CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Research Volume Three

Global Commission on Internet Governance

Mapping the Digital Frontiers of Trade and Intellectual Property

Research Volume Three

Global Commission on Internet Governance

Mapping the Digital Frontiers of Trade and Intellectual Property

CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Published by the Centre for International Governance Innovation and the Royal Institute of International Affairs

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

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

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

CHATHAM HOUSE
The Royal Institute of International Affairs

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

TABLE OF CONTENTS

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducted and supported independent research on Internet-related dimensions of global public policy, culminating in an official commission report — *One Internet*, published in June 2016 — that articulated concrete policy recommendations for the future of Internet governance. These recommendations address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

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

The Global Commission on Internet Governance focuses on four key themes:

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

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

www.ourinternet.org

PREFACE

When I and my colleagues at the Centre for International Governance Innovation and Chatham House envisioned and launched the Global Commission on Internet Governance (GCIG) in 2014, we were determined to approach the work ahead strictly on the strength of evidence-based research. To make this possible, we commissioned nearly 50 research papers, which are now published online. We believe that this body of work represents the largest set of research materials on Internet governance to be currently available from any one source. We also believe that these materials, while they were essential to the GCIG's discussions over these past months, will also be invaluable to policy development for many years to come.

The GCIG was fortunate to have Professor Laura DeNardis as its director of research, who, along with Eric Jardine and Samantha Bradshaw at CIGI, collaborated on identifying and commissioning authors, arranging for peer review and guiding the papers through the publication process.

Questions about the governance of the Internet will be with us long into the future. The papers now collected in these volumes aim to be forward looking and to have continuing relevance as the issues they examine evolve. Nothing would please me and my fellow Commissioners more than to receive comments and suggestions from other experts in the field whose own research has been stimulated by these volumes.

The chapters you are about to read were written for non-expert netizens as well as for subject experts. To all of you, the message I bring from all of us involved with the GCIG is simple — be engaged. If we fail to engage with these key governance questions, we risk a future for our Internet that is disturbingly distant from the one we want.

Carl Bildt

Chair, GCIG

November 2016

INTRODUCTION:
THE COMPLEX GEOPOLITICS OF DIGITAL PROPERTY AND TRADE

Laura DeNardis

INTRODUCTION

THE COMPLEX GEOPOLITICS OF DIGITAL PROPERTY AND TRADE

One of the most powerful and consequential intersections between the multi-trillion-dollar digital economy and Internet governance revolves around intellectual property (IP). For example, the digitization of major industries — music, movies, games, journalism — has created unprecedented IP challenges. It is technologically simple, and cheap, to copy and distribute products that used to necessitate the purchase of a physical medium. The Internet is also used to sell counterfeit products from pharmaceutical goods to luxury handbags, creating new challenges for patent and trademark holders. In turn, the infrastructures and institutions of the Internet are being called upon to block access to pirated and counterfeit goods.

In the digital economy, law enforcement functions once carried out by the state have shifted to the private sector. At the centre of the digital economy are the private companies that serve as the conduits and content intermediaries over which information flows. Search engine companies sometimes factor copyright infringement history into algorithms, demoting search engine rankings of sites alleged to be repeat offenders. Internet service providers deploy graduated response approaches, also called three-strikes policies, that cut off access to customers that repeatedly engage in illegal file sharing. The companies that administer the Internet's Domain Name System are often asked to redirect domain name query resolutions away from sites that sell counterfeit or pirated goods. Content intermediaries take down IP-infringing content in exchange for immunity from liability for illegal content flowing over their systems. These privatized governance functions can have significant collateral damage because they come into conflict with freedom of expression and the global flow of information. For example, cutting off home access because a teenager used peer-to-peer file sharing to exchange pirated music cuts off Internet access, and potentially education and livelihood, to an entire household.

As governments increasingly recognize the ways in which these Internet intermediaries serve as points of concentration for the flow of data, they view these companies as a means to control content, whether for censoring political speech or carrying out law enforcement functions. Hence, there are myriad attempts to impose regulations and constraints on businesses. In the first chapter in this collection, *Internet Intermediaries as Platforms for Expression and Innovation*, Anupam Chander (2016) examines the pressure to make these companies liable for the content that flows over their technological systems, ultimately warning that the threat of liability incentivizes companies to censor anything potentially controversial.

The intersections between the Internet and IP rights are many. The Internet makes it easier to infringe IP rights. It is also used to mediate and enforce IP rights. Completely distinct, and more hidden from public view, there are also IP rights embedded within the technological systems underlying the Internet, such as trademarks in domain names, patents embedded in standards and algorithms protected as trade secrets.

Exemplifying infrastructure-embedded IP rights are the patents often underlying the technical standards that product developers use as blueprints to ensure that their products are compatible with other technologies. Without these technology standards, there would be no interoperability between different companies' products, never mind cross-border interoperability and trade. These technical standards are protected by complex collections of patents that, while designed to incentivize innovation, impose restrictions or licensing fees that determine who is able to compete in a digital era often exaggeratedly described as a level playing field for competition.

In the second chapter, *Patents and Internet Standards*, Jorge L. Contreras (2016) offers a counternarrative to traditional accounts portraying essential standards as necessarily fraught with litigation over patents and thereby in need of reform. Core Internet standardization, emanating from the Internet Engineering Task Force and the World Wide Web Consortium, has had relatively minimal embedded IP rights, and has nevertheless led to unprecedented innovation and success. In Chapter Three, *Standards, Patents and National Competitiveness*, Michael Murphree and Dan Breznitz (2016) explore the effects of standards-essential patents in two case studies, Global System for Mobile and Code Division Multiple Access standards for mobile telecommunications. Alternatively, they discuss the benefits of royalty-free IP, or at least IP available under reasonable and non-discriminatory licensing terms.

A different set of IP rights conflicts materialize in domain names. Domain names, such as ourinternet.org, are the markers enabling humans to easily access and exchange information. Because this system of unique identifiers is a name space, it is also a speech space in which trademark conflicts often emerge. Who has the right to use a name when multiple parties own rights in different domains, such as united.com, hypothetically requested by United Airlines, United Van Lines and the Manchester United? When someone registers a website that appropriates a name owned by another party, how can this be expeditiously resolved? The assignment of most domain names is overseen by the

Internet Corporation for Assigned Names and Numbers (ICANN). In Chapter Four, Jacqueline Lipton reflects on how the already challenging array of problems around domain name registration was complicated when ICANN allowed the introduction of thousands of new generic top-level domains (gTLD). Her chapter, *Looking Back on the First Round of New gTLD Applications* (2016), also examines the tension between free speech and proprietary trademark interests.

It is no longer possible to think about trade issues and Internet governance issues as distinct spheres. In the digital economy in which trillions of dollars change hands in cross-border data flows, governance arrangements around this digital infrastructure are a proxy for trade arrangements. This linkage between trade and Internet governance is addressed in Susan Ariel Aaronson's chapter, *The Digital Trade Imbalance and Its Implications for Internet Governance* (2016). Aaronson examines attempts to use trade agreements to govern cross-border information flows, essentially serving as Internet governance mechanisms, and suggests that trade should be better aligned with other critical public interest objectives such as digital rights.

Some of the most intractable problems at the intersection of Internet governance and trade are questions of jurisdiction and also the role of traditional international organizations. In the sixth chapter, *Solving the International Internet Policy Coordination Problem*, Nick Ashton-Hart (2015) suggests that subject-area specific approaches to Internet public policy are a mistake and that international coordination should leverage existing fora. In Chapter Seven, *Governance of International Trade and the Internet: Existing and Evolving Regulatory Systems*, Harsha Vardhana Singh, Ahmed Abdel-Latif and L. Lee Tuthill (2016) examine the relevance of the WTO and free trade agreements in the digital environment. The connection between local jurisdiction efforts and globally coordinated approaches is especially difficult in the area of cyber security, a topic taken up in the final chapter in this collection, *Cyber Security and Cyber Resilience in East Africa* by Iginio Gagliardone and Nanjira Sambuli (2015), by looking at three case studies in East Africa: Kenya, Ethiopia and Somalia.

The digital economy is completely dependent upon a stable and secure system of infrastructure and governance. Trade and property are now intertwined with digital systems. Property not only flows over the network. It is embedded deeply within the network via trademark and patent arrangements. Trade not only flows over the network. The digital flows themselves have intrinsic value and infrastructure points of control have economic and political value. As governments have increasingly recognized the points of power that IP rights arrangements and trade arrangements have over the cross-border digital flow of currency and data, tensions and jurisdictional conflicts over Internet governance have also increased. The stakes are high because governance of the Internet is now not only about content and infrastructure but also about governance of trade and of property. This research volume brings together global scholars to examine the implications of the evolving geopolitics of digital trade and property and recommend solutions for promoting a stable system of global governance.

WORKS CITED

Aaronson, Susan Ariel. 2016. *The Digital Trade Imbalance and Its Implications for Internet Governance*. GCIG Paper Series No. 25. Waterloo, ON: CIGI.

Ashton-Hart, Nick. 2015. *Solving the International Internet Policy Coordination Problem*. GCIG Paper Series No. 12. Waterloo, ON: CIGI.

Chander, Anupam. 2016. *Internet Intermediaries as Platforms for Expression and Innovation*. GCIG Paper Series No. 42. Waterloo, ON: CIGI.

Contreras, Jorge L. 2016. *Patents and Internet Standards*. GCIG Paper Series No. 29. Waterloo, ON: CIGI.

Gagliardone, Iginio and Nanjira Sambuli. 2015. *Cyber Security and Cyber Resilience in East Africa*. GCIG Paper Series No. 15. Waterloo, ON: CIGI.

Lipton, Jacqueline D. 2016. *Looking Back on the First Round of New gTLD Applications: Implications for the Future of Domain Name Regulation*. GCIG Paper Series No. 31. Waterloo, ON: CIGI.

