raised questions about who should most appropriately have oversight, how to equitably reflect the globalized nature of the Internet and how to procedurally create necessary legitimacy for centralized oversight.

2.2a IP Addresses

Background

IP addresses are the unique numerical addresses that all devices that connect to the Internet must have, either permanently or temporarily for a session. The system that distributes IP addresses is hierarchically organized. At the top is the IANA function of ICANN. IANA distributes blocks of IP numbers to the five regional Internet registries. RIRs then distribute IP numbers to local Internet registries and national Internet registries, which allocate or assign them to smaller ISP companies, businesses and users.

Under the long-standing standard for Internet addresses, Internet Protocol version 4 (IPv4), each binary address is 32 bits in length. This design feature provides a reserve of approximately 4.3 billion unique Internet addresses. In February 2011, these addresses had been fully allocated by IANA to the five RIRs and to incumbent users who predated the formation of the RIRs. This depletion has been accelerated by the introduction of Internet enabled devices, such as mobile phones and game consoles, as well as the rise of overall Internet connectivity (Kurbalija 2012). Therefore, an important current policy question about IP addresses involves how to manage the remaining reserve of IPv4 addresses. There is broad consensus that the prevailing IPv4 address reserve will soon be exhausted, a phenomenon with significant implications, especially in parts of the developing world without large existing stores of IPv4 addresses (DeNardis 2013).

In 1990, the Internet standards community identified the potential depletion of IP addresses as a crucial design concern (DeNardis 2009). Subsequently, the IETF recommended a new protocol, IPv6, to expand the number of available addresses, from 32 to 128 bits. This would supply the world with 2^{128} or 340 undecillion addresses (ibid.). Despite the fact that IPv6 has been available and implemented in products for a long time, for a variety of political and technical reasons, the deployment to IPv6 has barely begun (DeNardis 2013).

Contemporary Issues

IPv6 Implementation

Compatibility

Part of the difficulty is that an IPv6-only Internet device cannot communicate with IPv4-only devices: a computer or phone connected to the Internet via IPv6 would not be able to connect natively to an IPv4 Web server. Yet, "IPv4 sites are the norm and will likely remain the norm for the foreseeable future" (DeNardis 2009). Going forward, policy makers and technical actors must determine what type of market intervention or government regulation is necessary (if at all) to address the exhaustion of the IPv4 address space or to provide incentives for upgrading to IPv6.

IPv4 Address Transfer

In the early days of the Internet, before the RIR system was in place, some organizations received large allocations of IP addresses. These addresses became known as "legacy address space" and account for about 40 percent of all IPv4 addresses. These organizations have no relationship with the RIRs, because the RIRs were established after these early IP address allocations. However, because IPv4 addresses are now scarce, a voluntary redistribution of IPv4 addresses has been occurring with the emergence of new "IPv4 address broker businesses" advertising online to facilitate these transfers. There is concern that a growing market in IPv4 addresses has developed, with a significant proportion of addresses coming from the legacy allocations. There is also some concern that legacy address markets provides incentives to delay and/or resist the transition to IPv6.

Works Cited

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

———. 2013. *Internet Points of Control as Global Governance*. CIGI Internet Governance Paper Series No. 2. www.cigionline.org/sites/default/files/no2_3.pdf.

Suggested Readings

ITU. 2013. "IPv4 and IPv6 Issues." www.itu.int/en/wtpf-13/Documents/backgrounder-wtpf-13-ipv4-ipv6-en.pdf.

2.2b Domain Names

Background

The DNS is a critical operation that translates between the domain names that people use and the binary addresses that computers use. For this reason, the DNS is often referred to as the Internet's phonebook. Through this address resolution process, the DNS resolves billions of queries per day. In a very simplified way, the DNS can be described as an "enormous, hierarchal database management system that is distributed globally across countless servers" (DeNardis 2013). The Internet's root name servers contain a master file known as the root zone file. This file lists the IP address and associated names of the official DNS servers for all TLDs: generic top-level domains (gTLDs), such as .com, .edu, .gov, etc.; and country codes (ccTLDs), such as .ch for China or .uk for the United Kingdom.

Contemporary Issues

The TLD Expansion and Globalization

Technically, the potential to create new TLDs is almost unlimited. However, the introduction of new gTLDs has been a slow and sometimes contentious process. After six years of consultations, in 2011, ICANN approved a new gTLD program that would end most restrictions on gTLDs and allow any organizations to apply and run their own TLD, including TLDs in non-Latin language scripts — called Internationalized Domain Names (IDNs). These new IDNs are important because they will further facilitate the creation and accessibility of content in non-Western languages. The new gTLD application guidebook contains policy requirements for gTLDs. One of these requirements is that "applied for strings must be comprised of three or more visually distinct letters or characters in the script, as appropriate" (Seng 2009). This imposes some constraints on Chinese, Japanese and Korean languages, where every ideograph represents a word. This means that the three-character policy would require TLDs to be at least three words (ibid.).

In 2012, ICANN started taking applications for new TLDs: they received nearly 2,000 proposals ranging from .blog, .shop, .apple to .books. Companies that submitted applications paid a US$185,000 application fee to ICANN. The application fee has raised a number of important concerns regarding competition because it may discourage smaller business from applying. Moreover, under the new gTLD program, applicants would commit to being responsible for the registry, raising initial questions about whether there would be a free market for any entity wanting to register, or whether there would be anti-competitive behaviour around new gTLDs. New gTLDs will allow similar companies and organizations a specialized Web suffix, such as .shoes or .jeans, which would be commercially desirable. This raised a number of questions: who would own and manage commercially desirable gTLDs such as .shoes; and how would fair competition for a commercially desirable gTLD be ensured?

Geographic and Commercial Applications

New gTLDs can create conflict between geographic and commercial applicants. This was the case when Brazil and Peru objected to a bid made by Amazon for the .amazon gTLD. Until now, the differences between commercial and geographic types of identity were easily distinguished; however, new gTLDs are changing this, as the lines between commercial and geographic distinctions are no longer as clear (Watts 2013). The Governmental Advisory Committee of ICANN has given geographic applicants priority in cases of conflict. This is, to some extent, controversial, as it demonstrates the influence the committee could exert over ICANN; to some, this is an unwelcome intrusion of the state, while to others, this is an important check on commercial dominance of the Internet.

Works Cited

DeNardis, L. 2013. "The Emerging Field of Internet Governance." In *Oxford Handbook of Internet Studies*, edited by William Dutton. Oxford: Oxford University Press.

Seng, J. 2009. "Why ICANN TLD Policy Imposes Severe Constraints on Development of Internationalized Domain Names." *CircleID* (blog). www.circleid.com/posts/20090720_icann_tld_policy_imposes_constraint_internationalized_domains/.

Watts, J. 2013. "Amazon v. the Amazon: Internet Retailer in Domain Name Battle." *The Guardian*, April 25. www.theguardian.com/environment/2013/apr/25/amazon-domain-name-battle-brazil.

Suggested Readings

Musiani, F. 2013. "New Global Top-Level Domain Names: Europe, the Challenger." *Internet Policy Review*. http://policyreview.info/articles/analysis/new-global-top-level-domain-names-europe-challenger#References.

2.3 Cloud Computing

2.3a Cloud Computing Technology

Background

Cloud computing involves running applications or storing data on a remote, Internet-based server, rather than on a local computer (Bradshaw, Harris and Zeifman 2013). Unlike uploading data to a local hard drive, when an individual uploads information to a cloud they are unaware of the physical location of the data.

Cloud services can be broken down into three categories (UN Conference on Trade and Development [UNCTAD] 2013):

- **Infrastructure as a service,** where the cloud provider's processing, storage and other computing resources allow the user to deploy and run software.
- **Platform as a service,** where the user's own applications and programming tools are owned and managed by a cloud provider.
- **Software as a service,** where a user takes advantage of software running on the cloud provider's network rather than on the customer's own hardware.

The essence of what we've come to know as cloud computing is not new — users have uploaded and stored data on remote servers for years, most commonly with their own ISPs. What is novel about cloud computing, as it is known today, are the expansion of the type and quantity of information that can be uploaded, and the commensurate expansion in the number of individuals and firms using and offering remote servers for business and personal applications. However, the rapid expansion of cloud computing services raises a number or challenges and risks that relevant stakeholders must consider.

Contemporary Issues

The Developing World and Cloud Computing

Limited Internet Infrastructure

Due to a lack of basic Internet infrastructure, the options for cloud services available in low- and middle-income countries are different than those in advanced economies. Limited Internet infrastructure — such as IXPs, broadband, fibre optic cables, and power grids and outlets — impacts the availability, quality and speed of a user's connection. This also affects a country's ability to build local data centres. As a result, there is a "significant digital divide in terms of data centre and server availability across countries" (UNCTAD 2013). Limited Internet infrastructure also affects the type of cloud services available to a particular region. While many Internet users make use of basic cloud services, such as email or VoIP, these applications require "far less speed and can tolerate more latency than advanced cloud services relevant to the business world" (ibid.).

Cost of Communication

The cost of communication is another challenge for developing countries. Many businesses in the developing world cannot afford the combined costs of utilizing cloud services, connecting to the Internet via ISPs and purchasing hardware required for an Internet connection. These combined costs are likely to form a much higher proportion of a business's expenses in the developing world compared to advanced economies.

Data Privacy and Security

Data privacy and security are concerns for both developed and developing countries. Cloud computing services will often route and store data on a server that is located in a foreign country, raising a number of legal, jurisdictional and regulatory challenges concerning data security and privacy. In countries that carry out surveillance on its citizens and have poor privacy laws, citizens of that state may also be concerned if cloud servers store their personal data locally. To date, there is no international harmonized privacy framework that regulates data transfers across borders. As of 2013, 99 countries have national laws that cover data privacy in some way (ibid.), yet there is no standard for how much protection these laws offer, and foreign and domestic data are often held to different standards under domestic legal regimes.

Works Cited

Bradshaw, S., K. Harris and H. Zeifman. 2013. "Big Data, Big Responsibilities: Recommendations to the Office of the Privacy Commissioner on Canadian Privacy Rights in a Digital Age." CIGI Junior Fellows Policy Brief No. 8. www.cigionline.org/sites/default/files/no8_0.pdf.

UNCTAD. 2013. "Information Economy Report 2013: The Cloud Economy and Developing Countries." http://unctad.org/en/PublicationsLibrary/ier2013_en.pdf.

2.3b Firms as Internet Consumers

Background

Across industries, firms rely upon the Internet for carrying out their core business. They use the Internet for communication, e-commerce, supply chain management, financial transactions, marketing and most other basic business functions. Cloud computing applications, in particular, are increasingly being used by firms in the conduct of business. Examples include: using cloud-based email to communicate with customers and partners; backing up essential business documents on a cloud-based server rather than solely on a hard drive; and cloud-based social media applications, such as Facebook, to advertise to a broad customer base. In addition, companies are increasingly using cloud applications to outsource administrative costs and relocate programs and data to external servers. As firms continue to use the Internet as a medium for business applications, communication and advertisement, Internet governance will have a large impact on how firms do business.

Contemporary issues

Rapid adoption of cloud-based ICT architecture and services creates a number of challenges for firms as large Internet consumers. Under the current model of interconnection and Internet routing, data travels across Internet infrastructure without regard for national borders. Even if contracts require cloud services to be hosted in "safe" countries, internationalization of data hosting creates difficulties in ensuring data can flow between legal jurisdictions without becoming subject either to third-country legal regimes or other means of government access.

Aside from issues relating to data transit, the increasing internationalization of data hosting and other such services creates more straightforward policy challenges. The collection and storage of customer information by firms that operate online poses important liability questions in the event such data is compromised, lost, or perceived to be improperly used. To the extent firms operate digitally in multiple jurisdictions, they may face additional liability and/or increased compliance costs created by differences in data protection and lawful intercept regimes. They may also face brand risks associated with operating digitally in jurisdictions consumers see as unsafe or as unduly authoritarian.

To the extent that states adopt data localization requirements, whether in response to concerns about foreign intelligence activity or for other reasons, firms may also be faced with the difficult choice between withdrawal from such markets and the implementation of costly changes to their core operations. Such changes might include the construction of local data centres and the decentralization of service departments that work with the data in question.

As firms continue to move their business online, and as consumers continue to use the Internet as a medium for brand recognition and purchasing products, any interruption to business services offered online will impact a firm's ability to compete in the marketplace. Business interruption can occur as a result of incidents of consumer data theft or other cybercrimes, as well as damage to Internet infrastructure due to a violent conflict or natural disaster. On the one hand, decentralization reduces the risk of damage at any particular geographic location; however, it also creates vulnerability from damage at any of these geographic locations. Policy makers and firms may want to consider how Internet resilience can be further increased, in order to reduce the incidence and severity of business interruption, as well as whether (and how) firms might be compensated in such circumstances.

Suggested Readings

National Board of Trade. 2012. "How Borderless is the Cloud? An Introduction to Cloud Computing and International Trade." Sweden: National Board of Trade. www.kommers.se/Documents/dokumentarkiv/publikationer/2012/rapporter/publication-how-borderless-is-the-cloud.pdf.

UNCTAD. 2013. "Information Economy Report 2013: The Cloud Economy and Developing Countries." http://unctad.org/en/PublicationsLibrary/ier2013_en.pdf.

2.3c Taxation and Transfer Pricing

Background

Transfer pricing is "the setting of prices for transfers within [a] multinational enterprise [MNE]" (Eden 2011). Transfer pricing is an issue that must be addressed when a corporation is conducting business in more than one country. Within MNEs, international transfer pricing is often a source of conflict of objectives. CEOs and corporate controllers do not always agree on the use of transfer pricing techniques for "cost allocation of resource decisions, economic business decisions…and overall tax strategies" (Abdallah and Maghrabi 2009). Transfer pricing also engenders disputes between firms and states. States wish to protect their taxable revenues, whereas corporations wish to lower their taxable earnings through transfer pricing schemes. As a result, transfer pricing has been described as the "grey area of tax" (*Financial Post* 2013).

For some, transfer pricing is "the biggest tax avoidance scheme of all" (Sikka 2009). As globalization has provided corporations with the ability to design, manufacture and sell products on a global basis, such a structure gives corporation discretion in allocating costs to each country and shifting profits through intrafirm trade.

In order to protect the interests of the state, the Organisation for Economic Co-operation and Development (OECD) has established international rules on transfer pricing (see OECD 2010). However, these rules rely on the notion of "cost," which can be unclear. In general, the rule that governs cost is the "arm's length" principle, where normal commercial prices are used to transfer goods and services. However such prices are not easy to find, especially when markets are dominated by a very limited number of multinationals.

Contemporary Issues

Personal data is generating a new wave of opportunity for economic and societal value creation (World Economic Forum 2011). Many websites, such as Google and Facebook, are a means to commercialize access to personal information. The data collected about individuals is often transferred between servers, and sold and resold on second and tertiary markets. If ICT firms are profiting off of the sale and resale of personal data, policy makers must ask important questions related to taxation and transfer pricing: given that the sale of personal data is becoming a new asset for ICT firms, should data sales be taxable like other goods and services that move between firms across borders? If yes, how do policy makers determine the price of personal data? Should firms be transparent in the intra-irm movement of data across borders? If yes, how do states hold firms accountable to intrafirm transfer pricing of personal data?

Works Cited

Abdallah, W. M. and A. S. Maghrabi. 2009. "Do Multinational Companies have Effective Transfer Pricing Systems of Intangible Assets and E-commerce?" *International Journal of Commerce and Management* 19 (2): 115–26.

Eden, L. 2011. "The Ethics of Transfer Pricing." Paper presented at the AOS Workshop on Fraud in Accounting, Organizations and Society. www.business.ualberta.ca/en/Departments/AOIS/Conferences/FraudInAccountingOrganizationsAndSociety/~/media/business/Conferences/FraudInAccountingOrganizationsAndSociety/Documents/EDEN-SMITH-ETHICS-OF-TP-AOS-UK-FINAL.PDF.

Financial Post. 2013. "Transfer Pricing Presents Risks and Opportunities." *Financial Post*, February 19. http://business.financialpost.com/2013/02/19/transfer-pricing-presents-risks-and-opportunities/.

OECD. 2010. "OECD Guidelines for Multinational Enterprises." www.oecd.org/ctp/transfer-pricing/transfer-pricing-guidelines.htm.

Sikka, P. 2009. "Shifting Profits Across Borders." *The Guardian*, February 12. www.theguardian.com/commentisfree/2009/feb/11/taxavoidance-tax.

World Economic Forum. 2011. "Personal Data: The Emergence of a New Asset Class." www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

2.4 The Intersection of Internet Governance and the International Trade Regime

In a relatively short period of time, the Internet has shifted from a source of information to a market for goods, services and ideas, increasing economic growth, expanding access to information, and altering the way that trade is done. Trade agreements, such as the Trans-Atlantic Trade and Investment Partnership (TTIP) and the Trans-Pacific Partnership (TPP), are increasingly incorporating chapters on e-commerce, the cross-border delivery of services, the flow of information and the inclusion of new Internet-related intellectual property rights, but no substantial progress has been achieved at the global level since the Uruguay Round. Therefore, much of the existing international legal mechanisms and governance infrastructure for managing issues that arise at the intersection of Internet governance and the international trade regime have become highly inconsistent or outdated.

2.4a Transnational Data Flows and Cloud Computing

Background

The Internet has increased the amount of global trade by increasing the free flow of digital products and services across borders, as well as the global flows of information and financial flows that support global trade in offline products. Flows of digital products and services across borders are increasingly occurring via cloud computing technology. The term "cloud computing" is used to describe a wide range of services delivered using computing resources. Generally, it involves running applications or storing data on a remote, Internet-based server, rather than on a personal computer. Common cloud services include email programs, social networks and file hosting services. In addition to individual users, cloud computing services are being increasing used by actors in both the private and public sector.

Free trade agreements increasingly include cloud-related provisions. Most notably, discussions of the TTIP and the TPP have dealt with the facilitation of cross-border data transfer. An eventual agreement may include language committing parties not to introduce or maintain unnecessary barriers to electronic data flows across borders. US negotiators have been pushing to prevent countries from implementing "localization requirements" that require companies doing business in one jurisdiction to physically locate computer servers there.

Localization requirements are problematic for technical reasons. Since cloud suppliers have strong incentives to optimize their capacity, data is often moved between different servers, depending on where storage space is available (National Board of Trade 2012). When cloud services are being used to process data, it is also common for the information to be moved between servers. This means that even if there is an agreement with the customer about where the information shall be stored, it may be moved to another location during processing, and then returned and stored in an agreed location (ibid.). The results are that a customer can be exposed to another country's legal system, regardless of the storage location stated in the agreement. Further, since Internet traffic is routed in a border-blind manner, there may be exposure to another legal system in transit. These technical aspects of how cloud computing functions are of vital legal importance, as they raise important questions regarding the security and privacy of data in the cloud.

Contemporary Issues: Transnational Data Flows

Cloud Computing and Server Localization

As discussed in Sections 2.1b and 2.3, Brazil has raised concerns about its citizens' data being routed through US infrastructure and thus potentially subject to American jurisdiction. In response, Brazil is developing a plan that may require local data storage centres for large Internet corporations, such as Facebook and Google. While installing localized data storage centres may help promote consumer privacy by protecting users' data, the proposition has been met with opposition by Internet corporations. In a letter to the Brazilian government, about a dozen Internet companies wrote that "in-country data storage requirements would detrimentally impact all economic activity that depends on data flows" and argued that this policy would push companies away (Reuters 2013).

Works Cited

National Board of Trade. 2012. "How Borderless is the Cloud? An Introduction to Cloud Computing and International Trade." Sweden: National Board of Trade. www.kommers.se/Documents/dokumentarkiv/publikationer/2012/rapporter/publication-how-borderless-is-the-cloud.pdf.

Reuters. 2013. "Brazil to Insist on Local Internet Data Storage after US Spying." Reuters, October 28. www.reuters.com/article/2013/10/28/net-us-brazil-internet-idUSBRE99R10Q20131028.

Suggested Readings

Aaronson, S. 2012. "Trade and the Internet: Risks and Challenges of this New Technology." *The Magazine of International Economic Policy*. www.international-economy.com/TIE_W12_Aaronson.pdf.

Caile, D., K. Kalinich, P. Fair and A. Lawrence. 2013. "Data Sovereignty and the Cloud, A Board and Executive Officer's Guide: Technical, Legal and Risk Governance Issues Around Data Hosting and Jurisdiction." http://cyberlawcentre.org/data_sovereignty/CLOUD_DataSovReport_Full.pdf.

Berry, R. and M. Reisman. 2012. "Policy Challenges of Cross-Border Cloud Computing." *Journal of International Commerce and Economics*.

Savage, L. C. 2013. "Trade Agreements, Privacy, and the Cloud." *Maclean's Magazine*, June 17. www2.macleans.ca/2013/06/17/trade-agreements-privacy-and-the-cloud/.

World Economic Forum. 2011. "Advancing Cloud Computing: What To Do Now? Priorities for Industry and Government." www3.weforum.org/docs/WEF_IT_AdvancedCloudComputing_Report_2011.pdf.

Wunsch-Vincent, S. and A. Hold. 2011. "Towards Coherent Rules for Digital Trade: Building on Efforts in Multilateral versus Preferential Trade Negotiations." Swiss National Centre of Competence in Research.

2.4b Standards as Technical Barriers to Trade

Background

Internet standards are the "blueprints" for developers, as they provide common formats and specifications to ensure that products are interoperable with products made by other manufactures. As a result, standards perform "a key economic function by providing a common platform for product innovation and the production of multiple competing products" (DeNardis 2014).

Internet governance standards development has traditionally been "open," meaning standards with no (or minimal) intellectual property restrictions on their use are chosen. This open approach is often credited with contributing to economic growth, innovation and market conditions with fair competition among Internet companies. The IETF and the W3C, two main Internet standards-setting organizations, have traditionally published their standards openly. However, not all Internet-related standards are open. There are many information technology standards that have underlying patents which require royalty payments for use. For example, Wi-Fi standards have been at the centre of long-running patent lawsuits (ibid.).

Standardization is directly related to global trade conditions. When a country's technology companies have access to global and open Internet standards, they have an opportunity to develop and invest in innovative products that will interoperate with other products on the global market. The World Trade Organization (WTO) Agreement on Technical Barriers to Trade acknowledges the role of international standards in the facilitation of global trade by "improving efficiency of production and facilitating the conduct of international trade," and asserts that WTO members will "ensure that technical regulations are not prepared, adopted or applied with a view to or with the effect of creating unnecessary obstacles to international trade" (cited in DeNardis 2014).

Contemporary Issues

Open Standards and the Promotion of International Trade and Development

Governments have different policies requiring certain characteristics of standards-based

intellectual property in the technologies they procure. US policy states that the owners of any intellectual property "have agreed to make that intellectual property available on a non-discriminatory, royalty-free or reasonable royalty basis to all interested parties" (DeNardis 2014). The objective of this approach is to balance the rights of the patent holder with the promotion of innovation. Other countries, such as India, require that the government give preference to the adoption of royalty-free or open standards. The rationale for open standards policies includes "promoting an economic environment in which there is a level playing field for competition and innovation based on the standard, as well as avoiding vendor lock-in and dependence on a single vendor for products and services" (ibid.). Policy makers will have to consider whether or not Internet standards should be royalty bearing or open, what rights an Internet-standards patent holder should have and whether or not they should be compensated, and how international trade, economic growth and innovation should be weighed against standards-embedded patents.

Works Cited

DeNardis, L. 2014. *The Global War for Internet Governance*. London: Yale University Press.

Suggested Readings

WTO. 2014. "Technical Barriers to Trade." www.wto.org/english/tratop_e/tbt_e/tbt_e.htm.

2.4c Copyright and Trademarks

Intellectual property is an umbrella term encompassing the law of copyrights, trademarks, trade secrecy and patents. Knowledge, ideas and brand recognition are powerful resources in the global economy. In order to protect these key resources, intellectual property rights (IPRs) have been established in both international agreements and national jurisdictions. Key international governing bodies include the World Intellectual Property Organization and the WTO's trade-related aspects of intellectual property rights (known as TRIPS) agreement.

Background

Copyright and trademark laws balance the rights of individuals over their creative works with a recognition that extensive social and economic benefits flow from their circulation. However, traditional concepts of copyright and trademark are challenged by the Internet in numerous ways. This is largely due to the fact that the Internet collapses the distinction between transmitting, copying and using information. The potential for sharing information has become limitless, as digital technology gives everyone the ability to instantly upload and share copyrighted materials on websites with global reach.

Currently, policy debate over copyright and trademark IPRs is characterized by extreme polarization: state and corporate advocates of these IPRs continue to support extensive and systemic interventions into Internet governance mechanisms, while users and civil liberties groups form countermovements, supporting free and open access to knowledge, ideas and information.

Intensive lobbying efforts by recording and entertainment industries have begun to culminate in new regulatory actions by governments around the world. These actions have largely been aimed at using Internet intermediaries to filter or monitor the dissemination of copyrighted content. For example, the Stop Online Piracy Act (SOPA) and the PROTECT IP Act (PIPA) in the United States attempted to stop online piracy by giving Internet intermediaries permission to further block access to infringing websites and ban search engines to link to such sites. Internationally, the Anti-Counterfeiting Trade Agreement (ACTA) addresses IPR infringements in ways that may open the possibility for private policing and enforcement.

All of these regulatory actions have been met with strong countermovements from civil liberties groups, users and academics on the grounds of human right and freedom violations. Developing a legitimate legal mechanism that finds a balance between the interests of copyright holders and users is the biggest challenge faced by policy makers going forward.

Contemporary Issues

Striking a Balance

There is an ongoing struggle between the Internet's ability to facilitate information sharing and open networking, and the attempts of the owners of trademarked names and copyrighted content to build "legal and technical fences around their assets" (Mueller 2010). Traditionally, the balance between exclusivity and free use has been drawn by a concept that the law calls fair use or "fair dealing." While the specifics vary among

different legal systems that have adopted "fair use" doctrines, in general, the law provides an exemption from copyright liability for purposes of research, private study, education, parody, satire, criticism or review.

However, striking a fair balance in the digital age is a complex issue, given that digital reproduction has many applications. Further, fair use has been criticized for focusing on the rights of the right holder, leaving individuals ill-equipped to make fair use of digital information. Therefore, finding a fair definition of fair use is important for balancing the rights of right holders and users.

Enforcement

The growing regulatory trend emerging from the IPR debate is a shift from state responsibility for monitoring and policing Internet conduct onto private sector intermediaries. It is not only territorial boundaries that pose a problem to state regulation, but the massive scale and scope of the interactions enabled by the Internet: "if it is too difficult and costly for the state to police the billions of interactions among a billion individuals connected by the Internet, then one can vest those who provide the platforms and capabilities for digital communications with the responsibility for infringing actions by their users" (ibid.). Delegating responsibility to the private sector can be a strategy for overcoming the limits of territorial jurisdiction, but outlining what their roles will be and establishing accountability, legitimacy and transparency are all issues that need to be considered.

Considerations

Any restriction of fair use could weaken the position of developing countries. The Internet provides researchers, students and others from developing countries with a powerful tool for participating in global academic and scientific exchanges. A restrictive copyright regime could have a negative impact on capacity building in developing countries. Furthermore, restrictions of fair use could limit the right to freedom of speech and education.

Domain Name Trademark Disputes

Trademark disputes have been at the centre of many policy controversies over domain names. Since the establishment of the Internet, there have been a number of "cybersquatting" issues, where actors have tried to capitalize on the unique nature of domain names by registering a domain name that might become popular, such as a product or a name, and then selling it back to the owners of the product or to the individual. Traditionally, DNS trademark disputes have been managed by ICANN's Uniform Domain-Name Dispute Resolution Policy. However, this system has been criticized for having limited remedies and for being non-binding in the sense that decisions do not preclude a subsequent or contemporaneous court proceeding (Fernbach 2012). Furthermore, because intellectual property laws vary across national jurisdictions, a number of complexities have arisen, such as "where a trademark is registered versus where a server is located versus where a trademark infringing entity resides" (DeNardis 2013).

Works Cited

DeNardis, L. 2013. "The Emerging Field of Internet Governance." In *Oxford Handbook of Internet Studies*, edited by William Dutton. Oxford: Oxford University Press.

Fernbach, Terrence. 2013. "'What Is in a Name?' A Comparative Look at the ICANN Uniform Domain Name Dispute Resolution Policy and the United States Anti-Cybersquatting Consumer Protection Act." Munich Intellectual Property Law Center Master Thesis Series (2011/2012). March 2. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2226375.

Mueller, M. L. 2010. "IP vs. IP." In *Networks and States: The Global Politics of Internet Governance*. MIT Press: Cambridge.

Suggested Readings

Collins, S. 2010. "Digital Fair: Prosumption and the Fair Use Defence." *Journal of Consumer Culture* 10 (1): 37–55.

Kawashima, N. 2010. "The Rise of 'User Creativity' — Web 2.0 and a New Challenge for Copyright Law and Cultural Policy." *International Journal of Cultural Policy* 16 (3): 337–53.

Kurbalija, J. 2012. *An Introduction to Internet Governance*. Malta: DiploFoundation. www.diplomacy.edu/IGBook.

Wunsch-Vincent, S. and A. Hold. 2011. "Towards Coherent Rules for Digital Trade: Building on Efforts in Multilateral versus Preferential Trade Negotiations." Swiss National Centre of Competence in Research.

2.4d Technological Patents

Background

While copyright and trademark issues on the Internet receive more public attention, it is important to recognize that full consideration of IPR issues in the context of Internet governance should also include patents. Patents protect inventions by providing a government-granted monopoly to an invention that excludes others from making, using, selling or importing claimed inventions for a limited period of time. Only recently have patents started being granted for software, making patents applicable to Internet technology. Coordinating mechanisms around standards-based patents are also a complex area of IPRs built into the Internet's architecture.

"Patent trolling" refers to enterprises that apply for a massive number of patents, or that use patents they own to extract a toll from the competition, giving them an advantage in the market, or as a stand-alone business model. The term "troll" is often used by critics who compare these acts to mythical trolls who hide under bridges built by others and unexpectedly demands tolls or payments from those who wish to cross (Yeh 2012). Patent trolling has gained a significant amount of attention in the information and telecommunications industry over the past few years, as numerous firms have been entangled in courts around the world for patent infringement cases.

Contemporary Issues

"Fuzzy" Patents

Patenting software raises a number of issues that current laws and governing infrastructure are unable to address. In order for an invention or process to be patented, it must be deemed "novel and non-obvious." However, the legal conditions of novelty and non-obviousness have been poorly applied to software patents. One way governing bodies determine whether or not something is novel and non-obvious is by making sure the requested patent hasn't been captured by a "prior art" condition — i.e., something similar has not been created. However, because software programmers develop an incredible amount of code, it is hard to distinguish the novelty and non-obviousness conditions (Vee 2010).

A second reason it is difficult to examine the novelty and non-obvious factor when it comes to software patents is because software patent applications only require a written description. Consequently, many software patent applications have "fuzzy boundaries," as they are deliberately written with vague and expansive scope, in order to maximize their potential value. The vagueness of these patents allows companies to take advantage of the patent system. Currently, companies litigate software patents at a rate that is 30 percent higher than other patents (Bessen and Meurer 2008, 187). The higher rates of litigation on software patents and the huge spending on patent litigation indicates that companies are treating patents as commodities and attempting to acquire them and defend them as a means to extract revenue. This is at odds with the purpose of the patent system, which is to allow creators to profit from their innovations — but in good faith efforts to innovate, rather than in attempts to maximize individual corporate profits.