Murphree, Michael and Dan Breznitz. 2016. *Standards, Patents and National Competitiveness*. GCIG Paper Series No. 40. Waterloo, ON: CIGI.

Singh, Harsha Vardhana, Ahmed Abdel-Latif and L. Lee Tuthill. 2016. *Governance of International Trade and the Internet: Existing and Evolving Regulatory Systems*. GCIG Paper Series No. 32. Waterloo, ON: CIGI.

ABOUT THE AUTHOR

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

CHAPTER ONE:
INTERNET INTERMEDIARIES AS PLATFORMS FOR EXPRESSION AND INNOVATION

Anupam Chander

INTRODUCTION[1]

Many of the biggest companies in the world today are intermediaries for online information. Facebook intermediates information sharing among its 1.5 billion users. Google intermediates the entire Internet for individuals performing more than three billion searches a day. Alibaba intermediates the distribution of wares from millions of sellers to 350 million buyers across the world in a single year. Tencent's WeChat app intermediates messages among some 700 million people. Individuals across the world upload 400 hours of video every minute to YouTube (Brouwer 2015). Internet companies serve as intermediaries for literally billions of transactions a day. They have become a crucial means for communication and commerce, as well as for education and entertainment. The Chinese website Qidian.com, to cite another example, is "the world's leading self-publishing platform, with 1 million registered writers and 100 million paying members" (Box and West 2016, 52).

For better or worse, Internet intermediaries have become a focal point for Internet regulation across the world. Because they help businesses, organizations and individuals to connect across the world in ever more domains of life, Internet intermediaries have come to be seen as crucial arbiters of what is allowed and not allowed in a society. Governments see Internet intermediaries as central points at which to exercise control, a far easier task than to regulate the individuals who use the Internet directly. Governments often require intermediaries to censor information so that it is not distributed among their citizenry, and also to turn over some of the information they gather from their users.

But requiring Internet intermediaries to serve as online censors and police harms free expression and undermines the development of new enterprises, which generally lack the resources to satisfy extensive monitoring obligations. When the law exposes intermediaries to liability for the actions of their users, intermediaries have an economic incentive to censor anything potentially controversial. When the law requires intermediaries to reveal the actions of their users to the police, individuals refrain from even legal actions.

Internet intermediaries can foster freedom online, or they can undermine it, through censoring and monitoring the population.

GLOBAL INTERMEDIARIES, LOCAL PROBLEMS

Intermediaries have long existed — think real-estate agents to stockbrokers to the village matchmaker. Yet, there is something different, both quantitatively and qualitatively, about the new breed of intermediaries on the Internet. The Internet has brought with it new types of intermediaries with new capabilities operating at scales far beyond yesteryear's librarians and brokers. These intermediaries now operate not at the scale of a town, but at the scale of a country or even the world. YouTube offers a local version in more than 88 countries, in 76 different languages; 80 percent of YouTube's views come from outside the United States,[2] where it is headquartered.

Online intermediaries include a wide array of companies essential to the Internet: Internet service providers (ISPs), which provide Internet access to households and businesses; Internet hosting services, which rent computer server space to others; social media platforms (in so-called Web 2.0 services), which allow users to share writing, photos, audio and video; and search engines. More recently, new forms of Internet intermediaries, such as Uber, Didi Chuxing and Airbnb, have arisen. Relying on the fact that smartphones know where we are at all times, these new intermediaries offer services tailored to an individual's precise location in the world. Thus, today's intermediaries depend on both the micro scale of the Internet, pinpointing where a user is geographically, and the macro scale of the Internet, allowing intermediaries to connect, quite literally, one billion people in a day.

Online intermediaries have increasingly found themselves part of global flashpoints concerning local regulation. Take a few recent examples. A Brazilian court has frozen US$6 million in a Facebook bank account in Brazil because Facebook says it cannot access or decrypt messages sent via its Whatsapp platform in a case involving illicit drugs (Reuters 2016a). Hungary now has a law permitting the national communications authority to block Internet access to "illegal dispatcher services" (Dunai 2016), thus granting the government the ability to ban intermediaries such as Uber and Didi Chuxing.

Since today's intermediaries often operate across national borders, connecting people wherever they may be, intermediaries are subject to rules that often vary or even conflict in what they allow or require.

FREE EXPRESSION

Article 19 of the United Nation's Universal Declaration of Human Rights states that freedom of expression is a universal human right: "Everyone has the right to

1 The author thanks Anna Barich for excellent research assistance, and is grateful for a Google Research Award supporting related research. Some of the passages herein are drawn from "How Law Made Silicon Valley" (Chander 2014a, 653–56, 670–72, 675-676), "Law and the Geography of Cyberspace" (Chander 2014b, 104-105) and "Free Speech" (Chander and Le 2014).

2 See www.youtube.com/yt/press/statistics.html.

freedom of opinion and expression; the right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media regardless of frontiers" (United Nations 1948). The civil society group Article 19, named after the provision, argues that intermediary liability rules can adversely affect freedom of expression. It observes "risks posed by the currently widespread regime of liability to the exercise of freedom of expression online" (Article 19 2013, 4). It accordingly proposes that "hosts should in principle be immune from liability for third-party content in circumstances where they have not been involved in modifying that content" (ibid., 16).

Online intermediaries have helped make the Internet the modern town hall and village square. There is an emerging consensus in the human rights community that limiting intermediary liability promotes freedom of expression. As a report for UNESCO by Internet freedom advocate Rebeccca MacKinnon and others concludes, "limiting the liability of intermediaries for content published or transmitted by third parties is essential to the flourishing of internet services that facilitate expression" (MacKinnon et al. 2014, 179). UN Special Rapporteur Frank LaRue (2011, 6-7) observed the value of Internet intermediaries to freedom of expression:

> With the advent of Web 2.0 services, or intermediary platforms that facilitate participatory information sharing and collaboration in the creation of content, individuals are no longer passive recipients, but also active publishers of information...platforms are particularly valuable in countries where there is no independent media, as they enable individuals to share critical views and to find objective information.

LaRue observed the simple logic that leads from intermediary liability to censorship: "Given that intermediaries may still be held financially or in some cases criminally liable if they do not remove content upon receipt of notification by users regarding unlawful content, they are inclined to err on the side of safety by overcensoring potentially" (ibid., 12). In their 2011 Joint Declaration on Freedom of Expression and the Internet, the four UN special rapporteurs on freedom of expression recommended that:

> No one who simply provides technical Internet services such as providing access, or searching for, or transmission or caching of information, should be liable for content generated by others, which is disseminated using those services, as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so ('mere conduit principle').…At a minimum, intermediaries should not be required to monitor user-generated content and should not be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression (which is the case with many of the 'notice and takedown' rules currently being applied). (UN Special Rapporteur et al. 2011)

But online intermediaries have often been targeted precisely because of the information they help disseminate. In the wake of the horrendous attack on Istanbul's Ataturk Airport this year, Turkey's government reportedly moved to block or throttle (slow down) Facebook, Twitter and YouTube. An Istanbul court "later expanded the order to include all media, noting that news about the attack may spread 'fear and panic, which may serve to the intentions of terrorist groups'" (Risen 2016).

INTERMEDIARY LIABILITY LAW

The law regulating Internet intermediaries varies across the world. A comparison of legal regimes shows that the United States is notably more hospitable to such enterprises than many other leading technologically advanced nations.

What follows is a comparison of the intermediary liability laws of the United States and those of the European Union and Japan.

INTERMEDIARY LIABILITY LAW IN THE UNITED STATES

In the 1990s, the US Congress passed two pieces of legislation that proved essential to the rise of the global Internet as we know it today: the Communications Decency Act (CDA) of 1996 and the Digital Millennium Copyright Act (DMCA) of 1998. These statutes helped encourage the development of Internet intermediaries by increasing confidence that they would not be held liable if a user utilized their services to violate someone else's rights.

Because many (and perhaps most) individuals will infringe copyright at some point when they use online services to share information, holding the online service liable for that infringement would make that service leery of open-ended sharing. Perhaps a service would have to monitor each user post — an expensive proposition. Monitoring obligations would make impossible a service such as Craigslist, where individuals and businesses post some 80 million classified

advertisements a month.[3] Each of Craigslist's 40 employees would have to review two million advertisements per month, or Craigslist would have to hire legions more employees, jeopardizing its ability to offer a free service supported by advertising alone.

Any technology that allows individuals to share information can lend itself to copyright infringement. A company like Yahoo that allows individuals to post whatever they want online faces a high risk that its service will be used for extensive copyright infringement. Such a company would be liable for direct infringement every time it delivered a copy of a copyrighted work, for contributory infringement if it had knowledge and made a material contribution to the infringement, and for vicarious infringement if it controlled and earned a direct financial benefit from the infringement. Given that statutory damages for direct infringement alone range from US$200 to US$150,000 per work,[4] and that millions of works are copied online each day, the spectre of liability would be enough to stop most Internet companies in their tracks.

The DMCA offered ISPs safe harbours from liability for copyright infringement by users. The DMCA established a notice-and-takedown regime that did not place the policing burden for discovering copyright infringement on the Internet intermediary. Rather than monitoring their own networks for possible copyright infringement — a costly and difficult task — online intermediaries could wait for copyright holders to notify them of specific infringements. The statute insulated Internet intermediaries that duly cooperated with copyright holders upon receiving a notice of infringement.[5] This had a clear effect: relying on the DMCA, US courts, for example, sided with YouTube against Viacom's claims that YouTube abetted copyright infringement by holding that YouTube could not be held liable for users who uploaded Viacom's copyrighted videos.[6]

The DMCA achieved a relatively peaceful coexistence between northern and southern California — where technology companies in Silicon Valley, in the north, would banish repeat offenders and take down material if requested by the copyright owners, often based in Hollywood, in the south. By performing these duties diligently, Silicon Valley enterprises generally managed to avoid liability for the widespread copyright infringement that still occurred through their systems. While some have legitimately criticized Title II (the Online Copyright Infringement Liability Limitation Act) of the DMCA for leading firms to take down material too quickly for fear of jeopardizing their safe harbour, the DMCA marked a significant accomplishment for Silicon Valley in creating rules that allowed Web 2.0 enterprises to flourish without either excessive copyright-management costs or high liability risks.