Standards-embedded Patents

Internet standards serve as blueprints that product developers follow to achieve compatibility with other products. As discussed in Section 2.4b, many (but not all) Internet standards are generally considered to be open standards. At the nexus of global Internet governance are intellectual property and Internet standards, and some stakeholders are concerned about the increasing extent of royalty-bearing patent applications and claims for standards required for the exchange of information over the Internet. These critics argue that royalty-bearing patents on standards will have a negative effect on innovation, economic competition and costs to end-users. Part of their concern emanates from the evolution of more complicated conditions of intellectual property rights under technical standards necessary for routine Internet use. As more devices that connect to the Internet embed hundreds of different standards (such as a smartphone), it becomes more difficult for new innovators to pay royalty fees to patent holders (DeNardis 2014). In contrast, proponents of standards-based patents argue that innovators should be compensated for their ideas, and a small royalty fee that is non-discriminatory and reasonable is a fair way to balance the need for innovation and rights of the patent holder.

Works Cited

DeNardis, L. 2014. *The Global War for Internet Governance*. London: Yale University Press.

Vee, A. 2010. "Carving up the Commons: How Software Patens are Impacting our Digital Composition Environments." *Computers and Composition* 27 (1): 179–92.

Yeh, B. 2012. "An Overview of the Patent-Troll Debate." Congressional Research Service. www.eff.org/sites/default/files/R42668_0.pdf.

Suggested Readings

Bessen, J. and M. Meurer. 2008. *Patent Failure*. Princeton: Princeton University Press.

Bessen, J., J. Ford and M. Meurer. 2012. "The Private and Social Costs of Patent Trolls." *Regulation* (Winter). www.cato.org/pubs/regulation/regv34n4/v34n4-1.pdf.

Kurbalija, J. 2012. *An Introduction to Internet Governance*. Malta: DiploFoundation. www.diplomacy.edu/IGBook.

2.5 The Internet and Economic Development

Developed countries are a decade ahead of the rest of the world in terms of Internet access. This is an important concern, because the Internet is increasingly viewed as an economic and social platform that not only supports activities across the entire economy, but also provides a space for different cultures to share their values, ideas and knowledge.

There is clear evidence that access to the Internet can aid countries in their development by improving access to health services and education, and by offering new opportunities for employment. It is both an important and pressing concern that all populations living in the developing world have the necessary means to access and meaningfully utilize the Internet.

While on the one hand it is important to maintain a clear distinction between the issues of technical governance and coordination that ensure the stability and end-to-end accessibility of the Internet, and issues arising from how the Internet is used on the other hand, it is also important to bear in mind that current Internet governance debates are occurring in the context of a real and persistent digital divide. That divide is a product of the globally uneven deployment and penetration of ICTs but also a product of inequalities in access to the kinds of skills and training necessary to allow individual users to maximize their use of ICTs.

Although this briefing book cannot address all issues relating to this digital divide, let alone all policy-relevant aspects of Internet use, the following section addresses a selected group of development-related issues. It should also be noted that progress on these development issues can be expected to improve Internet governance by ensuring that users, firms and other stakeholders in developing and emerging markets are able to participate fully and meaningfully in Internet governance debates, as well as in the deployment and operation of Internet infrastructure.

2.5a Developing and Emerging Countries as Internet Consumers

Background

In many parts of the developing world, people are connecting to the Internet at an unprecedented rate. By the end of 2011, more than three billion people worldwide were using the Internet. While only 24 percent of people in developing countries are connected, this number is projected to reach 50 percent by 2015 (OCHA 2012). In addition, the convergence of mobile and Internet technologies is opening up new opportunities for connection. According to the Broadband Commission (2013), "mobile broadband subscriptions overtook fixed broadband subscriptions in 2008, and show an astonishingly high growth rate of some 30 percent per year, the highest growth rate of any ICT, exceeding fixed broadband subscriptions by a ratio of 3:1."

ICTs facilitate access to knowledge materials that are necessary for economic development, cultural realization and individual fulfillment. Instead of being constrained by location, ICTs can act as a gateway to money, communication services, books, education and work to users wherever they are (World Economic Forum 2013). ICTs also play an important role in supporting economic growth, business innovation and the creation of high-quality jobs. Particularly, research has demonstrated that ICTs are "now widely recognized everywhere as an important source of efficiency gains for companies that will allow them to optimize their production function and liberalize resources toward other productive investments" (ibid.). This is particularly true as more businesses in the developing world make use of cloud computing applications to reduce IT costs and start-up costs (National Board of Trade 2012).

Contemporary Issues

Infrastructure

In order to connect to the Internet and experience it with a good quality of service, Internet infrastructure is needed in many parts of the developing world. Although Internet infrastructure has seen substantial growth over the past few years, there are many pockets throughout the developing world that are unable to connect to the Internet or experience good quality of service. In particular, three areas of infrastructure can be expanded to help improve connectivity and reduce the digital divide are: submarine cables — undersea fibre optic cables which make up the part of the Internet backbone that connects continents across the ocean; IXPs — the locations where Internet traffic moves between networks and network operators; and broadband towers.

Costs

In addition to basic Internet infrastructure, communities need access to affordable broadband services and the equipment necessary to utilize them. In 2012, the cost of using the Internet as a proportion of average income in developing countries was 40 percent (OCHA 2012). High Internet prices disproportionately impact women compared to men, as women have lower incomes and often have less control over spending (Broadband Commission 2013). More affordable prices will play a significant role in reducing both the digital divide and the digital gender gap.

Intellectual Property

Some scholars argue that accessing knowledge and technology is a crucial element of sustainable development, and that an access-enabled copyright regime is necessary for supporting sustainable development (Schonwetter and Ncube 2011). These experts argue that intellectual property policies threaten to impede the benefits available to developing countries, as they make digital content inaccessible, hinder the adaptation of software to local needs, drain revenues from developing countries to developed countries, and allow the abuse of IPRs in software and other technologies (Bannerman 2008). This is in contrast to the views of other experts who support the current intellectual property regime. These latter experts commonly argue that the implementation of current intellectual property policies in developing countries encourages economic growth by providing incentives to authors and inventors for creativity and innovation, encouraging research and development, and providing security to those who invest in IP products and related industries, including the area of ICTs (ibid.). Policy makers must consider whether or not an access-enabled copyright regime is necessary for promoting development, and whether or not the current intellectual property regime is sufficient at incentivizing economic growth while making digital content and other forms of knowledge accessible.

Works Cited

Bannerman, S. 2008. "Intellectual Property Issues in ICT4D." International Development Research Centre. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1014166.

Broadband Commission. 2013. "The State of Broadband 2013: Universalizing Broadband." www.broadbandcommission.org/documents/bb-annualreport2013.pdf.

National Board of Trade. 2012. "How Borderless is the Cloud? An Introduction to Cloud Computing and International Trade." Sweden: National Board of Trade. www.kommers.se/Documents/dokumentarkiv/publikationer/2012/rapporter/publication-how-borderless-is-the-cloud.pdf.

OCHA. 2012. "Humanitarianism in a Networked Age." https://docs.unocha.org/sites/dms/Documents/WEB%20Humanitarianism%20in%20the%20Network%20Age%20vF%20single.pdf.

Schonwetter. Tobias and Caroline Ncube. 2011. "New Hope for Africa? Copyright and Access to Knowledge in the Digital Age." *Info* 13 (3): 64–74. www.emeraldinsight.com/doi/abs/10.1108/14636691111131457.

2.5b Developing and Emerging Countries as Digital Innovators

Background

Developing economies play an important role as producers in the Internet economy. Their unique experiences provide them with opportunities to innovate ICT and related Internet applications. The developing world is not solely a consumer of Internet technology, but also plays an important role in the production and design of many ICTs. There are already many examples of innovative ideas coming from the developing world.

One example is "Ushahidi," a platform that was initially developed in Kenya to crowd-map

reports of violence after the post-election fallout at the beginning of 2008. Relying on open-source software, Ushahidi captures, organizes and shares critical information gathered from social media and text messages. The Ushahidi platform has since been adopted and used in other countries. In particular, it was used in Haiti in 2010 and in the Philippines in 2013 after the devastating natural disasters to help relief efforts, by creating real-time reports about trapped persons and disseminating information for specific needs such as food, water and shelter.

Free and open-source software (FOSS) plays an important role in the ability of developing countries to design ICT according to local needs. FOSS encapsulates a couple of different philosophies of software development and licensing. The first, "free software," operates on the philosophy that software code is like a language, and therefore should not be owned because it is foundational to the society that uses it. The second, "open-source software," requires that software code be made openly available, but does not necessarily include a clause that prevents the use of open-source code in proprietary software.

The use of FOSS is often pointed to as a way to encourage software localization, expand IT knowledge and skills, and increase the security and independence of the developing world. First, FOSS "not only creates the potential for a 'spin off' IT sector to grow in developing or least developing countries, but also allows users and developers to create their own software tailored to their own needs and their own national and regional languages" (Story 2004). Second, FOSS encourages the development of computer programming, maintained and developmental skills within the local user community for free. Finally, FOSS is a way that developing countries can assert independence from the proprietary software.

Contemporary Issues

Open-Source Software, Patents and Other Challenges

Countries such as the United States and the United Kingdom grant patents in software, while many developing countries do not (Bannerman 2008). Although these countries do grant patents in software, their legitimacy and legality are still highly contested in the courts. In general, software patents have been criticized for presenting a particular danger to FOSS initiatives. A FOSS programmer or user could unknowingly infringe on a software patent in a FOSS program, which would mean that the FOSS developer or user would have to pay damages or licensing fees to the patentee (ibid.). In addition, there are other issues to consider when adopting FOSS. Although FOSS may reduce the costs of accessing and utilizing software, there are other relevant costs that may still prevent an individual from using it, such as the cost to connect to the Internet or to purchase hardware that would be able to run the programs. In addition, language barriers, lack of education in information technology, lack of Internet infrastructure, and the poor availability and reliability of electricity are other barriers.

Works Cited

Bannerman, S. 2008. "Intellectual Property Issues in ICT4D." International Development Research Centre. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1014166.

Story, A. 2004. "Intellectual Property and Computer Software: A Battle of Competing use and Access Visions for Countries of the South." UNCTAD-ICTSD Project on IPRs and Sustainable Development: Issue Paper No. 10. Geneva: International Centre for Trade and Sustainable Development and UNCTAD. www.iprsonline.org/unctadictsd/docs/CS_Story.pdf.

Suggested Readings

May, C. 2006. "Escaping the TRIPS Trap: The Political Economy of Free and Open Source Software in Africa." http://onlinelibrary.wiley.com/doi/10.1111/j.1467-9248.2006.00569.x/abstract.

2.5c Developing and Emerging Countries, Multinational Enterprises and Foreign Direct Investment

Background

Foreign direct investment (FDI) is a cross-border investment by a resident firm or entity into a foreign economy. FDI is a key element of international economic integration as it creates direct and long-lasting links between economies. It encourages technology transfer between countries and allows host countries to promote their products on an international market. FDI is an additional source of funding for investment and can also be used as a tool for development (OECD 2013).

In the context of Internet governance, FDI is particularly useful for improving Internet and telecommunication infrastructure in developing countries, and is the biggest source of private investment into this infrastructure. This is especially true today, as markets in the developing world are largely untapped due to a lack of infrastructure or incredibly high costs to connect. As a result, markets in Asia, Africa and Latin America present ICT corporations with the biggest market for new customers.

One contemporary example of FDI in Internet and communication infrastructure is the Internet.org project, launched by Facebook, Ericsson, MediaTek, Nokia, Opera, Qualcomm and Samsung. The goal of the project is to tap into the developing world's markets, by making the Internet more accessible and affordable across the developing world.

Contemporary Issues

Monopolies and Incumbents

Internet access is very costly in many places in the developing world. In some cases, it costs as much as 40 percent of an earner's average income to connect. Some stakeholders have argued that incumbent telecommunication operators are responsible for keeping prices high and stifling economic growth (Southwood 2014). The privatization and increased competition in the telecommunication sector has been cited as a solution to reduce costs of Internet access. In contrast, however, incumbent telecommunication operators are a large source of government revenue in the developing world. Opening up these monopolies to private investment may in turn lower the amount of (vital) revenue governments can collect.

Another solution policy makers can consider is improving public-private partnerships (PPPs) that contribute to Internet infrastructure development. The ITU has published a report on best practices PPPs can adopt to improve broadband access, use public funds more effectively, manage risks, and stimulate and create demand to ensure the broadband infrastructure is effectively used (see ITU 2012).

Works Cited

ITU. 2012. "Developing Successful Public-Private Partnerships to Foster Investment in Universal Broadband Networks." www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/documents/GSR12_BBReport_Yardley_PPP_7.pdf.

OECD. 2013. "OECD Factbook 2013: Economic, Environmental and Social Statistics." www.oecd-ilibrary.org/sites/factbook-2013-en/04/02/01/index.html?itemId=/content/chapter/factbook-2013-34-en.

Southwood, R. 2014. "We Name Africa's Telecom Delinquents." *Tech Central*. www.techcentral.co.za/we-name-africas-telecoms-deliquents/46200/.

Suggested Readings

Goel, V. 2013. "Facebook Leads an Effort to Lower Barriers to Internet Access." *The New York Times*, October 21. www.nytimes.com/2013/08/21/technology/facebook-leads-an-effort-to-lower-barriers-to-internet-access.html?_r=0.

Internet.org. 2013. "Technology Leaders Launch Partnership to make Internet Access Available to All." https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851572_595418650524294_1430606495_n.pdf.

2.5d Internationalization of Internet Content

Background

Different societies have rich and unique histories that should be recognized and shared. One of the fundamental aspects of internationalizing Internet content is ensuring that technology will support text in any writing system of the world. This will allow cultures with different writing systems to communicate with a global audience and share their values, knowledge and ideas with others. Internationalizing the Internet and its content is important for both accessing content through domain names and viewing content uploaded online.

ICANN has played an important role in internationalizing the DNS. Until recently, TLDs were limited to the Latin alphabet and were therefore largely inaccessible to various populations around the world. However, in May 2010, ICANN began approving TLDs in a variety of scripts, including Chinese, Arabic and Cyrillic. While the introduction of IDNs is considered to be one of the main successes of the Internet governance regime, there are still a number of technical and policy issues that need to be addressed.

Contemporary Issues

International Standards and Technical Challenges

Despite IDNs being available for over a decade, they have not worked in all email applications (EURid and UNESCO 2012). For example, social networking sites such as Facebook require users to create an account with an email address; however, it does not support IDN email addresses in user accounts, despite its extensive support for multilingualism on its content pages. In 2012, the IETF published standards for IDNs in email; however, they have not been adopted in email clients such as Gmail and Outlook (ibid.).

As new gTLDs are being rolled out by ICANN, there are also some barriers for the development of IDNs. The new gTLD application guidebook contains policy requirements for gTLDs. One of these requirements is that "applied for strings must be comprised of three or more visually distinct letters or characters in the script, as appropriate" (cited in Seng 2009). This imposes serious constraints on Chinese, Japanese and Korean languages, where every ideograph represents a word. This means that the three-character policy would require TLDs to be at least three words (Seng 2009).

The internationalization of Internet content is both a technical and a policy issue: in order to help make Internet content more accessible worldwide, policy makers need to work with technical experts to help establish sound policy and standards that promote International content.

Works Cited

Seng, J. 2009. "Why ICANN TLD Policy Imposes Severe Constraints on Development of Internationalized Domain Names." *CircleID* (blog). www.circleid.com/posts/20090720_icann_tld_policy_imposes_constraint_internationalized_domains/.

EURid and UNESCO. 2012. *World Report on Internationalized Domain Names Deployment*. www.icann.org/en/resources/idn/eurid-unesco-deployment-08nov12-en.pdf.

Suggested Readings and References

W3C. 2013a. "Internationalization." www.w3.org/standards/webdesign/i18n.

———. 2013b. "Working Group Charter on Internationalization." www.w3.org/2012/07/i18n-charter/charter.html.

2.5e Access and Infrastructure Expansion

Background

Over the past five years, Internet infrastructure has seen substantial growth due to the rapid growth of mobile services. In Africa, for example, SIM card uptake grew from 23 percent in 2007 to 65 percent in 2011 (African Development Bank Group 2013). However, the spectacular growth in the mobile sector has not been replicated in the landline broadband segment. Although Internet penetration has almost doubled between 2007 and 2011, about 87 percent of the African population is still unable to connect to it (ibid.). High access costs are the largest barrier of entry due to limited Internet infrastructure such as Internet interconnection points, submarine cables, wireless broadband towers and reliable power grids.

Contemporary Issues

Infrastructure Expansion

Submarine and Other Backbone Cables

Access to international Internet backbones depends on the availability of submarine fibre optic cables. For landlocked countries, increasing the number of cross-border terrestrial fibre optic cables that connect landlocked countries to submarine cables could help deliver Internet access to end-users. In addition, there are many coastal countries that have no submarine cables and others with only one or two cables that may not fully benefit from competition on those cables. A small number of additional submarine cables could substantially increase the available Internet bandwidth and improve the quality of service for countries around the world.

IXPs

The expansion of local IXPs is another component of a comprehensive solution to access problems. IXPs provide a concentrated shared location where Internet traffic can move between networks and network operators. The location of the IXP is important because it can determine the distance and cost of sending information from one network to another. When IXPs are local, Internet traffic can be handled locally, reducing the costs of the communication and increasing the speed for users. In countries without IXPs, the handoffs between networks have to take place in foreign countries. This can increase costs as information is transferred across foreign networks and then sent back to the country of origin (OECD 2011). The

lack of local IXPs also creates challenges relating to the privacy and security of data in transit.

Mobile Towers and Broadband Expansion

Rural areas consistently lag urban areas in deployment of mobile broadband infrastructure. Broadband is increasingly regarded as central to the development of an information and knowledge-based society and key to achieving digital inclusion. The affordability of broadband is a key barrier to extending Internet access in developing countries. While broadband is becoming more affordable around the world, huge discrepancies in affordability still exist. In 2012, fixed broadband services remain expensive, accounting for 30.1 percent of average monthly income in developing countries, compared to just 1.7 percent in developed countries (Broadband Commission 2013). In poorer countries, like Sub-Saharan Africa, the cost is extreme: fixed broadband Internet services cost more than 100 percent of an individual's average monthly income (ibid.).

Works Cited

African Development Bank Group. 2013. "Connecting Africa: An Assessment of Progress Towards the Connect Africa Summit Goals."

Broadband Commission. 2013. "The State of Broadband 2013: Universalizing Broadband." www.broadbandcommission.org/Documents/bb-annualreport2013.pdf.

OECD. 2011. "The Relationship Between Local Content, Internet Development and Access Prices." www.oecd.org/sti/ieconomy/50305352.pdf.

Suggested Readings

Schummann, R. and M. Kende. 2013. *Report for the Internet Society: Lifting Barriers to Internet Development in Africa: Suggestions for Improving Connectivity*.

2.5f The Governance of Big Data

Background

A massive amount of data is being generated from a variety of sources (UN Global Pulse 2012). This data is called big data, which can be defined as "an umbrella term that represents the massive volume and variety of data that is created and stored on the Internet" (Bradshaw, Harris and Zeifman 2013). Big data is enabled by the Internet and devices that connect to it; for example, it is collected in the process of online searches, the creation of social media accounts, surveys and the data mining of phone calls and text message logs (ibid.). It is also collected in large stores of actual content, such as eHealth, scientific data and other forms of knowledge. Most of the data collected through our interactions with technology is done by private corporations and while some of this data collection is incidental, much is an intrinsic part of the business models driving the global information economy.

Big data is increasingly viewed as a tool to fill the void of real-time data. Unlike traditional sources and techniques for data collection, such as surveys and census data, that generate a long-term picture, big data sources are much more effective at generating a real-time picture for decision makers. The UN Global Pulse (2012) has outlined some of the common features of big data sources:

- Digitally generated: data is created digitally (as opposed to being digitized manually) and can be manipulated by computers.
- Passively produced: data is a by-product of our daily lives or interactions with digital services.
- Automatically collected: there is a system in place that extracts and stores data as it is generated.
- Geographically or temporarily traceable: data is associated with a time or place.
- Real time: data can be analyzed in real time.

As a result, private corporations, governments and humanitarian aid agencies are beginning to explore how these new data sources can be used to improve development and build more resilient communities. While big data has generally been applied to hard sciences and business, there is already evidence of its applicability beyond these fields. Applying big data analytics to public health, for example, can help detect disease outbreaks before confirmed diagnosis or laboratory confirmations. Google Dengue Trends is one example that works on predictive public health, monitoring certain search terms that indicate dengue activity.

However, applying big data to the field of development faces several challenges; some concerns relate to privacy and security concerns, whereas other concerns pertain to data analysis. This section will highlight some of the contemporary issues policy makers will have to consider.

Contemporary Issues

Privacy and Security

Privacy is one of the most sensitive issues when it comes to accessing, utilizing and securing data. Internet users — who are the primary producers of data — may be unaware that they are producing data, and may be unaware of how it is being used. For example, people routinely consent to Terms of Service (ToS) agreements, Web forms and surveys, or onsite paperwork, such as health questionnaires or store loyalty programs, without fully realizing how their data might be used or misused. Furthermore, many people who are aware of the privacy risks associated with using the Internet and mobile technology are unable to avoid them due to ToS agreements that give companies permission to collect and store an individual's data. While it can be said that consumers consent to these agreements by using the services in question, in reality they have little to no ability to negotiate the contracts themselves. Because many Internet services — such as search engines, email or social media — have become an essential part of society, opting out of ToS agreements essentially amounts to opting out of the economy and digital public sphere.

Furthermore, data can often be sold or distributed to third parties without an individual's knowledge as to where the data is going and for what purposes it will be used. While most companies purchase data as a major marketing asset, governments and NGOs have also been known to buy and sell data (Bradshaw, Harris and Zeifman 2013). This raises a number of security concerns for individuals, as it can put their physical security or privacy at risk. Even if data is anonymized before it is sold, studies have shown that it is fairly easy to de-anonymize information (UN Global Pulse 2012). This raises a number of security concerns regarding the traceability of data. When information can be tracked back to a particular individual or group of individuals, it can put these people at risk. Information that identifies individuals who report on acts of violence or human right violations could be used by governments or armed groups for retribution (OCHA 2013).

Accuracy and Interpretation

An important challenge in applying big data to any particular issue is making sure that the data used in analysis is accurate. However, there are challenges in ensuring that information is actually accurate and representative of any given situation. For example, data could easily be false or fabricated, or it might simply reflect an individual's perceptions rather than fact. There might also be difficulties in interpreting the information if sarcasm, slang or ironies are used. Big data sets are also prone to selection effects and other sampling errors such as the systematic underrepresentation of individuals with limited or no Internet connectivity and the systematic overrepresentation of the most connected individuals.

A second and related challenge to getting the picture right is recognizing bias in the data. While bias and accuracy might appear to be similar, there are important differences: a piece of data may be factual, but it might also contain a built-in bias due to factors such as participation. A 2011 Gallup poll of cellphone users across Africa highlights the risk of such a bias. The poll showed that cellphones tended to be sued more by the educate elite in richer countries. For example, "76 percent of people with over nine years of education owned a mobile phone in South Africa, whereas only 10 percent of people with less than four years of education owned a mobile phone in the Central African Republic" (OCHA 2013). One of the promises of big data is its alleged objectivity; that there will be less discrimination against minority groups because "raw data is immune to social bias, allowing analysis to be conducted at a mass level and thus avoiding group based discrimination" (*Sydney Morning Herald* 2013). Yet, big data cannot fully capture the whole picture if all of society is not represented, and is therefore highly discriminatory in terms of who has access to the Internet and mobile technology.

Works Cited

Bradshaw, S., K. Harris and H. Zeifman. 2013. "Big Data, Big Responsibilities: Recommendations to the Office of the Privacy Commissioner on Canadian Privacy Rights in a Digital Age." CIGI Junior Fellows Policy Brief No. 8. www.cigionline.org/sites/default/files/no8_0.pdf.

OCHA. 2013. "Humanitarianism in the Network Age." https://docs.unocha.org/sites/dms/Documents/WEB%20Humanitarianism%20in%20the%20Network%20Age%20vF%20single.pdf.

Sydney Morning Herald. 2013. "Is Big Data All it's Cracked Up to Be?" *Sydney Morning Herald*, May 13. www.smh.com.au/it-pro/business-it/is-big-data-all-its-cracked-up-to-be-20130513-2jh55.html.

UN Global Pulse. 2012. "Big Data for Development: Challenges and Opportunities." www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-UNGlobalPulseJune2012.pdf.

Suggested Readings

UN Global Pulse. 2013. "Big Data for Development: A Primer. Harnessing Big Data for Real Time Awareness." www.unglobalpulse.org/sites/default/files/Primer%202013_FINAL%20FOR%20PRINT.pdf.

World Economic Forum. 2012. "Big Data, Big Impact: New Possibilities for International Development." www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf.

2.6 Competition Policy and Regulation

Background

Incumbent Operators

Physical network infrastructure is needed to deliver high-speed Internet service. However, it is costly to build and requires local governments in many countries to grant relevant construction permits. There are many challenges for new market entrants. When a new ISP wishes to enter the market, instead of building its own physical infrastructure, it will often pay existing network operators a rate to piggyback off their networks. Some stakeholders have argued that incumbent network operators engage in anti-competitive behaviour, often throttling the service that smaller ISPs are offering their customers and offering poor customer support. This is especially problematic in the developing world where ISPs are often smaller businesses that do not have the capital to develop infrastructure or the capacity to reach more remote areas. As a result, many stakeholders have been arguing for a more liberalized telecommunication sector to increase competition.

Search Engines

Search engines must perform several important tasks, such as mapping content available on the Internet, employing algorithms to provide a list of the most relevant search results without tampering, and aggregating and indexing information (Langford 2013). In November 2010, the European Union launched an antitrust investigation of Google, prompted by complaints from smaller, competitive EU search engines that Google was employing search biases in its algorithms, constituting an antitrust violation. The Federal Trade Commission (FTC) launched an inquiry into Google that ended in early 2013 when "the FTC concluded that there was insufficient evidence to bring an enforcement action against Google" (ibid.). The EU investigation was recently settled as Google agreed to give its EU rivals more prominence in specialized search results, making searches in Europe look different than searches in the United States. Despite this settlement, Google's competitors still feel that the remedies "hardly provide them with protection" because they "do not believe Google has any intention of holding themselves to account on these proposals" (*The New York Times* 2014).

Contemporary Issues

Telecommunication Monopolies

Market forces may result in an increasingly oligopolistic global market structure for Internet access (Kurbalija 2012). This problem exists in both developed and developing countries. Some stakeholders have argued that the process of liberalizing network operators — i.e., privatizing the telecommunication sector — will solve the problem of monopolies and incumbent operators. However, liberalization has been criticized by other stakeholders who argue that it could simply lead to the replacement of a public monopoly with a private monopoly, affecting the price and quality of Internet services.

Transition Issues Associated with Telecommunication Liberalization

A considerable number of countries have liberalized their telecommunication markets. However, countries that have not yet undergone this process are often faced with a hard choice: to liberalize and make their telecommunication market more efficient, or to preserve an important source of government revenue from existing monopolies. Liberalizing telecommunication markets has been a point of contention throughout the developing world. Brazil and India are usually mentioned as countries where liberalization facilitated the fast development of the Internet and ICT sector, benefiting their overall economic growth. However, least developed countries found the liberalization of telecommunications to be a major challenge: the telecommunication sector in these countries are an important source of

budgetary income, and as the monopolies started to disappear, governments also lost an important source of revenue (ibid.). Managing these difficult transition issues will require thoughtful leadership and openness to innovative financing mechanisms.

Antitrust and Search Engines

For years, there has been a debate as to whether or not searches engines should be regulated. On the one hand, state regulation could be effective at ensuring fair competition in search results. However, search algorithms are valuable industry secrets. If states were to begin regulating search engines, private firms would need to give up the details of their valuable algorithm to state authority if meaningful regulation were to occur.

Some search models are being regulated. For example, airline Computer Reservation Systems (CRS) are searches that have been considered as a model for the regulation of larger search engines such as Google (see Langford 2013). However, unlike CRS regulations, which have "relatively few variables, a small number of parties, and a steady number of flights based on existing routes," Google search algorithms continuously seek out and organize billions of web pages, are constantly updated and are of far greater complexity than the ranking systems a CRS probably would employ" (ibid.). Going forward, policy makers will need to determine if regulation is needed to promote and protect fair competition in search algorithms.

Works Cited

Kurbalija, J. 2012. *An Introduction to Internet Governance*. Geneva: DiploFoundation. www.diplomacy.edu/IGBook.

Langford, A. 2013. "gMonopoly: Does Search Bias Warrant Antitrust or Regulatory Intervention?" www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11086&context=ilj.

The New York Times. 2014. "Google Settles Its European Antitrust Case; Critics Remain." *The New York Times*, February 6. www.nytimes.com/2014/02/06/technology/google-reaches-tentative-antitrust-settlement-with-european-union.html?_r=0.

Section 3:
Ensuring Rights Online

3.1 Establishing the Principle of Technological Neutrality for Human Rights

Background

The Universal Declaration of Human Rights (UDHR) was drafted with foresight to accommodate future technological developments so that individuals could continue to exercise their basic human rights regardless of new technological developments (UNGA 2013). The UDHR was also drafted so that technology, despite its developments, would remain neutral — meaning that the same rights people have offline, must also be protected online. Therefore, international human rights should remain relevant and applicable, and neutral to new technologies, such as the Internet and other emerging ICTs.

During the 20th Session of the Human Rights Council in June 2012, the UNHRC reaffirmed the neutrality of technology by passing Resolution A/HRC/20/L.13 on the Promotion, Protection and Enjoyment of Human Rights on the Internet. The resolution "affirms that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights" (UNHRC 2012).

Despite this resolution, there has not been a direct translation from rights offline to rights online; in particular, a number of challenges are evident as a result of revelations about online surveillance. States and corporations actively collect information about individuals, including their own citizens; Internet content is blocked for various purposes, some of which may infringe on an individual's right to freedom of expression; and social media platforms are being monitored and sometimes restricted by governments to limit freedom of expression, assembly and religion.

It is important to recognize that rights, both online and offline, are not absolute and have limitations that are generally defined by national laws. Article 29 of the UDHR states that: "In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society" (UN 1948).

These limitations are important because individuals not only have rights, but also have duties to ensure that the rights of others are respected. The commitment to ensuring that all human rights are technology-neutral is an important first step by the UNHRC. The challenge for policy makers going forward is not defining new rights for cyberspace, but affirming how existing human rights are relevant on the Internet.

Works Cited

UNGA. 2013. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

UNHRC. 2012. "Resolution on the Promotion. Protection, and Enjoyment of Human Rights on the Internet." www.regeringen.se/content/1/c6/19/64/51/6999c512.pdf.

UN. 1948. "The Universal Declaration of Human Rights." www.un.org/en/documents/udhr/.

3.2 Privacy and the Right to be Forgotten

Background

Rapid technological advances are changing the world around us, bringing new challenges for the protection of privacy and personal data. These advances allow individuals to share information about themselves easily and on a global scale. Social networking sites and cloud computing are two examples that pose challenges to data protection, as they can involve the loss of an individual's control over their potentially sensitive information when they upload and share their data with programs hosted on third-party hardware. At the same time, data collection techniques are evolving. They are becoming "increasingly elaborated and less easily detectable," as new and sophisticated tools allow operators to better target and monitor an individual's behaviour (European Commission 2010).

In response to these concerns, European policy makers have called for the recognition of a "right to be forgotten," which would provide individuals with a legal mechanism to have their personal information permanently removed from online databases (ibid.). This right has already been exercised in a number of European jurisdictions, as Spanish and Italian authorities have demanded the removal of content from Google on the grounds that the information infringed on the privacy of their respective citizens (Bennett 2012).

Many commentators have confronted the right to be forgotten, arguing that it is inconsistent with the fundamental values of freedom of expression and freedom of the press. Others have also suggested that the EU approach could create a "property right in information," producing a "bureaucratic nightmare which might interfere with business demands for data" (ibid., 166).