Section 230 of the CDA warded off claims for intermediary liability for defamation and a host of other civil claims. Again and again, Section 230 proved invaluable to shield web enterprises from lawsuits, as demonstrated by a plethora of cases.[7] Perhaps every major Internet enterprise has relied on the statute to defend itself over the years. CDA Section 230 insulated web enterprises from the reach of a variety of federal and state causes of action, both statutory and common law (Lemley 2007). These include, for example, the Federal Fair Housing Act, Title II of the Civil Rights Act of 1964, the Washington State Consumer Protection Act, and common law actions such as invasion of privacy, negligence and tortious interference with business relations. As the US Fourth Circuit Court of Appeals noted, a notice-and-takedown system would inevitably lead to firms generally choosing to take down controversial statements rather than face any spectre of liability.[8] As Neal Katyal (2001, 1007-1008) writes, "because an ISP derives little utility from providing access to a risky subscriber, a legal regime that places liability on an ISP for the acts of its subscribers will quickly lead the ISP to purge risky ones from its system."

Protection from liability has depended not only on congressional action, but also on judicial interpretation and common law-making. The DMCA's safe harbours for Internet intermediaries are limited to protections from copyright-infringement claims, and Section 230 of the CDA does not apply to intellectual property claims. Courts interpreting common law doctrines have acted on their own to limit the liability of online intermediaries for trademark infringement by users.

The end result was that, for more or less the same behaviour, an Internet company might find itself in legal trouble in Europe but scot-free in the United States. An entrepreneur founding a company that allows individuals across the world to buy and sell goods might well choose the United States as a more welcoming legal regime to register with. Such a company based in Europe might find itself encumbered by obligations to determine whether the multitude of goods sold on its site were authentic. Such a burden might well prove too demanding for a fledgling corporation. Consider the case of eBay. Two years after its founding, in 1995, eBay still had fewer than 50 employees.

3 See www.craigslist.org/about/factsheet.

4 Copyright Act, Title 17, US Code, Section 504(c)(1)-(2) (2012) (providing statutory damages of $750 to $30,000 per work, but permitting damages per work to be reduced to $200 in cases where the defendant was not aware, and had no reason to believe, that infringement was occurring, or increased to $150,000 in cases of willful infringement).

5 DMCA, Title 17, US Code, Section 512 (1998).

6 *Viacom Int'l Inc. v. YouTube Inc.* 940 F. Supp. 2d 110 (SDNY 2013); *Viacom Int'l Inc. v. YouTube Inc*. 676 F.3d 19 (2nd Cir. 2012).

7 For a lengthy list of examples, see Chander (2014a, 653–55, n58).

8 *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997).

A year later, in mid-1998, with 76 employees, it was hosting 500,000 items for sale, with 70,000 items added per day. At the time, it was valued at US$2 billion. It is hard to imagine that such a small group of employees could have vetted the literally tens of thousands of classified items coming in each day to ascertain whether they were authentic (Chander 2014b, 104-105).

Despite popular understanding of the United States as an intellectual property maximalist state, US intellectual property law has proven a good deal more flexible than that in other technologically advanced states. The hospitable legal framework did more than help American enterprise, it has created what has become the engine for free speech across the world today. US companies now serve as free-expression platforms for the world.

INTERMEDIARY LIABILITY LAW IN THE EUROPEAN UNION

The European Union's intermediary liability law proved less welcoming to Internet entrepreneurs than US law. Europe takes a unified approach to the issue of intermediary liability, setting the same standard for holding intermediaries liable, regardless of the nature of the underlying offence. There is logic to this approach, even if it is unlike the American approach, which, as noted, offers different rules for intermediary liability for copyright, trademark and other offences.[9] The European Union's Electronic Commerce Directive sets out what are essentially safe harbours from liability for specified intermediary activities, such as acting as a "mere conduit," "caching" or "hosting" (but not search services). Some countries go further, so as to include safe harbours for search engines and hyperlink providers (Verbiest et al. 2007). Yet, from the perspective of Internet intermediaries, these safe harbours remain inferior to the American ones, providing less protection from copyright, trademark, defamation and other claims. Some of the deficiencies of EU law vis-à-vis US law for Internet intermediaries are explained here.[10]

First, the European approach stops far short of the near-blanket exclusion from liability offered by the CDA for non–intellectual property related wrongs.[11] Second, the EU's Electronic Commerce Directive largely adopts the DMCA's notice-and-takedown approach, but leaves open the possibility of additional proactive responsibilities on the part of the online intermediary. Even while disavowing any duty to "monitor," the EU law expressly contemplates the imposition by member states of "duties of care" on intermediaries to detect and prevent certain activities (European Parliament 2000). Third, the European directive lacks a statutory notice-and-takedown regime, creating greater uncertainty among European providers as to whether they have somehow acquired sufficient knowledge to be held liable if they do not delete material on their own (Peguera 2009, 490).

The two directives proved inferior to their US counterparts from the perspective of ISPs for the opposite reasons — the first for lack of specificity, and the second for too much specificity. While the Electronic Commerce Directive followed the DMCA's Title II in granting ISPs certain immunities arising from web-hosting activities, it did not specify the exact circumstances that would guarantee freedom from liability. Nor did the directive offer immunity to search engines (Kuczerawy and Ausloos 2015). At the same time, the very specificity of the directive undermined its usefulness to web enterprises. Rather than an open-ended doctrine of fair use, EU law allowed only specified exceptions to the exclusive rights of the copyright holder.[12] These proved less flexible in responding to technological developments than did US fair use, which allowed a court to consider each new case individually, based on multiple factors. As one British scholar notes, fair use "provide[d] the courts with some flexibility of response to change in the way copyright works are disseminated and used, whether arising from new technologies, social behavior or institutional structures" (MacQueen 2009, 209; see also Hargreaves 2011).

Even as late as 2008, European lawyers could only advise that "The scope of liability of Web 2.0 websites is an unsettled point of law" (Joslove and De Spiegeleer-Delort 2008). It was not until 2012 that the European Court of Justice made clear that Internet intermediaries would not be required to affirmatively filter their entire networks for copyright infringement. In cases brought by the Belgian collecting society SABAM against the Internet access provider Scarlet and the online social network Netlog, the court held that enjoining these companies to filter uploads by all users on behalf of copyright owners would violate the privacy and speech rights of users, and would be unduly costly and burdensome to the Internet

9 The Europeans describe their approach as a "horizontal" one, encompassing secondary liability for all illicit behaviour (Peguera 2009, 482–84).

10 I do not mean to suggest that European law is invariably hostile to Internet intermediaries. For example, an Italian court recently rejected an attempt to hold Google liable for the automatically generated suggestions of additional search terms that happened to add offensive words after a person's name (Coraggio 2013).

11 See Pfanner (2010), who quotes a London lawyer as saying, "The issue of when a host was liable has been getting a bit vague, and some hosts in Europe have been getting a little bit nervous."

12 "This more restrictive approach limits the room to manoeuvre for the courts. The District Court of Hamburg, for instance, refused to bring thumbnails of pictures displayed by Google's image search service under the umbrella of the right of quotation" (Senftleben 2010, 536).

enterprise.[13] While the judgments in *SABAM v. Netlog* and *Scarlet v. SABAM* clearly support Web 2.0 enterprises, they arrived nearly a decade after the rise of such companies in the United States.

INTERMEDIARY LIABILITY LAW IN JAPAN

In Japan, running a bulletin board service in 1997 might render you liable for defamation occurring on that service. That year, a Tokyo trial court held Nifty Service, an ISP, liable for failing to delete defamatory messages (Tanaka 2001, 67). A heated exchange on a forum titled "Contemporary Ideas" had resulted in defamatory posts, which the forum's manager left up, "apparently believing that continuing the discussion and trying to engage the parties in a more issue-oriented dialogue would address the problem" (Mehra 2007, 801). It was not until 2001 that the Tokyo High Court would reverse the decision.

That same year, Japan's Diet passed the Law Concerning the Limits of Liability for Damages of Specified Telecommunications Service Providers, under which a telecommunications service provider would not be liable for the actions of its users unless it knew, or where there was "reasonable ground to find that said relevant service provider could know[,] the violation of the rights of others was caused by the information distribution via said specified telecommunications."[14] Like the European approach, the law applies to all intermediary activity, whether involving copyright, trademark or tort claims. By imposing not only an actual knowledge-and-takedown approach but also a more vague "reasonable ground" that the provider "could know," the 2001 limitation law was a pale shadow of the CDA Section 230 from the perspective of Internet enterprise.

In Japan, developing a peer-to-peer file-sharing service in the last decade might get you arrested. In 2002, Isamu Kaneko, a researcher at the University of Tokyo's School of Information and Science Technology, began distributing a peer-to-peer file-sharing program he wrote called "Winny." In May 2004, he was arrested for copyright infringement because he continued to distribute his program despite being aware that some had used it to infringe copyrights (*Daily Yomiuri* 2004). After his arrest, Kaneko, described as an "idol" among programmers, and who had taught a series of lectures to nurture "superprogrammers," resigned from his university position. In December 2006, the Kyoto District Court found him guilty, decrying his "selfish and irresponsible attitude," and concluding that he knew that Winny "was being used to violate the law and allowed users to do so" (*Daily Yomiuri* 2006). Yet, the judge conceded that "Kaneko did not specifically intend to cause copyright violations on the Internet" (ibid.). He was fined 1.5 million yen for the infringement. The Japanese Supreme Court would ultimately clear him of all charges, but not until December of 2011 (*Japan Times* 2011).