Contemporary Issues: Privacy and the Right to Be Forgotten

The Permanency of Data

There are two major points of contention around the right to be forgotten. The first is a technical problem built into the way that data is disseminated and stored on the Internet. Information cannot easily be deleted from the Internet once it has been uploaded, replicated, propagated and stored on multiple Internet servers. When a user uploads information to the Internet, a copy of the material is cached and can become accessible via web searches on a potentially permanent basis, making information easily searchable and duplicated by others (Australian Human Rights Commission 2014). Therefore, this technical feature of the Internet can significantly undermine the utility of a court ordering the removal of material from the Internet.

Universal Access and Other Fundamental Rights

The second point of contention surrounding the right to be forgotten is based on the principle of universal access. Universal access to information is one of the greatest virtues of the Internet, but it raises a number of important privacy concerns regarding the content of the data. Often, these privacy concerns are at odds with other fundamental rights, such as the freedom of speech. For example, forcing companies to block search results without any person or court overseeing the context in which content is appearing could be seen as a restriction on free speech. A worthy question policy makers should consider is "if an individual wants their personal data to be removed, and if there is no legitimate reason for keeping it, should it be removed?" (Walker 2012).

Works Cited

Australian Human Rights Commission. 2014. "Some Regulatory Challenges." www.humanrights.gov.au/publications/background-paper-human-rights-cyberspace/6-some-regulatory-challenges.

Bennett, S. C. 2012. "The Right to Be Forgotten: Reconciling EU and US Perspectives." *Berkeley Journal of International Law* 30 (1): 161–95.

European Commission. 2010. "Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee, and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union." http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

Walker, R. K. 2012. "Note: The Right to Be Forgotten." *Hastings Law Journal* 64 (101): 257–86.

3.3 Freedom of Expression and Freedom of Assembly Online

Background

The discussion on freedom of expression on the Internet has been a contentious policy area, especially in terms of Internet censorship. On the one hand, the Internet is an incredibly powerful communication platform that gives individuals and groups a vehicle to exercise their rights. On the other hand, this shift in communicative power has "spawned greater efforts to restrict and control information and communication on moral, cultural, and political grounds" (UNESCO 2012). This has largely been driven by both a need to "improve the quality and security of services, such as screening out spam emails and viruses," as well as a need to block content deemed inappropriate by society (ibid.). The nature and degree of legitimate targets of online censorship vary significantly, depending on the actor and the cultural or political character of the state where it occurs.

Contemporary Issues

Online Censorship

Internet censorship has been on the rise. In 2007, the OpenNet Initiative reported that only a few governments were censoring online content, but today, OpenNet estimates that more than 40 countries are doing so (cited in UNESCO 2012). While there can be legitimate reasons for actors to filter content, determining what is filtered, how it is filtered, who it is filtered by and for what purposes are important questions that need to be considered.

Governments and private information intermediaries can block and censor information for a variety of reasons. Often, it is not clear to what extent these actors actively engage in blocking access to materials on the Internet. Filtering methods can be applied at various points throughout the network by various actors along the chain. ISPs can restrict access to specific content through a number of technical measures, such as IP blocking, DNS tampering and URL blocking by using a proxy. Content providers can also employ content restriction techniques, by removing search results from a search engine or issuing take-down notices (OpenNet Initiative 2014). However, these Internet filtering technologies have been criticized for being prone to over-blocking, which can inhibit freedom of speech, as well as under-blocking, which raises questions about their effectiveness (OECD 2010).

It is important to note that protecting certain human rights or freedoms often has a direct and immediate impact on other rights and freedoms. Internet freedom is complex: filtering content might cause conflict between the right to freedom of expression and rights to dignity and reputation, rights to safety, intellectual property rights, the right to innovation, respect for privacy, and freedom of association and belief and the right to work. It is important, therefore, to ask how online rights should be weighed against each other when they conflict.

Works Cited

OECD. 2010. "Workshop Summary: 'The Role of Internet Intermediaries in Advancing Public Policy Objectives.'" www.oecd.org/sti/ieconomy/45997042.pdf.

OpenNet Initiative. 2014. "Overview of Internet Censorship." https://opennet.net/about-filtering.

UNESCO. 2012. "Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet." http://unesdoc.unesco.org/images/0019/001915/191594e.pdf.

Suggested Readings

UNHRC. 2011. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

Nash, V. 2013. "Analyzing Freedom of Expression Online." In *The Oxford Handbook of Internet Studies*, edited by William Dutton. Oxford: Oxford University Press.

3.4 Differentiating Cybercrime and Cyber Protest

Background

The Internet is an increasingly vital medium for political speech and action, including protest. Democratic societies and international human rights law provide a significant degree of latitude for such activity, even though it can sometimes be offensive and even disruptive. As additional measures to facilitate cooperation on investigating and prosecuting cybercrime are contemplated, concerted efforts are advisable to consider whether these may have chilling effects on political speech and action.

Hacktivism is defined as the "non-violent use for political ends of illegal or legally ambiguous digital tools like website defacements, information theft, website parodies, DoS attacks, virtual sit-ins and virtual sabotage" (Hampson 2012). Particular hacktivist groups, such as Anonymous, have attracted media attention for taking direct digital action against governments and corporations, shedding light on issues ranging from free speech on the Internet, to publicizing rape cases and assisting in the so-called Arab Spring (Coleman 2013).

In popular media, hacktivism sometimes carries a negative connotation. However, the range of hacktivist activities exists on a scale: at one end, forms of hacktivism exploit illegal access to networks causing extensive damage or harm; while at the other end, forms of hacktivism are primarily used to advocate for political or social change,

with little to no damage or harm. Calibrating legal regimes to account for such differences, at least in sentencing, may be advisable in order to balance mutually legitimate, yet sometimes conflicting societal values.

Contemporary Issues

In most developed countries, laws generally prohibit hacktivism. However, these countries also protect the right to protest as an essential element of free speech. Hackers and technologists can play an important role in whistleblowing and in the communication of citizen preferences and views to policy makers. However, many national governments still treat all hacktivism as straightforwardly criminal. Such a stance imposes significant costs on citizens contemplating online political speech or action.

Works Cited

Coleman, G. 2013. *Anonymous in Context: The Politics and Power Behind the Mask*. CIGI Internet Governance Papers No. 3. Waterloo: CIGI. www.cigionline.org/sites/default/files/no3_8.pdf.

Hampson, N. C. N. 2012. "Hacktivism: A New Breed of Protest in a Networked World." *Boston College International and Comparative Law Review* 35 (2): 511–42. http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1685&context=iclr.

Suggested Readings

Sauter, M. 2013. "The Future of Civil Disobedience." In "Internet Monitor 2013: Reflections on the Digital World." http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366840.

3.5 Protecting Vulnerable Populations Online

Background

Most discussion related to Internet safety has been primarily concerned with youth. However, other kinds of populations are also vulnerable to an array of harmful content, including depictions or representations of violence and self-harm, pornography, discrimination and racism, as well as harmful behaviours, such as grooming, bullying, harassment, hate crime and stalking.

Contemporary Issues: Protecting Vulnerable Populations

Hate Speech

The Internet can be a platform for spreading democratic principles and sharing differing ideas and opinions. However, it can also be used as a vehicle for disseminating hate speech. Legal treatments of hate speech vary, with some jurisdictions viewing it as a negative but unavoidable consequence of free and open spaces, and other jurisdictions treating it as a serious criminal matter. For example, the United States encourages the free and open exchange of ideas online, while Germany directly blocks hate speech on the Internet. The main questions policy makers need to ask are: Should we monitor and control hate speech online? If so, how can a balance be found between attempts to protect vulnerable populations while ensuring a culture of vibrant expression?

Sexual Exploitation, Abuse and Child Protection

Child protection has been one of the most contentious debates around freedom of expression online. It is important, however, to note that not only children are at risk online. The use of the Internet for the recruitment, advertisement and sale of men, women and children is a global issue that has grown exponentially as a result of Internet technology. There are many vulnerable individuals that can be targeted and exploited sexually online. This raises a number of important questions: how much regulation is enough regulation when it comes to protecting vulnerable populations online; whether enforcement should be performed exclusively by law enforcement agencies or done in partnership with private Internet intermediaries; and how can the Internet's infrastructure create an environment where regulation can be efficient and effective?

Suggested Readings

Office for Democratic Institutions and Human Rights. 2010. "Incitement to Hatred vs. Freedom of Expression: Challenges of Combating Hate Crimes Motivated by Hate on the Internet." www.osce.org/odihr/68750.

Institute of Health Economics. 2010. "Sexual Exploitation of Children and Youth Over the Internet: A Rapid Review of the Scientific Literature." www.ihe.ca/documents/Online%20Sexual%20Exploitation.pdf

Polaris Project. 2014. "Internet Based Human Trafficking." www.polarisproject.org/human-trafficking/sex-trafficking-in-the-us/internet-based.

3.6 Economic Liberties Online

Background

The Internet is not only a platform to express social rights, such as freedom of speech or freedom of assembly, but can also be used by individuals to express or carry out their basic economic rights. The UN International Covenant on Economic, Social and Cultural Rights recognizes various rights that can be applied to the Internet and other ICTs.

The Internet has become an important tool for conducting business. Companies use email to communicate with partners and customers, web pages to advertise and sell products, and cloud servers to maintain business databases. Article 6 of the covenant recognizes that "everyone has the right to work, which includes the right of everyone to the opportunity to gain his living by the work which he freely chooses or accepts" (UN 1976).

The Internet has also become an important platform for innovation, as individuals and corporations create new products and advertise them online, develop software and applications for users to download, or create images, stories or music and share them online. In the age of Web 2.0, innovation and creativity online has grown exponentially, as many popular websites rely on users to create, upload and share their work and ideas. These platforms and applications have become an important part of cultural life, as individuals share and connect with each other. Article 15 of the covenant states:

1. The States Parties to the present Covenant recognize the right of everyone:
   (a) To take part in cultural life;
   (b) To enjoy the benefits of scientific progress and its applications;
   (c) To benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.
2. The steps to be taken by the States Parties to the present Covenant to achieve the full realization of this right shall include those necessary for the conservation, the development and the diffusion of science and culture.
3. The States Parties to the present Covenant undertake to respect the freedom indispensable for scientific research and creative activity.
4. The States Parties to the present Covenant recognize the benefits to be derived from the encouragement and development of international contacts and co-operation in the scientific and cultural fields (ibid.).

Contemporary Issues

Online Payments

Purchasing products online or making donations to non-profit organizations through major credit companies such as PayPal, MasterCard or Visa are now commonplace activities in many countries. These services not only help businesses and other organizations reach a larger audience, but they also make it easy for individuals to buy products or donate money. Prevention of access to these services should be understood as entailing significant restrictions on the economic rights of affected individuals and organizations. In December 2010, PayPal, MasterCard and Visa refused to accept donations made to WikiLeaks when it released a number of leaked classified documents to the public. By blocking online payment systems, individuals may not be able to fully express their economic or social rights online.

Right to Innovate

According to the Covenant on Economic, Social and Cultural Rights, all individuals have a right to innovate and benefit from their innovations (UN 1976). However, these rights often come into contention in the age of Web 2.0 applications. Users will often mix, rip and burn content online, creating potential conflict with copyright holders. Copyright contentions online are further debated in terms of development and access to knowledge. Going forward, policy makers will need to consider how to balance the rights of copyright holders and users, so that users can continue to make fair use of works and exercise their right to creative activity, and copyright holders can

benefit from their contributions to society. Lack of access to high-quality broadband also threatens enjoyment of the right to innovate, by shutting disadvantaged individuals out of modern markets and innovation ecosystems.

Works Cited

UN. 1976. *International Covenant on Economic, Social and Cultural Rights*. www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx.

3.7 The Right to Access the Internet

The Internet has become an essential platform for exercising individual human rights. Therefore, having access to the Internet is a particular concern. Barriers to access can exist for a number of reasons, such as a lack of Internet infrastructure, high costs or digital illiteracy. Some groups of people are more prone to facing these access barriers than others. It is important that policy makers and stakeholders recognize these challenges so that, in the future, the Internet can continue to be an open platform that promotes human rights for all segments of society.

3.7a Women and the Internet

Background

In many developing countries, there are huge disparities between men and women in terms of Internet access. According to a study published by Intel Corporation (2012), nearly 25 percent fewer women and girls are online compared to men and boys. This disparity grows wider in poorer regions, like Sub-Saharan Africa where approximately 43 percent of women do not have access to the Internet (ibid.). Women in many developing countries are also less likely to use the Internet for business purposes than men, and often lag in terms of overall digital literacy.

The Internet is a catalyst for fostering digital inclusion among women, which can improve gender equality across a variety of social, economic and political dimensions. The Internet also empowers women and girls by: giving them a voice to effectively participate in political processes; providing them with access to resources to educate themselves and their children; giving them opportunities to improve their own health and the health of their families and communities; and providing a forum for starting their own businesses or to help keep them safe (ibid.).

Contemporary Issues

Reducing Costs

Communities, and especially women, need access to affordable broadband services and the equipment and training necessary to utilize it. High Internet prices "disproportionately impact women compared to men, as women have lower incomes and often have less control over spending" (Broadband Commission 2013). More affordable prices will play a significant role in reducing the digital gender gap. There are ways to achieve cost reductions through public support, "such as increasing tele-centres, libraries, and community services centres" (UNESCO 2012). National policy making that considers gender can also help lower costs for women who wish to access the Internet. However, most national governments do not have gender considerations in their ICT policies.

National Policy Making

Gender concerns are largely absent from ICT policies, just as ICT is largely absent from gender policies. The Broadband Commission (2013) recently found that only 30 out of 119 (29 percent) countries included a reference to gender in their National Broadband Plan. Many states are not treating affordable, pervasive access as a basic right for the entire population. There is a need to prioritize gender equality issues at all levels of policy making.

Works Cited

Broadband Commission. 2013. "Doubling Digital Opportunities: Enhancing the Inclusion of Women and Girls in the Information Society." www.broadbandcommission.org/Documents/working-groups/bb-doubling-digital2013.pdf.

Intel Corporation. 2012. "Women and the Web." www.intel.com/content/dam/www/public/us/en/documents/pdf/women-and-the-web.pdf.

UNESCO. 2012. "Community Information and Technology Centres: Focus on South East Asia." www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/programme_doc_telecentre_study_en.pdf.

3.7b Persons with Disabilities

Background

International organizations, national governments, companies and the technical community all play an important role in ensuring that people with disabilities can access and use ICT. Internationally, the United Nations Convention on the Rights of Persons with Disabilities recognizes that access to information and communication technologies can enable persons with disabilities to participate more fully in life (ISOC 2012).

Through the legislative process, national governments play an important role in increasing access for persons with disabilities and a number of countries have created specific legislation to promote accessibility online. For example, the US government has incorporated accessibility into public procurement policy, which encourages ICT manufacturers to supply products that are more accessible. As a result, products from companies such as Microsoft and Apple are now designed to be accessible (ibid.).

The technical community also plays an important role in increasing accessibility for persons with a disability by setting standards that form the basis of user interaction with ICT. The IETF has developed several frameworks for improving accessibility, such as real-time text, which enables a person with a hearing impairment to communicate by text in real time. The W3C has also developed guidelines on making Web content as accessible as possible (ibid.).

Contemporary Issues

For an individual with a disability, accessibility means "being able to use a product or service as effectively as a person without a disability" (ibid.). However, when it comes to the Internet and the various applications made available through new technologies, persons with disabilities will face different barriers as there are various degrees and types of disabilities. For example, "an individual with a visual impairment who uses screen reading software may be confronted by a website that has confusing navigation, or that lacks descriptions of images, while a [person with a] hearing impairment may be unable to participate in online conferencing because it lacks captioning" (ibid.). While there have been many positive developments in terms of making technology accessible, there are still many challenges, which require raised awareness and innovation by relevant actors.

Works Cited

ISOC. 2012. "Internet Accessibility: Internet use by persons with disabilities: Moving Forward." www.internetsociety.org/sites/default/files/bp-accessibilitypaper-20121105-en.pdf.