Japan's 2001 law limiting liability for ISPs in certain circumstances was far less friendly to such companies than the DMCA. Rather than the relatively clear safe harbours of the DMCA, Japan's law removed any protections if the provider knew *or should have known* of infringement occurring through its service, a far more uncertain standard, especially given the likelihood that some users will infringe on any Web 2.0 service.

INTERMEDIARY LIABILITY AND THE IMPACT ON INNOVATION

Imagine the boardroom in a Silicon Valley venture capital firm, circa 2005. A start-up less than a year old has already attracted millions of users. Now that start-up, which is bleeding money, needs an infusion of cash to survive and grow. The start-up allows users to share text, photos and videos, and includes the ability to readily share text, pictures and videos posted by friends. If that start-up can be accused of abetting copyright infringement on a massive scale, or must police its content like a traditional publishing house, lest it face damages claims or an injunction, the firm's US$100 million investment might go to plaintiffs' lawyers in damages and fees.[15] A court injunction might stop the site from continuing without extensive human monitoring, which could not be justified by potential revenue. Because of the insulation brought by US law reforms in the 1990s, American start-ups did not fear such a mortal legal blow. The legal privileges granted to Internet enterprises in the United States helped start-ups bridge the so-called "valley of death," the stage between creative idea and successful commercialization, in which most start-up enterprises founder.

While many European and Asian nations leave intermediaries open to liability for the actions of their users in certain cases, the United States generally limits

13 Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, paras. 46–48 (Feb. 16, 2012), available at http://curia.europa.eu/juris/celex.jsf?celex=62010CJ0360&lang1=en&type=TXT&ancre=; Case C-70/10, *Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Éditeurs SCRL (SABAM)*, 2011 E.C.R. I-11959, paras. 48, 52 (Nov. 24, 2011), available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62010CJ0070&from=EN.

14 Tokutei denkitsuushin ekimu teikyousha no songaibaishou sekinin no seigen oyobi hasshinsha jouhou no kaiji ni kansu ru houritsu [Law Concerning the Limits of Liability for Damages of Specified Telecommunications Service Providers and the Right to Request Disclosure of Identification Information of the Senders], Law No. 137 of 2001, art. 3, translated at www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/laws/Compensation-Law.pdf (Japan).

15 This hypothetical scenario finds real-world inspiration in the origins of Pinterest (Lynley 2012; Tsukayama 2012).

liability. Liability limitations in the United States allowed the firms of Silicon Valley to worry about improving and expanding features and attracting and retaining customers, rather than policing their services for fear of lawsuits. The success of US Internet companies has depended not only on well-educated entrepreneurs and the availability of venture capital, but also on laws that reduced the legal risks in building platforms for the use of millions.

The example of public Wi-Fi in Germany helps dramatize the relationship of intermediary liability and the decision to offer a service. It has long been difficult to find public Wi-Fi in Germany. This is not for lack of technology in the country, but rather because of the law making Wi-Fi intermediaries liable for the actions of their users: "Private hotspot providers in Germany are liable for the misconduct of users. If, for example, a user were to download music or a movie on a particular hotspot, the provider ran the risk of being sued for piracy" (Brady 2016). Demands for compensation for copyright piracy made against ISPs abounded — "regardless of whether the provider was aware of the activity" (Moody 2016). When a German non-profit organization opened up its Wi-Fi to the public and someone used it illegally, "members of our office had an awkward interview at the police," it reported (Foundation for a Free Information Infrastructure 2015). The European Court of Justice is currently considering the issue of the liability of a free public Wi-Fi operator for copyright infringement (Masnick 2016). In May 2016, the German government lifted the spectre of liability, but it may be a while before individuals and businesses feel confident that they will not be liable in offering free Wi-Fi.

SURVEILLANCE AND LAW ENFORCEMENT

Information intermediaries have found themselves at the centre of another controversy — that of governmental surveillance. Because intermediaries gather a tremendous amount of data about users in their ordinary course of conduct, governments may seek that data for surveillance and other law-enforcement purposes. If the information is stored in one country but demanded by another — the laws of the two countries may come into conflict. The privacy laws of one country may interfere with the law-enforcement provisions of another. As David Kris (2015) describes:

> For example, a U.S. provider that stores data in the United States, from the email account of a British citizen located in England, might be simultaneously required (by DRIPA [the UK Data Retention and Investigatory Powers Act 2014]) and forbidden (by ECPA/SCA [the US Electronic Communications Privacy Act/Stored Communications Act]) to produce the email. Correspondingly, a U.S. provider that stores email abroad might be simultaneously required (by the SCA) and forbidden (by a foreign data protection law) to produce the email.

Laws vary widely on the steps necessary before a government authority can require an intermediary to turn over information about its users. While the revelations of Edward Snowden cast American practices in a negative light, laws around the world can also be problematic. A study for the Council of Europe reports that even in some of its member states, "Administrative authorities, police authorities or public prosecutors are given specific powers to order internet access providers to block access without advance judicial authority. It is common to see such orders requiring action on the part of the internet access provider within 24 hours, and without any notice being given to the content provider or host themselves" (Swiss Institute of Comparative Law 2015, 3).

Eager to access the information that online intermediaries might have on those distributing information in their countries, authoritarian governments, in particular, have increasingly sought to require online intermediaries to store data within their countries, facilitating access by their security services. In 2016, Iran's Supreme Council for Cyberspace, for example, ordered messaging apps to store data within the country (Reuters 2016c). This follows a broad data localization mandate issued by the Russian government in 2015. Such data localization requirements facilitate a government's access to data by preventing the intermediary from shielding efforts to turn over data held abroad based on jurisdiction.

MANILA PRINCIPLES: BEST PRACTICES FOR REGULATING INTERNET INTERMEDIARIES

In 2015, a group of civil society organizations, including the Electronic Frontier Foundation, the Centre for Internet Society India and Article 19, proposed the "Manila Principles on Intermediary Liability." The Manila Principles are a set of best practices guidelines for limiting intermediary liability for content to promote freedom of expression and innovation. The six Manila Principles are:

> Intermediaries should be shielded by law from liability for third-party content.
>
> Content must not be required to be restricted without an order by a judicial authority.
>
> Requests for restrictions of content must be clear, be unambiguous, and follow due process.

> Laws and content-restriction orders and practices must comply with the tests of necessity and proportionality.
>
> Laws and content restriction policies and practices must respect due process.
>
> Transparency and accountability must be built into laws and content restriction policies and practices.[16]

The Manila Principles focus on due process, including the requirement of judicial orders for content takedown, as well as transparency and accountability. The principles have attracted early support in the human rights community. David Kaye (2015, 19), UN special rapporteur on free expression, observes, "The recently adopted Manila Principles on Intermediary Liability, drafted by a coalition of civil society organizations, provide a sound set of guidelines for States and international and regional mechanisms to protect expression online."

RIGHTS AND RESPONSIBILITIES: PRIVACY, HARMFUL SPEECH AND PRIVATE CONTROL

At the same time that Internet intermediaries help us as individuals connect, learn and converse, they also gain a tremendous amount of information about us and can, if they wish, exercise control over what we share and read. Thus, while freeing Internet intermediaries from liability for what their users do, we might still be concerned about what the intermediaries themselves do.

Many of the concerns raised with Internet intermediaries have revolved around privacy because of the tremendous data sets that they acquire. In the United States, the Federal Trade Commission has entered into settlements with Facebook, Google, Snapchat and Twitter whereby those companies pay for independent privacy audits conducted on a biannual basis for 20 years. These audits seek to ensure that these companies comport themselves according to the privacy promises they make in their terms of use.

Recently, some have worried that Internet intermediaries might manipulate the information on their services. These companies must also take care not to manipulate unfairly the information we receive through their services. They should also attend to the ways that automated algorithms can reinforce societal hierarchies (Chander, forthcoming 2017).

Facebook, Google, Twitter and others have increasingly been called upon to block the social media accounts of entities allegedly associated with international terrorism. Israel's security head has called Facebook a "monster" because it sets "a very high bar for removing inciteful content and posts" (Reuters 2016b). The Council of Europe, however, has cautioned member states to "ensure that their legal frameworks and procedures in this area are clear, transparent and incorporate adequate safeguards for freedom of expression and access to information in compliance with Article 10 of the European Convention on Human Rights" (Council of Europe 2016). Microsoft has issued a policy announcing its approach to online terrorist content. This is hardly a usual policy arena for a multinational company, but Microsoft's opening observation makes clear why this is necessary: "The Internet has become the primary medium for sharing ideas and communicating with one another and the events of the past few months are a strong reminder that the Internet can be used for the worst reasons imaginable" (Microsoft Corporation 2016). It amended its community guidelines to explicitly bar terrorist content, and stated that it would remove such content when it learned of it through a reporting system it provided online: "When terrorist content on our hosted consumer services is brought to our attention via our online reporting tool, we will remove it." To avoid becoming the arbiter of who is a terrorist ("There is no universally accepted definition of terrorist content," the company noted), Microsoft indicated that it would rely upon the list of organizations included on the Consolidated United Nations Security Council Sanctions List. Microsoft's policy seems a promising start, and its workability and consequences should be reviewed over time.

CONCLUSION

The Organisation for Economic Co-operation and Development (2010) concludes that Internet intermediaries increase user empowerment and choice, and improve purchasing power. Every second, some 2,534,097 emails are sent, 133,975 YouTube videos viewed, 56,896 Google searches conducted, 39,019 gigabytes of traffic posted through the Internet, 2,321 Skype calls made and 7,387 Tweets sent, according to estimates by the Internet Live Stats website.[17] The law regulating these and other online intermediaries helps determine whether such services are possible.

16 See www.eff.org/files/2015/10/31/manila_principles_1.0.pdf.

17 As of October 25, 2016. See www.internetlivestats.com/one-second/.

WORKS CITED

Article 19. 2013. *Internet Intermediaries: Dilemma of Liability*. Article 19. www.article19.org/data/files/Intermediaries_ENGLISH.pdf.