3.7c Digital Literacy

Background

Digital literacy is how people make, understand and share meaning on a digital platform. It incorporates a wide range of interrelated skills that fall under literacies such as ICT literacy, media literacy, visual literacy and communication literacy (Canadian Internet Forum 2010). Although there is no single universal definition of digital literacy, the concept is built upon three principles: the skills and knowledge to use a variety of digital media software and hardware; the ability to understand digital media content and applications; and the knowledge and capacity to create with digital technology (ibid.).

Having the hardware to connect to and use the Internet and other ICTs is only meaningful for an individual if they have the knowledge and skills required to use them. Unlike traditional communication technologies, the Internet is user-driven. It stimulates creativity and new opportunities that can lead to innovation and growth, and can improve productivity for individuals and businesses. In addition, it provides a wealth of knowledge that can improve all aspects of human well-being. However, many people lack the knowledge and skills necessary to use the Internet and other ICTs, limiting their ability to take advantage of this technology and improve their lives.

Contemporary Issues

Expanding Digital Literacy

In both the developed and developing worlds, digital literacy is a barrier to Internet access for different segments of the population. The elderly and the poor are particularly vulnerable. Often, these populations do not have access to ICTs, or the time to learn how to use them. This is further complicated when ICTs are manufactured in languages that are not native to an individual's state. It is important for policy makers to recognize that access requires an expansion of infrastructure, content and devices that are internationalized, as well as services that teach people the skills they need to use ICTs to their full potential.

Works Cited

Canadian Internet Forum. 2010. "Digital Literacy Consultation Backgrounder." www.cira.ca/assets/Uploads/wp-cif-digital-literacy-backgrounder.pdf.

Section 4:
Current Internet Governance Ecosystem

4.1 The Governance Role of Private Sector Actors

4.1a Network Operators and Content Intermediaries

Background

Network Operators

Network operators are companies or organizations that operate the networks that collectively make up the global Internet. These include ISPs, cellular providers, content-distribution networks, cable companies and others. Because network operators have a physical presence, they must interact with the national authorities in the jurisdictions in which they operate (Kurbalija 2012). Since network operators, such as ISPs, are the closest connection between the end-user and Internet content, they play an important role in enforcing legal rules on the Internet. In the past few years, states have controversially begun to assign governance responsibility to network operators, raising questions of accountability and creating compliance costs for those firms (ibid.).

Content Intermediaries

Internet content intermediaries such as Facebook, Google and Twitter perform a number of Internet governance functions related to IPR enforcement, privacy and data protection. Increasingly, large content intermediaries, such as Google and Facebook, are developing their own infrastructure to deliver Internet content (and especially their own content) to end-users (Wholson 2014).

Contemporary Issues

Intellectual Property

Internet platforms, such as YouTube and Facebook, allow users to broadcast themselves and share their work across a variety of media formats. Combined with the "rip, mix and burn" nature of the Internet, this information sharing process often involves the illegal usage of copyrighted materials (Collins 2010). This has drawn certain Internet users into conflict with copyright owners seeking to maintain rights over their work. Because Internet content providers host information that may infringe copyrighted information, they have often been at the centre of this conflict.

Common to all legal systems is the principle that a content intermediary cannot be held responsible for hosting materials that breach copyright if they are not aware of the violation (Kurbalija 2012). Across various legal jurisdictions, the main difference lies in the legal action taken after the content intermediary is informed that the material it is hosting is in breach of copyright: US and EU law employs a Notice-Take-Down procedure, which requests the network operator to remove such material in order to avoid being prosecuted; in contrast, Japanese law employs a Notice-Notice-Take-Down procedure, which provides the user of the material with the right to contest the request for removal (ibid.). These takedown procedures have been criticized for their implications for freedom of expression. Because the notice-take-down system is inexpensive for the copyright holder, the system invites more frequent abuse than a standard copyright adjudication. Under the Digital Millennium Copyright Act, if an individual feels their content was wrongly issued a takedown notice, they can submit a dispute or counter-notice. However, this can be risky and costly for an individual, because issuing a counter-notice or dispute gives the copyright holder the option to sue the individual (Electronic Frontier Foundation [EFF] 2013).

In recent years, there has been increased pressure on network operators to handle copyright enforcement, since their position of gatekeepers between end-users and Internet content places them in the best position to control content. Network operators will employ a number of techniques to monitor what citizens are using their bandwidth for. However, the use of these techniques to monitor copyright compliance has been highly criticized by privacy advocates for infringing on an individual's privacy rights.

Law Enforcement Cooperation and Network Operators

While law enforcement officials can work with network operators to help track down criminals, several governments in the developed world have been introducing bills that give police the ability to ask for subscriber information without a warrant (CBC 2012). This raises privacy and human right concerns relating to the adequacy of oversight mechanisms and judicial review procedures.

While governments maintain that the kind of information law enforcement officials would get would be no different than what is found in the public phonebook, privacy advocates argue that in the age of big data and interconnectedness, law enforcement officials could easily track an individual's movement and learn more about their behaviours.

Monopoly

In countries with telecommunication monopolies, it is common for incumbent operators to also provide Internet access. However, telecommunication monopolies are often criticized for precluding other ISPs from entering the market, inhibiting competition (Kurbalija 2012; Southwood 2014). The lack of competition often results in higher prices and lower quality of service, which can exacerbate the digital divide. In some cases, telecommunication monopolies tolerate the existence of other network operators, but "interfere at an operational level, such as providing lower bandwidths or causing disruptions in services" (Kurbalija 2012).

Traffic Shaping

Network management techniques are often employed by network operators to shape and prioritize certain Internet traffic, such as online games, video calls or streaming video. These techniques include: throttling bandwidth-intensive traffic; inhibiting competing services; or blocking content, applications and services at the request of governments. Network operators often argue that these techniques are important for improving the user experience. For example, network operators will often give Internet traffic carrying voice conversation over VoIP services priority over traffic carrying a simple email; while a user can hear delays in VoIP services, they won't notice a minor delay in email exchange. However, proponents of net neutrality argue that "all bits are created equal" and that Internet traffic must be treated equally (ibid.). Network operators continue to challenge this view, arguing that "it is the users who should have equal access to Internet services and if this is to happen, Internet traffic cannot be treated equally" (ibid.).

ToS Agreements

ToS agreements outline the relationship between the user and the network operator or the content intermediary. In many cases, ToS agreements are restrictive for the user. Often, they give content intermediaries and network operators permission to collect, store and share an individual's data. In many cases, the ToS can be changed at any time and users can be disconnected from services for various reasons. ToS agreements can also allow network operators to block content at their discretion. These rules can have implications for a user's privacy, as well as Internet censorship and universal access. However, there are no basic consumer protection rules when it comes to regulation of network provider ToS agreements. While it is important to recognize that content intermediaries provide users many online services free of monetary cost in exchange for rights to collect and use data, one should ask whether or not ToS agreements should be allowed to insert or enforce provisions that put individual privacy and security at risk (Bradshaw, Harris and Zeifman 2013).

Some grassroots campaigns have attempted to push for more transparency and fairness in user agreements. For example, the "Terms of Service; Didn't Read" project aims to create a database that analyzes the fairness of user agreements from Internet content providers. The project employs a crowd-sourcing approach, inviting individuals to submit ToS agreements for consideration in a Google Group. Other initiatives include the Swedish "CommonTerms" website, which advocates for agreements to be explained through a standard set of privacy icons instead of lengthy, hard-to-read documents. Another initiative called "TOSBack" tracks the changes a website makes to their terms, which can be updated as often as once a month for major content platforms such as Facebook (Luckerson 2012).

Data Sales

Internet content providers often employ a variety of tools to collect unique data about their customers, such as HTTP cookies, flash cookies, location, cellular number, web bugs and globally unique identifiers (Bradshaw, Harris and Zeifman 2013). This information is used for customized delivery of online advertisements and frequently shared with third parties over the Internet. This exchange is often done without the individual's knowledge about where the data will end up and for what purposes it will be used. The resale of data in tertiary markets is also a major concern, as it greatly inhibits an individual's ability to access their data, verify its contents and ask for removal (ibid.).

Works Cited

Bradshaw, S., K. Harris and H. Zeifman. 2013. "Big Data Big Responsibilities: Recommendations to the office of the Privacy Commissioner on Canadian Privacy Rights in a Digital Age." CIGI Junior Fellows Policy Brief No. 8. www.cigionline.org/sites/default/files/no8_0.pdf.

CBC. 2012. "Online Surveillance Bill Targets Child Porn." CBC News, February 14. www.cbc.ca/m/touch/world/story/1.1196827.

Collins, S. 2010. "Digital Fair: Prosumption and the Fair Use Defence." *Journal of Consumer Culture* 10 (1): 37–55.

EFF. 2013. "A Guide to YouTube Removals." www.eff.org/issues/intellectual-property/guide-to-youtube-removals.

Kurbalija, J. 2012. A*n Introduction to Internet Governance*. Geneva: DiploFoundation. www.diplomacy.edu/IGBook.

Luckerson, V. 2012. "New Site Grades Those Pesky Terms of Service Agreements You Never Read." *Time Magazine*, August 20. http://business.time.com/2012/08/10/new-site-grades-those-pesky-terms-of-service-agreements-you-never-read/.

Southwood, R. 2014. "We Name Africa's Telecom Delinquents." *Tech Central*. www.techcentral.co.za/we-name-africas-telecoms-deliquents/46200/.

Wholson, M. 2014. "Facebook Drones to Battle Google Balloons in the War of Airborne Internet." *Wired*. www.wired.com/business/2014/03/facebooks-drones-launch-race-airborne-internet/.

Suggested Readings

ISOC. 2012. "Internet Interconnections: Proposals for New Interconnection Model Comes up Short." www.internetsociety.org/sites/default/files/Internet%20Interconnections%20Proposals%20For%20New%20Interconnection%20Model%20Comes%20Up%20Short.pdf.

4.1b RIRs, TLD Registries and ccTLD Registries

Background

RIRs

RIRs are private, non-profit organizations responsible for the distribution and management of IP addresses in specific regional areas. Each device connected to the Internet has a unique IP address, either assigned permanently or assigned temporarily for a session. IP addresses are allocated from the IANA to RIRs for distribution. RIRs will allocate or assign these numbers as required to various network operators, government bodies, educational institutions and private enterprises. Currently, there are five RIRs that operate independently in the management of IP addresses. These organizations are: The American Registry for Internet Numbers; Latin America and Caribbean Network Information Centre; Asia-Pacific Network Information Centre; Reseaux IP Europeens Network Coordination Centre; and African Network Information Centre.

TLD Registries

TLD registries are responsible for maintaining a database of names and associated IP address for every domain name registered within a given TLD. The IANA delegates authority for overseeing each global TLD to registry operators. For each TLD and gTLD (such as .com or .org) and for each country code TLD (such as .ca or .ch) there is a registry operator. For example, VeriSign, Inc. operates the .com and .net domains (among others), and a non-profit organization called EDUCAUSE has long maintained the authoritative mapping information for the .edu domain and also assigns domains in the .edu space. Some of these registry operators are also domain name registrars, meaning they assign domain names to individuals and institutions requiring these names (DeNardis 2014).

ccTLD Registries

ccTLDs are two-letter Internet TLDs designated for a particular state. Examples include .ca, .uk and .jp. In many countries, extensive use is made of the ccTLD, while in other countries most domain name registrations are under gTLDs (such as .com and .org) rather than ccTLD. Some ccTLDs are in demand for use outside of their home country because their name can be used as a part of a commercially meaningful phrase. As a result, some smaller countries have opened up

their ccTLDs for worldwide commercial purposes. For example, Tuvalu has partnered with VeriSign to sell domain name registrations using the .tv ccTLD for television stations.

Contemporary Issues

ccTLD Administration

Most ccTLD registries are local non-profit organizations responsible for administering and operating a ccTLD in compliance with local or regional legislation. ICANN has formal agreements with a few ccTLDs; however, the relationship between ICANN and ccTLD registries mostly operates under codes of best practices, such as ICANN's Accountability Framework document and ICANN's Country Code Names Supporting Organization.

During the 2005 World Summit on the Information Society, the Tunis Agenda recognized that "governments have legitimate interests in the management of their respective ccTLDs" (OECD 2006). However, most ccTLDs are managed in the interest of the local community and in compliance with local or national laws. Policy makers must ask whether or not governments should have more authority over their respective ccTLD. Some stakeholders have argued for more oversight and similarity in the governance of ccTLDs, not only from national governments but from ICANN, to help improve accountability and legitimacy. In contrast, other stakeholders argue that the present governance model strengthens the ccTLD community by allowing ccTLDs to reflect local requirements, without any "one-size-fits-all" rules (ibid.).

Domain Name Trademark Disputes

Domain name trademark disputes have arisen since the development of the World Wide Web. Part of the contemporary problem is that "there is no direct connection between the system for registering trademarks, which is territorially nation-bound and publicly administered, and the system for registering domain names, which is privately administered with no ex ante consideration of trademark rights" (DeNardis 2014). Not surprisingly, trademark disputes have represented a significant policy controversy for the domain name administration.

Shortly after the inception of the Web, academics and legal experts started asking what the appropriate legal remedies for dealing with trademark-infringing domain name registrations would be and whether or not domain name registrars would assume any responsibility for infringement. Domain name trademark disputes are a complicated problem for Internet governance: in trademark law, it is possible for two registered trademarks to be identical if they are registered as different classes of goods or services. However, this does not translate into the Internet environment, where each domain name must be globally unique (ibid.).

In order to address contemporary trademark disputes, ICANN has established an arbitration procedure called the Uniform Domain-Name Dispute Resolution Policy (UDRP). The UDRP arose initially from a United States Commerce Department proposal after an international consultation by World Intellectual Property Organization. When a registrant applies for a domain name, he or she must declare that the domain name they are applying for does not infringe on the rights of a third party. The registrant must also agree to participate in an arbitration process if a third party comes forward with a claim. A dispute is usually required to be resolved by agreement, court decision or arbitration before the registrar of the domain name will cancel or transfer the domain name in question. However, if the dispute is viewed to be an "abusive registration," the third party can submit their claim through an "approved dispute-resolution service provider," or they can file a complaint in a jurisdictionally appropriate court (DeNardis 2014).

The UDRP has been criticized because it was not formed through the same type of deliberative international construction that gives legitimacy to other types of global governance institutions, often undergoing ratification by multiple nations' legislative bodies (ibid.). However, advocates of the system argue that the nation-state deliberative governance approach would have taken years, giving free reign to domain name trademark violations in the interim. A second criticism of the UDRP takes aim at the "approved dispute-resolution service provider" system, suggesting that trademark holders "forum shop" and use the service providers most likely to rule in their favour. However, advocates suggest that the UDRP is still a relatively recent and evolving system of trademark governance, and despite the criticism against its constitution and operations, advocates suggest that it has provided much quicker and much less expensive global resolution of trademark disputes than litigation, particularly considering the cross national complications

of such litigation (ibid.). Going forward, policy makers will have to consider if the UDRP is an appropriate forum for dealing with trademark and domain name issues, and whether or not improvements can be made to the current system.

Works Cited

DeNardis, L. 2014. *The Global War for Internet Governance*. London: Yale University Press.

OECD. 2006. "Evolution in the Management of Country Code Top-Level Domain Names." www.oecd.org/internet/ieconomy/37730629.pdf.

Suggested Readings

ITU. 2013. "IPv4 and IPv6 Issues." www.itu.int/en/wtpf-13/Documents/backgrounder-wtpf-13-ipv4-ipv6-en.pdf.