Box, Sarah and Jeremy West. 2016. "Economic and Social Benefits for Internet Openness." OECD Background Paper. doi:10.1787/5jlwqf2r97g5-en.

Brady, Kate. 2016. "Germany to Abolish Provider Liability Law, Open Path to More Free Wifi." DW, May 11. www.dw.com/en/germany-to-abolish-provider-liability-law-open-path-to-more-free-wifi/a-19249024.

Brouwer, Bree. 2015. "YouTube Now Gets Over 400 Hours of Content Uploaded Every Minute." TubeFilter, July 26. www.tubefilter.com/2015/07/26/youtube-400-hours-content-every-minute.

Chander, Anupam. 2014a. "How Law Made Silicon Valley." *Emory Law Journal* 63 (3): 639–94.

———. 2014b. "Law and the Geography of Cyberspace." *World Intellectual Property Organization* Journal 6 (1): 99–106.

———. Forthcoming 2017. "The Racist Algorithm?" *Michigan Law Review* 115.

Chander, Anupam and Uyen P. Le. 2014. "Free Speech." *Iowa Law Review* 100 (2): 501–49.

Coraggio, Giulio. 2013. "Google NOT Liable for Suggest Search Results." *GamingTechLaw* (blog), January 4. www.gamingtechlaw.com/2013/04/google-not-liable-for-suggest-search.html.

Council of Europe. 2016. "Rules for Blocking and Removal of Illegal Content Must be Transparent and Proportionate." Council of Europe, June 1. www.coe.int/en/web/human-rights-rule-of-law/-/rules-for-blocking-and-removal-of-illegal-content-must-be-transparent-and-proportionate.

Daily Yomiuri. 2004. "File-Sharing Author Arrested." *Daily Yomiuri,* May 11, 2.

———. 2006. "Winny Inventor Convicted." *Daily Yomiuri,* December 14, 1.

Dunai, Marton. 2016. "Hungary Passes Law that Could Block Uber Sites." Reuters, June 13. www.reuters.com/article/us-uber-hungary-ban-idUSKCN0YZ1KD.

European Parliament. 2000. *Directive, 2000/31, of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market.*

Foundation for a Free Information Infrastructure. 2015. "The German Störerhaftung of Wifi." *FFII* (blog), March 27. https://blog.FFII.org/the-german-storerhaftung-of-wifi/.

Hargreaves, Ian. 2011. *Digital Opportunity: Review of Intellectual Property and Growth.* UK Department for Business, Innovation & Skills. May 18. www.gov.uk/government/uploads/system/uploads/attachment_data/file/32563/ipreview-finalreport.pdf.

Japan Times. 2011. "Absurd Arrest Rectified." *Japan Times*, December 26 (editorial). www.japantimes.co.jp/opinion/2011/12/26/editorials/absurd-arrest-rectified/#.UlVbMGSSxJs.

Joslove, Bradley L. and Vanessa De Spiegeleer-Delort. 2008. "Web 2.0: Aggregator Website Held Liable as Publisher." International Law Office, June 26. www.internationallawoffice.com/newsletters/detail.aspx?g=4b014ec1-b334-4204-9fbd-00e05bf6db95#11.

Katyal, Neal Kumar. 2001. "Criminal Law in Cyberspace." *University of Pennsylvania Law Review* 149 (4): 1003–114.

Kaye, David. 2015. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.* Human Rights Council, May 22. A/HRC/29/32.

Kris, David. 2015. "Preliminary Thoughts on Cross-Border Data Requests." *LawFare* (blog), September 28. www.lawfareblog.com/preliminary-thoughts-cross-border-data-requests.

Kuczerawy, Aleksandra and Jef Ausloos. 2015. *European Union and Google Spain.* https://publixphere.net/i/noc/page/OI_Case_Study_European_Union_and_Google_Spain.

LaRue, Frank. 2011. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.* Human Rights Council, May 16. A/HRC/17/27.

Lemley, Mark A. 2007. "Rationalizing Internet Safe Harbors." *Journal on Telecommunications and High Technology Law* 6: 101, 102–5.

Lynley, Matt. 2012. "Pinterest: We're Not Going to Be Sued into Oblivion, and Here's Why." *Business Insider,* March 9. www.businessinsider.com/pinterest-were-not-going-to-be-sued-into-oblivion-and-heres-why-2012-3.

MacKinnon, Rebecca, Elonnai Hickok, Allon Bar and Hae-in Lim. 2014. *Fostering Freedom Online: The Role of Internet Intermediaries*. United Nations Educational, Scientific and Cultural Organization Report. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.

MacQueen, Hector L. 2009. "'Appropriate for the Digital Age'? Copyright and the Internet: 2. Exceptions and Licensing." In *Law and the Internet*, edited by Lilian Edwards and Charlotte Waelde, 183–225. Oxford, UK: Hart Publishing.

Masnick, Mike. 2016. "EU Court Of Justice Advocate General Says Open WiFi Operators Shouldn't Be Liable For Infringement." *TechDirt* (blog), March 17. www.techdirt.com/blog/wireless/articles/20160316/13090133923/eu-court-justice-advocate-general-says-open-wifi-operators-shouldnt-be-liable-infringement.shtml.

Mehra, Salil K. 2007. "Post a Message and Go to Jail: Criminalizing Internet Libel in Japan and the United States." *University of Colorado Law Review* 78 (3): 767–816.

Microsoft Corporation. 2016. "Microsoft's Approach to Terrorist Content Online." *Microsoft Corporate Blogs* (blog), May 20. http://blogs.microsoft.com/on-the-issues/2016/05/20/microsofts-approach-terrorist-content-online/#sm.0000v683y7u6hf1vzq116lgebcm77.

Moody, Glyn. 2016. "Germany Plans to Remove Owner Liability for Piracy on Open Wi-Fi Hotspots — Report." Ars Technica, May 13. http://arstechnica.co.uk/tech-policy/2016/05/german-open-wi-fi-storehaftung-law-repealed.

Organisation for Economic Co-operation and Development. 2010. *The Economic and Social Role for Internet Intermediaries.* April. www.oecd.org/internet/ieconomy/44949023.pdf.

Peguera, Miquel. 2009. "The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems." *Columbia Journal of Law & the Arts* 32 (4): 481–512.

Pfanner, Eric. 2010. "YouTube Can't Be Liable on Copyright, Spain Rules." *New York Times*, September 24, B7.

Reuters. 2016a. "Brazil Court Blocks Facebook Funds Over WhatsApp Dispute: Report." Reuters, June 30. www.reuters.com/article/us-brazil-facebook-whatsapp-idUSKCN0ZH3EX.

———. 2016b. "Israeli Minister Says Facebook a 'Monster', Hindering Security." Reuters, July 2. www.reuters.com/article/us-israel-facebook-idUSKCN0ZI0XB.

———. 2016c. "Iran Orders Social Media Sites to Store Data Inside the Country." Reuters, May 29. www.reuters.com/article/internet-iran-idUSL8N18Q0IN.

Risen, Tom. 2016. "Turkey Censors News, Social Media After Terrorist Attack." *US News*, June 29. www.usnews.com/news/articles/2016-06-29/turkey-censors-news-twitter-facebook-after-terror-attack.

Senftleben, Martin. 2010. "Bridging the Differences between Copyright's Legal Traditions — The Emerging EC Fair Use Doctrine." *Journal of the Copyright Society of the USA* 57 (3): 521–52.

Swiss Institute of Comparative Law. 2015. "Comparative Study on Blocking, Filtering and Take-Down of Illegal Content." ISDC, December 20. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168068511c.

Tanaka, Hisanari Harry. 2001. "Post-Napster: Peer-to-Peer File Sharing Systems: Current and Future Issues on Secondary Liability Under Copyright Laws in the United States and Japan." *Loyola of Los Angeles Entertainment Law Review* 22 (1): 37–84.

Tsukayama, Hayley. 2012. "Pinterest Addresses Copyright Concerns." *Washington Post*, March 15. http://articles.washingtonpost.com/2012-03-15/business/35447213_1_ben-silbermann-pinterest-content.

United Nations. 1948. *Universal Declaration of Human Rights.* Geneva, Switzerland: United Nations. www.un.org/en/universal-declaration-human-rights/.

UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression, and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information. 2011. "Joint Declaration on Freedom of Expression and the Internet." www.osce.org/fom/78309?download=true.

Verbiest, Thibault, Gerald Spindler, Giovanni Maria Riccio and Aurelie Van der Perre. 2007. "Study on the Liability of Internet Intermediaries." November 12. http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf.

ABOUT THE AUTHOR

Anupam Chander is Martin Luther King, Jr. Professor of Law and director of the California International Law Center at the University of California, Davis. A graduate of Harvard College and Yale Law School, Anupam has been a visiting professor at Yale, Chicago, Stanford and Cornell. He is the author of *The Electronic Silk Road: How the Web Binds the World Together in Commerce* (Yale University Press). He practised law in New York and Hong Kong with Cleary, Gottlieb, Steen & Hamilton. He served on the executive council of the American Society of International Law and serves as a judge for the Stanford Junior International Faculty Forum. The recipient of Google Research Awards and an Andrew Mellon grant on the topic of surveillance, Anupam has served as a member of the International Centre for Trade and Sustainable Development and the World Economic Forum expert group on the digital economy.

CHAPTER TWO:
PATENTS AND INTERNET STANDARDS

Jorge L. Contreras

ACRONYMS

ABA	American Bar Association
ANSI	American National Standards Institute
BCP	Best Common Practice
CERN	European Organization for Nuclear Research
DARPA	Defense Advanced Research Projects Agency
DSL	digital subscriber line
ETSI	European Telecommunications Standards Institute
FRAND	fair, reasonable and nondiscriminatory
FTC	Federal Trade Commission
GSM	European Groupe Spécial Mobile
HTML	Hyper Text Markup Language
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISOC	Internet Society
ITC	International Trade Commission
ITU	International Telecommunications Union
LTE	Long-Term Evolution
MIT	Massachusetts Institute of Technology
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
NTT	Nippon Telegraph and Telephone Corporation
OASIS	Organization for the Advancement of Structured Information Standards
P3P	Platform for Privacy Preferences
PAG	Patent Advisory Group
PTO	Patent and Trademark Office (United States)
RAND	reasonable and nondiscriminatory
RF	royalty free
RFC	Request for Comments
SDO	standards-development organization
SEP	standards-essential patent
SSO	standards-setting organization
TCP/IP	Transmission Control Protocol/Internet Protocol
W3C	World Wide Web Consortium

We reject: kings, presidents and voting.
We believe in: rough consensus and running code.

– David D. Clark (1992)

INTRODUCTION

Standards and Interoperability

Technical interoperability standards are sets of protocols and design parameters that enable products manufactured by different vendors to work together with minimal user intervention. These standards are embodied in nearly every electronic and technological device today. Broadly adopted interoperability standards can produce significant efficiency-enhancing network effects and other benefits, and are integral to the modern technology infrastructure (Shapiro and Varian 1999; Lemley and Shapiro 2007).

Standards may be developed in a variety of settings. Some health, safety and environmental standards are developed by governmental agencies. Most interoperability standards, however, are developed in the private sector. Individual firms may develop proprietary technologies that, through broad market adoption, become de facto standards (for example, Adobe's "portable document format" or PDF). In several well-known cases (such as Betamax vs. VHS, HD-DVD vs. Blu-ray), competing firms have engaged in commercial "standards wars" to determine which of their proprietary formats will prevail in the market (Shapiro and Varian 1999). Over the past two decades, however, most interoperability standards have been developed by groups of market participants that collaborate within voluntary associations known as standards-development organizations (SDOs).[1] The standards produced within these organizations are often referred to as "voluntary consensus standards," as they are developed through consensus-based collaborative processes and there is no requirement that participants use the resulting standards.

The Architecture of Internet Standardization

According to the Gartner Group (2015), more than six billion devices will be connected to the Internet in 2016. The interconnection and communication of these devices is made possible by hundreds of different standards at many different technological layers. The Transmission Control Protocol/Internet Protocol (TCP/IP) data model provides an abstract representation of the four functional layers of a computing or communications system and is frequently utilized to conceptualize the different technology layers that comprise the Internet. In Table 1, the four TCP/IP layers are shown with a set of exemplary

1 The alternative term "standards-setting organization" (SSO) is also used in the literature.

Internet standards, as well as with the SDOs responsible for these standards.[2]

As Table 1 illustrates, there are three distinct groups of SDOs involved in Internet standardization at the different layers of network architecture. The first group focuses on layer 1 — network — which corresponds to physical transmission and data link technologies. These include standards for both wired connections (for example, Ethernet, DSL and ISDN [Integrated Services Digital Network]) as well as wireless connections (2G/3G/4G). The major SDOs that serve these technical areas are the European Telecommunications Standards Institute (ETSI) and the Institute of Electrical and Electronics Engineers (IEEE), although a host of smaller SDOs and trade associations are also involved in various aspects of this field. Layers 2 and 3 include the "core" Internet protocols TCP and IP. These standards are maintained by the Internet Engineering Task Force (IETF). At the application layer, the IETF is joined by the World Wide Web Consortium (W3C), primarily responsible for the HTML descriptor language, and the Organization for the Advancement of Structured Information Standards (OASIS), which focuses on software interfaces.

In order for the Internet to operate seamlessly, the standards defining each of these layers must interface with the layers immediately above and below it. While this technical compatibility has largely been achieved in today's connected devices, there are striking differences among the SDOs that operate at the network, transport/Internet and application levels. One of the largest areas of divergence among these SDOs relates to their treatment of patents.

Table 1: Internet Standardization "Stack"

Layer	Standards	SDOs
4. Application	XML (data exchange)	W3C, OASIS
	HTTP, HTML (Web)	IETF, W3C
	IMAP, POP, MIME (email)	IETF
3. Transport	TCP, UDP	IETF
2. Internet	IPv4, IPv6, ICMP, ARP	IETF
1. Network	Ethernet, DSL, Wi-Fi, X.25	IEEE
	3G/4G	ETSI

Note: Acronyms used in this table: ARP — Address Resolution Protocol; DSL — digital subscriber line; HTTP — Hypertext Transfer Protocol; HTML — Hyper Text Markup Language; ICMP — Internet Control Message Protocol; IMAP — Internet Message Access Protocol; IPv4, IPv6 — IP version 4, IP version 6; MIME — Multi-Purpose Internet Mail Extensions; POP — Post Office Protocol; UDP — User Datagram Protocol; XML — Extensible Markup Language. *Source:* Author.

PATENTS AND STANDARDS

SEPs

A patent is a form of governmental grant that gives its owner the exclusive right to practise (i.e., make, use and sell) a claimed invention throughout the issuing country. Patent protection in most countries lasts for a period of 20 years from the date a patent application is filed. Patents may cover any system, device, product feature, process or improvement, so long as it is useful, novel and not obvious in view of existing technologies. These basic features of patent law are applicable in most developed countries through treaties including, most importantly, the Agreement on Trade-Related Aspects of Intellectual Property Rights (known as the TRIPS agreement).[3] In some countries, including the United States, patents are authorized for the express purpose of promoting innovation and scientific progress.[4]

While patents have historically covered new machines, compositions of matter and industrial processes, patents covering intangible inventions such as software and methods of doing business began to emerge in the last half century. In the early 1970s in the United States, the Supreme Court began to consider the patentability of inventions embodying computer software. In *Gottschalk v Benson* (1972)[5] and *Parker v Flook* (1978),[6] the Court rejected patents claiming software-based inventions on the ground that they constituted unpatentable mathematical algorithms. But in *Diamond v Diehr* (1981),[7] the Court allowed a patent for an improved method of curing rubber based on a known equation, reasoning that the method should not be rendered patent-ineligible simply because it relied on a mathematical algorithm. This holding opened the door to an increasing number of software-based patents, which were regularly affirmed by the Court of Appeals for the Federal Circuit, a specialized appellate court formed in 1982 for the purpose, among other things, of hearing

2 Table 1, of course, grossly oversimplifies the vast array of standards and SDOs involved in Internet technologies. In addition to the listed SDOs, at every layer there are numerous smaller consortia and industry collaborations that may compete or cooperate with the listed SDOs.

3 *Agreement on Trade-Related Aspects of Intellectual Property Rights*, 15 April 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 108 Stat 4809, 1869 UNTS 299.

4 Article I, Section 8, Clause 8 of The US Constitution authorizes Congress to "promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries" (US Const, art I, § 8, cl 8).

5 409 US 63 (1972).

6 437 US 584 (1978).

7 450 US 175 (1981).

appeals of patent cases. By the late 1990s, patents on so-called "business methods" were also being recognized by the courts following the Federal Circuit's decision in *State Street Bank & Trust v Signature Financial*.[8]

While recent US Supreme Court decisions are believed to have substantially limited the ability to patent both software and business methods,[9] it is estimated that at least 11,000 Internet-related business method patents are still in force in the United States (Rustad 2014). Outside of the United States, patents on software and business methods are less common, although they may often be upheld if they are tied to a "technical effect" or other outcome in the bricks and mortar world (Adelman et al. 2011).

Like other technologies, the product interface protocols and interoperable designs specified by technical standards are often covered by patents. Most of these patents are owned by one or more firms engaged in the standards-development process.[10] Patents that will always be infringed by a product conforming to a particular standard are referred to as standards-essential patents or SEPs. Complex technological products may implement dozens or even hundreds of standards (Biddle, White and Woods 2010), each of which may be covered by hundreds or thousands of SEPs (Blind et al. 2011). The result is a very large number of patents covering different aspects of certain standards.

Patent Concerns: The Debate over Hold-up and Stacking

The existence of patents covering standards is not inherently problematic, and many argue that the availability of patents provides the financial incentives necessary to fund significant advances in technology. However, once a standard is adopted, patents reduce the ability of competitors to create compatible products and may raise prices for consumers (Scotchmer 2006). Patents are thus two-edged swords when it comes to standardization: they have the potential to tip the balance of benefits and burdens sharply in favour of one group or another.

In the recent literature, commentators have observed two scenarios in which the balance of equities may tip too far in the direction of patent holders: royalty stacking and patent hold-up. Royalty stacking is a type of collective action problem that can occur when multiple SEP holders each charge a royalty to the manufacturer of a standards-compliant product. While any given royalty, viewed individually, might be reasonable and within market norms, the aggregate royalty burden on the product, accounting for hundreds or thousands of SEPs, could be excessive. For example, in *Microsoft v Motorola*, the court observed that

> there are at least 92 entities that own 802.11 SEPs. If each of these 92 entities sought royalties similar to [the patent holder's] request of 1.15% to 1.73% of the end-product price, the aggregate royalty to implement the 802.11 Standard, which is only one feature of the Xbox product, would exceed the total product price.[11]

Such royalty stacking could, if not curbed, impose barriers to market entry, raise prices for consumers and reduce innovation in product markets (US Department of Justice and US Federal Trade Commission [FTC] 2007).

Patent hold-up refers to a scenario in which a SEP holder may demand excessive royalties after product manufacturers have made significant investments in a standardized technology. Once such investments have been made, these manufacturers are said to be "locked-in" to the standard (Shapiro and Varian 1999; Farrell et al. 2007). In such cases, the cost of switching from the standardized technology to an alternative may be prohibitive, dramatically increasing a patent holder's leverage in any ensuing licensing negotiation and enabling it to charge excessive royalties (Farrell et al. 2007; Lemley and Shapiro 2007).