4.1c International Coordination of State-Firm Relations

Background

Within a state, national governments will regulate corporations that operate within their jurisdiction to ensure adequate competition and good practices. However, this traditional understanding of state-firm relationships is challenged by the rise of multinational corporations that operate in various jurisdictions across the world. These challenges are further complicated by information and telecommunication companies, who not only operate in various legal jurisdictions, but operate in a realm where rules are highly fragmented. Broadly speaking, states interpret and apply national laws around hate speech, defamation and Internet censorship in different ways. After the recent cyber espionage revelations, some states are becoming more sensitive about data privacy issues and have been pushing for restrictions on the business models of technology companies that monetize user information. Others do not want to put a strict limit (or any limit) on data aggregation and retention practices, because these activities are vital for their security and law enforcement functions. As a result, current state-firm relations are in flux. This contestation is two-sided: while governments look to assert greater control over Internet policy issues, technology companies have pushed back. In particular, seven major American ICT firms (AOL, Facebook, Google, LinkedIn, Microsoft, Twitter and Yahoo) have called for limitations and oversight when governments collect user information (see Reform Government Surveillance 2013). These major corporations are now lobbying the government, to help re-establish their legitimacy across the numerous jurisdictions in which they operate.

Contemporary Issues

Regulatory Issues

Internet firms face different regulatory constraints in the various states in which they operate. This increases the compliance costs for these corporations. For example, privacy laws pertaining to the collection and retention of data about individuals could conceivably require corporations to administer multiple web forms for users subject to different jurisdictions, and even build and maintain different data storage centres in various locations with different levels of security (Raymond 2013). In some cases, complying with all the relevant legal regimes may become impossible and necessitate withdrawing from some markets (ibid.). In other cases, it can create public relations dilemmas or challenge a corporation's core operating values and norms. Firms may face issues of this kind when they comply with censorship requests from relevant national authorities.

Judicial Issues

Once laws are established, they are then applied by the courts. This can cause further complexities for state-firm relations because different legal regimes will interpret and apply laws differently across jurisdictions, and laws are constantly changing as new precedents are set and courts discover gaps in, and unintended consequences of, legislation. Because Internet firms operate across various jurisdictions, this raises the question of whether there needs to be some level of international coordination, while also responding to local and regional judicial systems. However, there also needs to be room to apply laws based on local practices and values.

Works Cited

Raymond, M. 2013. "Internet Governance From the Bench." CIGI Commentary, June 17. www.cigionline.org/publications/2013/6/internet-governance-bench.

Reform Government Surveillance. 2013."Global Government Surveillance Reform." www.reformgovernmentsurveillance.com/.

4.2 The Governance Role of Public Sector Actors

4.2a The State

Background

For some countries, public officials have been involved in a variety of Internet governance activities, from participating in the various standards-setting fora to the establishment of IXPs. For other countries, public officials have lacked the technical knowledge and skills necessary to participate in these Internet governance mechanisms. For these states, constraints such as simultaneously training officials, developing policy and actively participating in the various international fora are becoming less significant, as more states continue to build capacity and participate in various Internet governance activities.

Mainly, states participate in Internet governance through the development of national legislation, covering a diverse set of issues such as privacy, data protection, intellectual property, cybercrime, cyber espionage and censorship. States also act as regulators of Internet-based firms by enforcing competition and antitrust policies.

The role of the state is a recurring theme throughout this briefing book, as it plays a critical role in shaping the governance of all relevant issues. However, the multi-stakeholder model, the speed at which Internet technology changes and the Internet's borderless nature challenge the autonomy and capacity of national governments to effectively govern aspects of the Internet that have direct impact on the economic and social aspects of the state.

Going forward, the precise role and authority of the state with regard to Internet governance will ultimately need to be determined by policy makers and other stakeholders within the context of a multi-stakeholder approach.

4.2b Regional Trade Agreements

Background

The Internet plays an important role in global economic growth. As more firms operate online and do business in a variety of national jurisdictions, regional trade agreements are becoming an important source of rules for Internet governance.

ACTA

ACTA was a regional trade agreement that aimed to establish international standards for IPR enforcement in areas such as medicine, counterfeit goods and copyright infringement on the Internet. Although ACTA was eventually rejected, many elements of it have been carried into the two major regional trade agreements discussed below.

TTIP

The TTIP is a free trade agreement that is currently being negotiated between the United States and the European Union. Although the TTIP is colloquially known as a trade agreement, its primary focus is regulatory barriers, not lowering tariffs (Alden 2014). This is why the TTIP is important for various stakeholders in Internet governance, due to its provisions related to data flows and data protection. US tech companies have lobbied the American government to create "a single global digital information marketplace" (Chester 2013). However, after the allegations of the NSA spying on European institutions and politicians, EU data concerns have escalated. This has led some EU commentators and politicians to call for the suspension of continued TTIP talks.

TPP

The TPP is a multinational trade agreement that is aimed at expanding the flow of goods, services and capital across borders. It is currently being negotiated by 12 nations, namely the United States, Japan, Australia, Peru, Malaysia, Vietnam, New Zealand, Chile, Singapore, Canada, Mexico and Brunei Darussalam. Like the TTIP, the TPP is an important trade agreement for various Internet governance stakeholders, particularly as it will include an important chapter on IPRs, as well as provisions on encouraging transborder data flows.

Contemporary Issues

IPRs and Internet Governance

The leaked intellectual property chapter of the TPP proposed reforms to patents, copyright, trademarks, civil liberties and liability of ISPs. Many Internet freedom organizations have criticized the chapter, saying that proposals would restrict innovation and force Internet service providers to police copyright. A few of the controversial TPP provisions that are listed are (cited in EFF 2013):

- Expanding copyright terms: Create copyright terms that will extend copyright ownership from the life of the author +50 years, to life of

the author +70 years and 120 years after creation for corporate owned works (such as Mickey Mouse).

- Regulate temporary copies: Treat temporary reproductions of copyrighted works without copyright holders' authorization as copyright infringement. This is incompatible with modern routing and interconnection practices, as all computers and networks rely upon the creation of temporary copies of programs and files.
- Adopt criminal sanctions for copyright infringement done without a commercial motivation.
- Expand ISP liability by providing legal incentives for ISPs to enforce copyright protection rules.

Policy makers will need to determine what governance function (if any) regional trade agreements should play for establishing rules around Internet governance issues related to copyright and intellectual property enforcement, the flow of data across borders and other trade-related Internet issues.

Multi-stakeholder vs. Multilateral

One criticism of the TPP negotiations is that it is creating Internet governance rules behind closed doors, which does not fit with the multi-stakeholder approach to Internet governance. Policy makers need to consider whether or not non-governmental stakeholders should be a part of these discussions, and if so, how would they enter these discussions in a meaningful way?

Works Cited

Alden, E. 2014. "How Obama's NSA Reforms Could Help TTIP." *Council on Foreign Relations* (blog), January 15. http://blogs.cfr.org/renewing-america/2014/01/15/how-obamas-nsa-reforms-could-help-ttip/?cid=soc-how_obamas_nsa_reforms_could_help_TTIP-11514.

Chester, J. 2013. "US could Exploit Trade Deal to Expand Spying." Deutsche Welle. www.dw.de/us-could-exploit-trade-deal-to-expand-spying/a-17013629.

EFF. 2012. "Trans-Pacific Partnership Agreement." www.eff.org/issues/tpp.

Suggested Readings

Komaitis, K. 2012. "The Anti-Counterfeiting Trade Agreement (ACTA): Lessons and Outcomes." *ISOC* (blog). www.internetsociety.org/blog/2012/07/anti-counterfeiting-trade-agreement-acta-lessons-and-outcomes.

———. 2013. "Reflections on the Transatlantic Trade and Investment Partnership (TTIP)." *ISOC* (blog). www.internetsociety.org/blog/2013/06/reflections-transatlantic-trade-and-investment-partnership-ttip.

WikiLeaks. 2013. "Secret TPP Treaty: Advanced Intellectual Property Chapter for All 12 Nations with Negotiating Positions." http://wikileaks.org/tpp/static/pdf/Wikileaks-secret-TPP-treaty-IP-chapter.pdf.

4.3 The United Nations

The appropriate role of the United Nations in Internet governance and Internet-related policy issues remains an area of considerable contention. A variety of bodies within the larger UN system have responsibilities pertaining to ICT policy, which at times sits uneasily between these areas. Together, these UN bodies deal with issues pertaining to human rights, development, infrastructure expansion, the promotion of inclusive Internet governance dialogue, e-commerce, intellectual property and cyber security.

The following sections of this briefing book are intended to provide an introduction to these efforts, without presuming an answer as to whether the UN should take a greater role in issues of Internet governance narrowly defined. In any such discussion, strong emphasis must be placed on avoiding unintended damage to the stability, security and end-to-end accessibility of the Internet.

4.3a UNHRC

Background

The UNHRC has 47 member states elected by the UNGA. The purpose of the UNHRC is to strengthen, promote and protect human rights around the world, address human right violations and make recommendations on violations. The UNHRC manages working groups on particular human rights issues and creates Special Rapporteurs for particular human rights

questions. It has played an important role in promoting human rights online, particularly with respect to freedoms of expression, assembly and privacy.

In June 2012, the UNHRC passed the Resolution A/HRC/20/L.13 on the Promotion Protection and Enjoyment of Human Rights on the Internet, affirming that the same rights that people have offline must also be protected online. In addition, the Special Rapporteur on the promotion of freedom of opinion and expression, Frank La Rue, has played an active role in promoting human rights online. In April 2013, he wrote an important report that explored the impact of mass online surveillance on human rights. The report warned that human rights standards have not kept pace with advances in surveillance technology, and argued that states have an obligation to "revise national laws regulating [surveillance] in line with human right standards" (UNGA 2013a). The report formed the basis for further UN discussion on human rights online, particularly in regards to mass surveillance and privacy online. In November 2013, the General Assembly passed Resolution A/C.3/68/L.45/Rev.1, recognizing the Right to Privacy in the Digital Age (UNGA 2013b).

Although these resolutions are non-binding, they provide an important mechanism for establishing international norms online. When states or other actors do not cooperate with the norm, it can be used as a public shaming tool by drawing public attention to human right violations.

Contemporary Issues

UNHRC Membership

On November 12, 2013, the UNGA elected 14 new states to serve on the UNHRC. The composition of the UNHRC matters for drafting and passing resolutions that represent a broad constituency of global values and interests. However, states can exercise their power in a negative way, by either diluting resolutions to suit their needs or by blocking them. Further, they can gain insider access to information regarding state human rights records and monitor what others are saying about their violations. In the end, this can drastically affect the future norms of online rights in ways that go against the visions of liberal democratic states.

Works Cited

UNGA. 2013a. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

———. 2013b. "The Right to Privacy in the Digital Age." www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1.

Suggested Readings

Sengupta, S. 2012. "U.N. Affirms Internet Freedom as a Basic Right." *NY Times Bits* (blog), July 6. http://bits.blogs.nytimes.com/2012/07/06/so-the-united-nations-affirms-internet-freedom-as-a-basic-right-now-what/?_r=0.

UNHRC. 2012. "The Promotion, Protection and Enjoyment of Human Rights on the Internet." www.regeringen.se/content/1/c6/19/64/51/6999c512.pdf.

4.3b UN Development Bodies: UNDP, UNCTAD, UN CSTD and UNESCO

Background

UNDP

The United Nations Development Programme (UNDP) works with states to help them withstand crisis and drive sustainable growth. The UNDP works with governments, civil society, industry and academia to bring information and communication technology to development efforts: as more people are connecting to the Internet, new opportunities for improving health care, agricultural development, political participation, economic development and health care arise. In addition, the UNDP is one of the main international actors that promotes women's rights online, and works with other UN bodies, such as UNESCO and the ITU, to help women gain access to the Internet (UNDP 2013).

UNCTAD

UNCTAD promotes the integration of developing countries into the world economy. UNCTAD works with governments, partners in industry, civil society and academia to bring information and communication technology to education, health and natural disaster management (see UNCTAD 2013). UNCTAD also focuses on how e-commerce and e-business applications can be used by developing countries to participate in global markets. UNCTAD has a number of programs that help developing countries with technical assistance. These programs focus on building capacity on the legal aspects of e-commerce, measuring the information economy and its impact on development, and monitoring trends with regard to ICT access, use impact and related policies.

CSTD

The UN Commission on Science and Technology for Development (CSTD) is a subsidiary body of the Economic and Social Council (ECOSOC). The role of the CSTD is to provide the UNGA and ECOSOC with high-level advice on relevant science and technology issues. Along with other UN organs, the CSTD plays an important role in WSIS action line implementation and WSIS review. In December 2012, CSTD established a Working Group on Enhanced Cooperation (WGEC), to examine the mandate of the WSIS regarding enhanced cooperation as contained in the Tunis Agenda, through "seeking compiling and reviewing inputs from all member states and other stakeholders, and to make recommendations on how to fully implement [the mandate of WSIS]" (UNCTAD 2014a). The WGEC is comprised of 22 member states and five representatives from the private sector, civil society, technical and academic communities and intergovernmental and international organizations (UNCTAD 2014b).

UNESCO

The United Nations Educational Scientific and Cultural Organization (UNESCO) "strives to build networks among nations" (UNESCO 2013). Recognizing that the Internet has the potential to bring countries together, foster sustainable development, build democratic societies, and enhance the free flow of information around the world, UNESCO has played an active role in many international forums such as the Internet Governance Forum (IGF) and WSIS implementation and review. UNESCO has constantly stressed that "the mechanisms of Internet governance should be based on the principles of openness, privacy and diversity, encompassing universal access, interoperability, freedom of expression and measures to resist any attempt to censor content" (ibid.). UNESCO also stresses that the Internet should respect cultural and linguistic diversity. Because of the speed and scale at which new technologies are becoming accessible, the emergence of the Internet as a public network is carving out fresh opportunities to widen public knowledge. However, Internet access is still a large concern in many parts of the developing world. UNESCO plays an important role in addressing issues of access, by actively working with states and non-state actors to address the digital divide.

Contemporary Issues

Incompatibility across International Organizations

As different UN organs work on important and often overlapping issues they risk encountering coordination problems, competition and duplicated efforts. For example, copyright rules established by the WTO may come in conflict when development organizations try to expand norms related to freedom of expression and access to knowledge; or various UN development organizations may inefficiently use resources to by working on overlapping or duplicate issues. Going forward, international organizations will need to be cognizant of these risks, while effectively coordinating their activities to ensure a coherent regime complex.

Works Cited

UNCTAD. 2013. http://unctad.org/en/docs/ecdr2003_en.pdf.

———. 2014a. "United Nations Commission on Science and Technology for Development." http://unctad.org/en/Pages/cstd.aspx.

———. 2014b. "Working Group to Examine the Mandate of WSIS Regarding Enhanced Cooperation as Contained in the Tunis Agenda (Working Group on Enhanced Cooperation (WGEC)." http://unctad.org/en/Pages/CSTD/WGEC.aspx.

UNDP. 2013. "The Internet Gender Gap." www.undp.org/content/undp/en/home/ourperspective/ourperspectivearticles/2013/01/10/the-internet-gender-gap-magdy-martinez-soliman.html.

UNESCO. 2013. "UNESCO and WSIS." www.unesco.org/new/en/communication-and-information/flagship-project-activities/unesco-and-wsis/about/.

4.3c UN GGE

Background

ICTs are reshaping the international security environment, as they are being increasingly incorporated into critical infrastructure and developed as instruments of warfare and intelligence. Recognizing the need to cooperatively address cyber threats and international security, the UNGA has, on three separate occasions, appointed the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security. The first GGE held its meetings in 2004 and 2005; the second group held its meetings in 2009 and 2010; and the third group began its work in 2012 and finished in 2013 (UN GGE 2010). During these meetings, all three groups have examined the existing and potential cyber security threats, and have been exploring cooperative measures to address them.

The most recent GGE, which concluded in July 2013, was composed of experts from 15 countries: Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, the Russian Federation, the United Kingdom and the United States. They produced a landmark consensus report, which affirmed that the UN Charter and existing international law applies to cyber space. Section III (16) of the report released by the GGE states:

> The application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability. Common understandings on how such norms shall apply to State behaviour and the use of ICTs by States requires further study. Given the unique attributes of ICTs, additional norms could be developed over time. (UNGA 2013)

Contemporary Issues

The Next Step Forward

The GGE report on Developments in the Field of Information and Telecommunications in the Context of International Security was a positive first step toward international cooperation on cyber security issues. However, there are a number of questions that need to be answered when moving forward. While the report recognizes a wide range of cyber threats, states a need for international cooperation to ensure peace and stability, and makes recommendations for how states can cooperate, these are only first steps: determining exactly how international law will apply to cyberspace and defining the scope of issues that fall under rules concepts of warfare, crime and espionage will be the next difficult, but important steps for states and policy makers.