A heated debate is currently under way regarding whether patent hold-up and royalty stacking are legitimate threats to standardization and technology markets, or whether they are mere theoretical possibilities.[12] Some argue that there is little empirical evidence of these market failures in the vibrant and rapidly advancing telecommunications marketplace, where prices continue to fall, product capabilities continue to expand and new market entrants continue to appear from all corners of the globe (Galetovic, Haber and Levine 2015). Others, however, respond that there is substantial empirical evidence for the general theory of hold-up, that its application to SEP markets is particularly salient and that evidence of hold-up in these markets is difficult to obtain primarily due to confidentiality restrictions placed on licensing agreements by the parties.[13] It may also be the case that, whatever the theoretical risk of

8 149 F (3d) 1368 (Fed Cir 1998).

9 *Bilski v Kappos*, 561 US 593 (2010); *Alice Corp. v CLS Bank International*, 573 US __, 134 S Ct 2347 (2014).

10 SDOs typically hold no patent rights in the standards that they produce.

11 *Microsoft Corp. v Motorola, Inc.*, Findings of Fact and Conclusions of Law, 2013 US Dist Lexis 60233 (WD Wash, 25 April 2013). See also *Ericsson Inc. v D-Link Sys.*, 773 F 3d 1201, 1209 (Fed Cir 2014).

12 Some of this literature is summarized in Contreras (forthcoming, 2016a).

13 The author thanks Carl Shapiro for these insights.

patent hold-up and royalty stacking is in an unregulated SEP market, affirmative measures already taken by SDOs and enforcement agencies may have reduced the occurrence of these behaviours, demonstrating not that hold-up and stacking are not serious issues, but that they must continue to be policed to prevent future occurrences.[14]

SDO Patent Policies

Many SDOs have adopted internal policies intended to reduce the possibility of royalty stacking and patent hold-up. While such policies existed as early as the 1950s (Contreras 2015b), SDO patent policies began to assume their current forms in the late 1990s, prompted by a settlement that Dell Computer reached with the FTC.[15] In this case, the FTC accused Dell of engaging in unfair methods of competition by seeking to enforce patents against implementers of a video bus standard after a Dell engineer had signed a statement certifying that Dell held no patents essential to the standard. In the settlement reached with the FTC, Dell agreed not to assert its patent against any third party implementing the standard.

A second wave of policy revisions occurred in the early 2000s, following litigation involving semiconductor design firm Rambus.[16] In that litigation, the FTC accused Rambus of engaging in anticompetitive practices by concealing — and later seeking to enforce — patents that it otherwise should have disclosed to an SDO. Although Rambus eventually prevailed on technical antitrust law grounds, the case underscored the importance of drafting extremely clear and detailed SDO patent policies.

The result is that today, almost all SDO patent policies impose one or both of the following obligations on SDO participants: an obligation to disclose patents essential to implementation of a standard, and/or an obligation to license patents essential to implementation of a standard, either on a royalty-free (RF) basis, or on a royalty-bearing basis at rates that are "fair, reasonable and nondiscriminatory" (FRAND) (synonymous with "reasonable and nondiscriminatory" [RAND]).[17]

Yet within these parameters, large differences exist among SDO patent policies. These differences can be observed when comparing SDOs in the different layers described in Table 1. Thus, SDOs in the network layer — including ETSI, the International Telecommunications Union (ITU) and the IEEE — typically permit their participants to charge FRAND royalties for SEPs covering the SDO's standards. The primary transport/Internet SDO, the IETF, permits royalties to be charged, but has strong informal norms favouring RF licensing. And application-focused SDOs such as W3C and OASIS largely produce standards subject to RF licensing commitments.[18]

The reasons for these distinctions and what they mean in practice are explored in the remainder of this chapter. For the sake of expediency, the chapter refers to "Internet" standards as the network and software layer standards that define the Internet and the World Wide Web, as the network standards published by ETSI, the IEEE and others have utility in a wide range of applications beyond the Internet (such as mobile telephony, computer networking, and so on).

NETWORK VS. INTERNET STANDARDS: OBSERVED DIFFERENCES IN PATENT DECLARATION AND ENFORCEMENT

Despite the precautionary policy measures taken by many SDOs, over the past decade voluntary consensus standards have become the subject of significant private litigation, regulatory enforcement and policy debate around the world. As one senior US government official lamented in a 2012 address to the ITU, "The world... is awash in lawsuits related to patented technologies" (Hesse 2012, 9).

But although there is a natural tendency to paint all technologies in the information and communications technology sector with the same brush, there are dramatic differences among fields when patents are concerned. Recent studies have shown that the most SEPs have been disclosed, and the most SEP-related lawsuits have been brought, in the wireless telecommunications area. Justus Baron and Tim Pohlmann (2015) collected more than 200,000 patent disclosures from 19 major SDOs. Of these, nearly 170,000 patent disclosures (84 percent) were

14 In this respect, the situation can be analogized to that of Ebola outbreaks in the United States. As of this writing, there is no evidence of a serious Ebola outbreak in the United States. However, this does not mean that Ebola is not a threat to the public health (as there is ample evidence of its seriousness from other jurisdictions). Rather, the absence of Ebola infection in the United States is a credit to its public health agencies and health care facilities, which have carefully monitored, contained and addressed potential outbreaks.

15 In re. *Dell Computer Corp.*, 121 FTC 616 (1996).

16 In re. *Rambus, Inc.*, 2006 WL 2330117, 2006-2 Trade Cas. 75364 (FTC, 2 August 2006), rev'd, 522 F (3d) 456 (DC Cir 2008).

17 In addition to constraints on royalty rates, most SDO patent policies contain a number of additional provisions (Bekkers and Updegrove 2012; ABA 2007; Lemley 2002).

18 More detailed comparisons of the terms of different SDO patent policies can be found in Bekkers and Updegrove (2012) and Lemley (2002).

made at ETSI alone. In contrast, only 667 patents were disclosed as essential to Internet standards developed at the IETF.

Similar contrasts between network and Internet standards emerge when SEP-related litigation is examined. Although the potential for conflict over the setting of FRAND royalty rates was recognized as early as the mid-1990s (Shurmer and Lea 1995, 386), litigation over the level of FRAND royalties did not become a significant phenomenon until five years ago. For example, in both *Apple v Motorola* and *Microsoft v Motorola*, the SEP owner (Motorola) offered to license SEPs covering two widely adopted standards at rates that the potential licensees argued were far in excess of reasonable levels and thus in violation of Motorola's FRAND commitments. In both cases, the manufacturers of standards-compliant products brought breach of contract actions against the SEP owner for the alleged violation of its FRAND commitments, among other things.

Table 2 shows all SEP-related cases that reached judgment in the US federal courts and International Trade Commission (ITC), as well as in courts in Europe and China, as reported by the Essential Patent Blog.[19]

As Table 2 illustrates, all cases pertained to network standards, either in the field of telecommunications (ETSI and ITU), or computing (Bluetooth and IEEE's 802.11 Wi-Fi standard). Notably absent from the SEP litigation picture, however, are standards pertaining to the Internet/application layers.

At first blush, the lack of patent acquisition and litigation surrounding Internet standards is surprising. After all, nearly every computer, smartphone and tablet in the world communicates via the Internet, and the market for Internet-enabled devices is enormous, suggesting that potential verdicts might present lucrative incentives for litigation. Why, then, have the patenting and litigation trends observed among network technologies not affected the Internet? The remainder of this chapter addresses this question.

Table 2: Recent Reported Decisions Involving SEPs (2012–2015)

Case	Court(s)	SDO/Standards
Microsoft v Motorola (2012)	W.D. Wash. (jury) 9th Cir.	ITU H.264 IEEE 802.11
Apple v Motorola (2012)	W.D. Wis. N.D. Ill. Fed. Cir.	ETSI UMTS, GPRS IEEE 802.11
Apple v Samsung (2013)	N.D. Cal. (jury) Fed. Cir. ITC	ETSI UMTS
Golden Bridge v Apple (2013)	D. Del.	GSMA W-CDMA (part of ETSI UMTS)
In re Innovatio IP Ventures (2013)	N.D. Ill.	IEEE 802.11
Wi-LAN v Apple (2013)	E.D. Tex. (jury)	ITU CDMA2000 IEEE 802.11
IPCom v Apple (2014)	Germany — Mannheim	ETSI UMTS
NXP v Blackberry (2014)	M.D. Fla. (jury)	IEEE 802.11 JEDEC e.MMC
InterDigital v Huawei, Nokia, ZTE, Nokia (2014, 2015)	ITC D. Del. China — Shenzhen	ETSI UMTS ETSI LTE ITU CDMA2000
Fujitsu v Tellabs (2014)	N.D. Ill. (jury)	ITU G.692
LSI v Realtek (2014)	N.D. Cal. (jury) 9th Cir. ITC	IEEE 802.11
Ericsson v D-Link (2014)	E.D. Tex. (jury) Fed. Cir.	IEEE 802.11
Rembrandt v Samsung (2015)	E.D.Tex (jury)	Bluetooth Special Interest Group
CSIRO v Cisco (2015)	E.D. Tex. Fed. Cir.	IEEE 802.11
Huawei v ZTE (2015)	CJEU	ETSI LTE

Note: Acronyms used in this table: CJEU — Court of Justice of the European Union; e.MMC — Embedded MultiMediaCard; GPRS — General Packet Radio Service; GSMA — GSM Association; W-CDMA — Wideband Code Division Multiple [or Multiplexing] Access. CDMA2000 is a family of third-generation mobile technology standards.
Source: Author.