Multi-stakeholder vs. Multilateral

Because the GGE is comprised of experts from states, this governance function could be described as multilateral instead of multi-stakeholder — the traditional Internet governance mechanism. Thus, another important issue that policy makers need to consider is whether or not non-governmental stakeholders should be a part of these discussions, and if so, how would they enter the discussions and activities of the GGE?

Works Cited

UNGA. 2013. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." www.mofa.go.jp/files/000016407.pdf.

UN GGE. 2010. "Developments in the Field of Information and Telecommunications in the Context of International Security." www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.pdf.

4.3d IGF

Background

The IGF was established by the UN Secretary-General in 2006 to provide an open and inclusive forum for multi-stakeholder policy dialogue regarding the Internet. Its mandate is to facilitate discussion of the development of open, transparent and inclusive Internet policy by identifying emerging issues and bringing them to the attention of the relevant bodies and the general public. It is a non-decision-making body, but provides an opportunity for various Internet stakeholders to share information and coordinate their activities.

Contemporary Issues

More than a Talk Shop?

The IGF is an open and inclusive forum that brings together different stakeholders for the purpose of dialogue. At the most recent IGF in Bali, and in all previous IGFs, there has been discussion as to whether or not the IGF should become more than a talk shop and develop actionable outcomes. However, there are no standards for who can join and participate in the IGF in any given year. While the IGF is a useful forum that allows different voices to share and debate, should a forum with no restriction on who joins become a key policy-making body? How would the IGF ensure transparency and accountability to all its stakeholders? This may be problematic for many individuals, organizations and governments who wish to participate at the IGF and the policy-making process, but who lack the funds required to travel. Giving the IGF decision-making power would therefore only reflect the views of individuals who can afford to make the trip.

Promoting Inclusiveness and Dialogue in the Multi-stakeholder system

For many individuals, governments and organizations, it is economically unfeasible to travel to the IGF every year. In order to address this issue, the IGF has introduced regional and national IGF initiatives, as well as remote participation as ways to promote openness and inclusiveness. However, this can still be problematic for stakeholders in the developing world. Regional IGF initiatives are still not fully representative. Although voices can be represented through remote or online participation, various parts of the world, due to time differences between where the IGF is located and a participant's home country, may still struggle to participate. Furthermore, there may be less value placed on individuals or organizations that participate online, as well as less opportunity to network, share ideas and promote discussion.

4.3e ITU

Background

The ITU is the key international organization involved in the regulation of telecommunications. It has played an important technical role developing rules for coordination among national telecommunication systems, allocating radio spectrum and managing satellite positioning. It also provides technical assistance to developing countries to help develop and build their Internet and communications infrastructure and capacity. It also plays an important role in setting voluntary technical standards and administering telecommunication-specific international treaties such as the ITRs.

The ITRs facilitate global interconnection and the exchange of telecommunication traffic across national borders. For example, the treaty sets rules around traffic flows between telecommunication networks, international routing, charging and billing between operators and other related issues. The ITRs were previously updated in 1988, at the World Administrative Telegraph and Telephone conference, prior to the commercialization of the Internet. In 2012, the WCIT was held in Dubai, to review and update the old ITRs.

Contemporary Issues

ITRs and the Internet

The proposals put forward at WCIT in 2012 did not gain traction. However, some telecommunication carriers are still concerned that "fair compensation is received for carried traffic by network operators" and "are interested in the prospect of United Nations member states facilitating the development of international IP interconnections" (DeNardis 2014, 224–26). Subsequently, this would place Internet interconnection somewhat under the jurisdiction of the United Nation, giving UN member states influence and oversight into Internet Infrastructure. Some stakeholders have argued that this would fundamentally change the way the Internet works, increasing the cost of Internet access, hindering access to knowledge and information and slow Internet economic development (see Centre for Democracy and Technology 2012). Policy makers will need to ask whether or not Internet technologies should or should not be included in the ITRs. Policy makers will have to consider whether or not telecommunication carriers are fairly compensated by the current model for interconnection, and will have to ask if changing the current model of interconnection will have any effect on fundamental human rights, Internet cost and access, and Internet economic development.

Changing Technologies, the ITRs and the ITU's Role

Some governments prefer the ITU to have a more direct role in Internet governance functions such as naming and addressing, standard-setting, cybercrime and spam. This was made clear when a proposal was made that suggested

that Internet governance should be done by states, and that states should be able to manage their own Internet naming and numbering and establish and implement policy regarding Internet access and traffic. However, an alternate view took the position that the new ITRs should continue to address only traditional international telecommunication traffic that a multi-stakeholder model of Internet governance should continue. Because the ITU's voting rights are exclusively for states, proponents of the multi-stakeholder model often argue that the ITU should not take any action that could extend its jurisdiction or authority over the Internet.

Legal Challenges Posed by Parallel Sets of ITRs

Once the 2012 ITRs enter into force, there will be two treaties simultaneously in force on the same subject matter. This creates a problem governed by Article 30 of the Vienna Convention on the Law of Treaties, which provides in this case that the 1988 ITRs will remain in force between states not party to the 2012 ITRs, as well as between a pair of states in which one state is party only to the 1988 ITRs and the other of which is party to both the 1988 and 2012 ITRs. The key point is that this creates a highly complex legal situation that could create increasing compliance costs for telecom operators and for national governments if the states party to the 2012 ITRs continue to update them over time.

Works Cited

Centre for Democracy and Technology. 2012. "ETNO Proposal Threatens to Impair Access to Open, Global Internet." www.cdt.org/files/pdfs/CDT_Analysis_ETNO_Proposal.pdf.

DeNardis, L. 2014. *The Global War for Internet Governance*. London: Yale University Press.

Suggested Readings

Mueller, M. 2012. "Threat Analysis of ITU's WCIT (Part 1) Historical Context." www.internetgovernance.org/2012/05/24/threat-analysis-of-itus-wcit-part-1-historical-context/.

4.3f UN Guiding Principles on Business and Human Rights and the UN Global Compact

Background

Information and telecommunication firms have enabled individuals to exercise their individual human rights at an unprecedented scale. However, ICT firms also collect an extraordinary amount of personal information, creating significant issues of trust and of corporate social responsibility. Recognizing their human rights obligations, many ICT firms have committed to upholding the UN Guiding Principles on Business and Human Rights (Access Now 2013). According to the Office of the High Commissioner for Human Rights (OHCHR), the Guiding Principles are grounded in recognition of: states' existing obligations to respect, protect and fulfil human rights and fundamental freedoms; the role of business enterprises as specialized organs of society performing specialized functions, required to comply with all applicable laws and to respect human rights; and the need for rights and obligations to be matched to appropriate and effective remedies when breached (OHCHR 2011).

Contemporary Issues

Guiding Principles Limitations

Corporations in many industries have endorsed the UN Guiding Principles and various stakeholders have sought to guide their actual implementation by producing secondary literature and projects that explore the principles. However, the application of the Guiding Principles to ICT has yet to be deeply explored, especially in regards to the third principle (Micek and Landale 2013). Civil society has just begun to fill this gap: Access Now published a report that offers pragmatic steps that ICT firms can take to incorporate the Guiding Principles, particularly the third pillar, into all aspects of their policies and operations (ibid.). While these are important first steps at ensuring ICT firms are responsible towards their consumers in terms of privacy and security, they do not address the underlying problem of corporate data collection and retention that allows different actors, such as states or other firms, to abuse the information.

Expanding the UN Global Compact

The UN Global Compact is a voluntary corporate responsibility initiative. It consists of 10 principles derived from the UDHR, The International Labour Organization's Declaration on Fundamental Principles and Rights at Work, the Rio Declaration on Environment and Development, and the United Nations Convention Against Corruption. Because it is a voluntary initiative, its principles are not legally binding or enforced, and are therefore intended to complement, not substitute, existing regulatory approaches for good business practices. ICT corporations play a large role in data collection, retention and use. Although initiatives such as the Guiding Principles help create best practices around data collection, retention and use, it does not state any limits to corporate power over data policies. The Global Compact could be a place to develop and disseminate codes of conduct and best practices to encourage ICT corporate social responsibility that respects human rights and individual privacy.

Works Cited

Access Now. 2013. "Telco Action Plan: Respecting Human Rights: Ten Steps and Implementation Objectives for Telecommunications Companies." Access Now. https://s3.amazonaws.com/access.3cdn.net/1f9ab2891a86f3f081_uom6iil1w.pdf.

Micek, P. and J. Landale. 2013. "Forgotten Pillar: The Telco Remedy Plan." Access Now. https://s3.amazonaws.com/access.3cdn.net/fd15c4d607cc2cbe39_0nm6ii982.pdf.

OHCHR. 2011. "Guiding Principles on Business and Human Rights." www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

Suggested Readings

United Nations Global Compact. 2013. "The Ten Principles." www.unglobalcompact.org/AboutTheGC/TheTenPrinciples/index.html.

4.4 The OECD

Background

In the period from 1998 to 2007, much of the OECD's work focused on ICT policy for development, particularly in terms of e-commerce and Internet infrastructure. However, as the Internet began to grow and expand throughout the developing world, there was increased recognition that it was a platform for productivity and innovation that could fuel economic and social growth throughout the world. Recognizing this, in 2008, the OECD held its Seoul Ministerial where it expanded its focus from ICT policy for development to consider issues such as security and privacy, consumer protection, digital content and broadband development (OECD, n.d.).

Following the Seoul Ministerial, the OECD convened various leaders from the stakeholder community to adopt a code of best practices for a shared and open Internet economy. This code includes: a focus on expanding the communications network and providing access at affordable prices; fostering the use of the Internet in critical areas such as health, education and energy in order to increase efficiency; measuring developments and quantifying the Internet's impact on the economy to develop evidence-based policies; and encouraging countries to follow a number of basic principles for Internet policy so that it remains open and dynamic (OECD 2011a). These basic principles, taken from the OECD's Council Recommendation on Principles for Internet Policy Making (OECD 2011b), are highlighted below:

- Promote and protect the global free flow of information.
- Promote the open, distributed and interconnected nature of the Internet.
- Promote investment and competition in high speed networks and services.
- Promote and enable the cross border delivery of services.
- Encourage multi-stakeholder cooperation in policy development processes.
- Foster voluntary developed codes of conduct.
- Develop capacities to bring publically available reliable data into the policy making process.
- Ensure transparency, fair process and accountability.

- Strengthen consistency and effectiveness in privacy protection at a global level.
- Maximize individual empowerment.
- Promote creativity and innovation.
- Limit Internet intermediary liability.
- Encourage cooperation to promote Internet Security.
- Give appropriate priority to enforcement efforts.

In addition to the OECD's Internet policy-making principles, the council has also developed Recommendations on the Protection of Children Online to help governments protect minors online through principles based on evidence-based policy making, and has made recommendations on international mobile roaming services to help increase competition and reduce high international mobile roaming prices. These recommendations are not legally binding but rather best practices stakeholders are encouraged to adopt.

Works Cited

OECD. 2011a. "OECD Council Recommendation on Principles for Internet Policy Making." www.oecd.org/sti/ieconomy/49258588.pdf.

———. 2011b. "The Internet Economy: Generating Innovation and Growth." www.oecd.org/internet/innovation/.

———. n.d. "The Internet Economy on the Rise: Progress since the Seoul Declaration." www.oecd.org/sti/ieconomy/internet-economy-on-the-rise.htm.

4.5 Individuals as Actors in Internet Governance

Background

The Internet has become an important tool for empowering individuals. The creation of the "networked public sphere" (NPS) has created a space where "citizens can come together to debate and decide what issues are most salient as well as determine how to act on them" (Etling 2013a). A few examples are highlighted below.

The Internet and Protests

Citizens are increasingly using the Internet and social media to mobilize and coordinate protests. The Arab Spring is the most recent high-profile example of Internet enabled protests, which eventually led to the fall of governments in a number of states. These examples complicate arguments put forward by skeptics that "online talk is cheap," "that online activism is not real activism" and "that the Internet is more useful for dictators" (ibid.). Recent research has demonstrated the importance of the Internet and social media in providing new sources of information and for increasing individual attendance at protests. For example, one study showed that social media greatly increased the likelihood that individuals would attend protests the first day, when "success is typically least assured and the risk of attendance is the greatest" (ibid.). While such protests allow citizens opportunities to mobilize politically, it must be noted that such movements can entail significant short-term costs in the form of upheaval and uncertainty. Further, it is important to recognize that these technologies can also be used by governments to track and identify protestors. Thus by using this technology in some parts of the world for the purpose of protest, citizens can run the risk of imprisonment or death.

Government and Corporate Accountability

Citizens are able to use the Internet as "a check on corruption, mismanagement and abuse of power by government, corporations, and political and economic elites" (ibid.). Online news platforms can be used to bring issues to the forefront of public debate, especially in cases where "political or economic elites have control over national media" (ibid.). Examples of this include: NowPublic, Global Voices Internationally and Ridus in Russia. There are other online platforms, such as the Terms of Service; Didn't Read, where individuals contribute to by analyzing the fairness of user agreements from Internet content providers (Luckerson 2012). This can be used to empower citizens by bringing issues regarding corporate power into public debate, and by providing citizens with information to make more informed decisions. However, it is important to remember that the same technology that provides citizens with accountability can be used to repress, censor, block or surveil its users.

Issue-specific Campaigning

The NPS has played an important role in the organization of protests and issue-specific campaigning. Over the past few years, the NPS has achieved some important victories. According to Etling (2013b), the "starkest examples are online efforts that killed Internet related legislation that was pushed by the music and recording industries." A number of successful tactics were used to defeat SOPA, PIPA and ACTA: specialized tech media news outlets and digital rights and freedom groups played a critical role in bringing the issue into the mainstream public sphere; major online platforms, such as Wikipedia, blacked out their websites and pointed to US voters to contact their congress representatives; within the technology industry, Google placed a banner on its site in opposition to legislation and connecting users to their congressional representatives; and users from online platforms, such as Reddit and gaming communities, pushed technology companies to reverse their support of SOPA and PIPA (ibid.).

Contemporary Issues

In addition to recognizing the many ways that citizens use the Internet, the main question policy makers must ask is if and how citizens can be plugged in to Internet governance mechanisms? It can be argued that citizens are represented by their membership in non-governmental organizations, however, is this representation enough? Are the diverse views or citizens captured by these organizations? If not, how can they be better captured and represented in Internet governance mechanisms?

Works Cited

Etling, B. 2013a. "Citizens as Actors." In "Internet Monitor 2013: Reflections on the Digital World." http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366840.

———. 2013b. "The Defeat of SOPA, PIPA and ACTA: The Networked Public Sphere Comes of Age." In "Internet Monitor 2013: Reflections on the Digital World." http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366840.

Luckerson, V. 2012. "New Site Grades Those Pesky Terms of Service Agreements You Never Read." *Time Magazine*, August 20. http://business.time.com/2012/08/10/new-site-grades-those-pesky-terms-of-service-agreements-you-never-read/.

Suggested Readings

Kelly, J. 2013. "Three Generations of the Networked Public Sphere." In "Internet Monitor 2013: Reflections on the Digital World." http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366840.

Tufekci, Z. 2013. "I Was Wrong about this Internet Thing: Social Media and the Gezi Park Protests." In "Internet Monitor 2013: Reflections on the Digital World." http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366840.

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.

CIGI Masthead

Managing Editor, Publications	Carol Bonnett
Publications Editor	Jennifer Goyder
Publications Editor	Vivian Moser
Publications Editor	Patricia Holmes
Media Designer	Melodie Wakefield

Executive

President	Rohinton Medhora
Vice President of Programs	David Dewitt
Vice President of Public Affairs	Fred Kuntz
Vice President of Finance	Mark Menard

Communications

Communications Manager	Tammy Bender	tbender@cigionline.org (1 519 885 2444 x 7356)

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