19 Beginning in February 2012, the Essential Patent Blog (www.essentialpatentblog.com) has tracked law and policy developments relating to SEPs and related issues. The cases in Table 2 are limited to those resulting in reported judicial decisions, which represent a small minority of the totality of SEP-related cases that are brought. For a more complete picture of SEP litigation relating to seven widely adopted standards (European Groupe Spécial Mobile [GSM], Universal Mobile Telecommunications System [UMTS], Long-Term Evolution [LTE], H.246, 802.11, Bluetooth and USB), see Contreras (forthcoming, 2016b). For a census of all FRAND-related litigation brought through 2012, see Contreras (2013b).

WHAT THE INTERNET IS NOT (YET)[20]

In many respects, the differences in patenting and standardization practices between the network and Internet/application layers may be explained by differences in their historical development and technical architectures. While the layperson may see no discernible difference between the 4G LTE standard that enables his or her smartphone to connect to a mobile network and the TCP/IP protocols that define the size and configuration of the data packets that traverse that network, these two technical areas exist across a significant gulf of history that has shaped the policies and norms that characterize these industries today.[21]

Telecommunications Technology and Patents

Differences in patenting patterns among network and Internet/application layer technologies may, in part, be explained by inherent technological differences between these layers. Lower-level network technologies, which are more closely tied to physical hardware, may be more susceptible to patent protection than higher-level Internet and application layer technologies, which are more akin to software-based inventions, for which patents may be less common[22] (Lehr 1995). Moreover, wireless telecommunications technologies have generally evolved in discrete generations, each lasting several years (for example, 2G to 3G, 3G to 4G), with each upward shift requiring significant infrastructural, manufacturing and marketing expenditures. Given these costs, the incremental cost of even heavy patenting could appear both small in comparison to overall expenditures, and worthwhile, to protect those sunk investments.

In addition to dealing with technologies that may generally be more prone to protection by patents, holders of patents in the network area may be more likely to declare even marginal patents as essential to network-based standards. Studies by David J. Goodman and Robert A. Myers (2005) and Fairfield Resources, Inc. (2007) have found that only 27 percent and 28 percent of patent families declared as "essential" to ETSI's GSM and W-CDMA standards, respectively, are actually essential to implementation of those standards. Interviews conducted by Knut Blind et al. (2011) also point to widespread over-disclosure of patents at SSOs.[23] In addition to over-disclosure, higher levels of patent declaration at ETSI could arise from factors such as the intentional inclusion of optional and non-essential patented features in ETSI standards, more feature-rich standards in general and greater granularity in patent claim drafting.[24]

The Roots of Telecommunications Standardization

Standardization in the telecommunications sector began not as a cooperative effort among competing firms, but as a (largely successful) attempt by national telephone monopolies to preserve their control over the industry. This approach was epitomized by AT&T in the United States, which operated under the telling slogan "One System, One Policy, Universal Service" (Russell 2014, 97; Wu 2010, 51). As described in detail by Andrew Russell (2014), AT&T standardized many aspects of the US telephony system to ensure that it could obtain a consistent and reliable supply of components from subcontracted manufacturers and to enable local exchanges to connect to its long-haul lines and thereby avoid competition in the long-distance market (ibid.).

Other national operators in Europe and Asia exerted similar levels of control. In Japan, for example, telecommunications standardization was largely driven by its century-old national telecommunications monopoly, Nippon Telegraph and Telephone Corporation (NTT). For decades, NTT, with the backing of the Japanese government, designed Japan's telecommunications infrastructure and supported a dedicated "family" of equipment manufacturers including Hitachi, Fujitsu and NEC (Kushida 2008). The NTT network was, until recently, characterized by proprietary standards developed in NTT's research labs and mandated by the national Ministry of Posts and Telecommunications for deployment by NTT's dedicated suppliers (ibid.).

In most countries, wireless telecommunications were not as heavily regulated as wireline communications, but scarce spectrum still invited governmental allocation and control, and standards were adopted at national and regional levels (Cowhey, Aronson and Richards 2006; Shurmer and Lea 1995). The contest among competing technologies frequently involved wrangling over patents. While first-generation analog wireless technologies

20 The title of this section owes a debt to Jonathan Zittrain's influential 2009 book *The Future of the Internet — And How to Stop It*, a cautionary tale about the direction that the Internet could take under increased regulation.

21 A decade ago, Suzanne Scotchmer (2006) recognized the fundamental differences between Internet and telecom standards, even before the most recent wave of SEP-related litigation. Yet the debate today has lost sight of many of these distinctions.

22 See the section on SEPs above.

23 There are several possible reasons that over-disclosure of patents may occur at SSOs. For example, SSOs may require declaration of patents at the application stage, before the actual scope of claims are known. Moreover, antitrust enforcement agencies have brought actions against firms that allegedly failed to disclose patents essential to particular standards, thus creating a significant motivation to disclose all patents that might, under any interpretation, be considered essential. See Contreras (2013b) for a more detailed discussion of these possible motivations.

24 This area is ripe for further empirical study.

represented a patchwork of largely incompatible, vendor-specific technical approaches, by the early 1980s the industry recognized the need for second-generation or 2G digital wireless telecommunications standards that would support both voice and data communications.

In Europe, ETSI was the focal point for the development of 2G and subsequent wireless standards. It was clear beginning in the late 1980s that patent issues at ETSI would be contentious, leading to a series of policy amendments and debates within the organization (Shurmer and Lea 1995, 391–93). During that period, Ericsson promoted a 2G standard based on time-division multiplex access technology, which eventually led to the GSM standard. Ironically, the largest holder of SEPs in GSM technology was Motorola, a US firm that conducted significant research and development operations in Europe (Bekkers, Verspagen and Smits 2002). A competing 2G proposal was advanced by a coalition of French and German firms, which had strong patent positions in their own technology (ibid.). Before this coalition agreed to support GSM at the newly formed ETSI, technology covered by some of these patents had to be included in the standard (Lundqvist 2014, 59). By the time GSM was approved by ETSI in 1990, five firms (Ericsson, Nokia, Siemens, Motorola and Alcatel) held broad patent coverage of the standard (Bekkers, Verspagen and Smits 2002).

The situation in the United States was less fractured, but even more patent-centric, as Qualcomm's CDMA technology became the basis for the leading 2G standard (Lundqvist 2014, 59). And, as noted above, each successive generation of wireless telecommunications standards has been burdened with more patents, opening the way for further disputes and litigation.

The Early Internet and Patenting

In contrast to telecommunications and other network technologies, the Internet was designed as a hardware-neutral set of protocols for connecting heterogeneous computer networks. It was initially conceived and funded by the US Department of Defense though its Defense Advanced Research Projects Agency (DARPA, also known as the Advanced Research Projects Agency, or ARPA; the agency changed its name periodically).[25] The project sought to design a reliable and resilient computer network that did not rely on the then dominant circuit-switched technology.[26] Building on theoretical work done at the Massachusetts Institute of Technology (MIT) and the Rand Corporation in the early 1960s, host computers at the University of California, Los Angeles; Stanford; University of California, Santa Barbara; and the University of Utah were connected in 1969 to form a prototype packet-switched network known as ARPANET. In 1973, Robert Kahn at DARPA and Vint Cerf at Stanford University developed the TCP/IP protocols to enable ARPANET to connect with other computer networks, laying the groundwork for the modern Internet.[27]

The pioneers of the Internet were employed primarily by the US government, its academic collaborators and a handful of private contractors (such as the Cambridge, MA-based Bolt, Beranek and Newman), leading to a distinctly non-commercial culture (Nickerson and zur Muehlen 2006). Large firms such as IBM and AT&T that were heavily invested in patenting activity were not part of the early Internet (Russell 2014). And in the days before the Bayh-Dole Act of 1980,[28] which provided a framework for patenting federally funded inventions, universities and federal agencies engaged in only sporadic patenting activity. Compounding this general disregard for patents was the legal understanding during the 1960s and 1970s that computer software and algorithms, the regime in which Internet standards were being developed, were simply not patentable (see the section on SEPs above). The combination of these factors resulted in few patents being filed on the fundamental protocols that defined the Internet (Weitzner 2004).

As personal computers, workstations and local area networks proliferated in the 1980s, the Internet expanded

25 The origins of the world's largest network have been documented many times. See, for example, Hafner and Lyon (1996), Segalier (1998), Wu (2010), Russell (2014) and DeNardis (2014).

26 Paul Baran at the Rand Corporation was one of the early theorists of distributed computing. He believed that a distributed network was more likely to survive a nuclear attack than a network dependent on end-to-end switching, as the existing AT&T network was. See Baran (1964), in particular the memorandum "directed toward examining the use of redundancy as one means of building communications systems to withstand heavy enemy attacks." See also Hafner and Lyon (1996, 54–58). Some recent commentators have questioned whether nuclear survival was the driving force behind ARPANET, arguing instead that developing remote time-sharing capability was the primary motivation for DARPA's interest in distributed computing. See, for example, Ian Peters' "History of the Internet," at www.nethistory.info/History%20of%20the%20Internet/beginnings.html.

27 The original TCP protocol was published in December 1974 as Request for Comments (RFC) 675, and the IP protocol was published in 1981 as RFC 791. The IETF document series extends back to a series of academic RFCs first published in 1968. The term RFC has in recent years lost its meaning and now simply refers to the definitive standards and reference document series published by the IETF. See DeNardis (2014, 71-72).

28 *Patent and Trademark Law Amendments Act* (Pub L 96-517, 12 December 1980). The Bayh-Dole Act both authorized and encouraged universities and other government contractors to patent inventions funded by federal agencies. Prior to the act, there was no uniform federal policy regarding patenting of federally funded inventions, and most of these inventions were not patented.

in size and popularity. Yet, despite its growing usage among businesses and the general public, Internet standards remained hardware-neutral and relatively lean.[29] This ongoing separation from the patent-rich hardware network layer may have left key design features of the Internet as less obvious targets for patenting, even by the commercial enterprises that soon became integral to its development and deployment, and even after the emergence of software and business method patents in the 1980s and 1990s.

THE IETF

The Origins and Growth of the IETF

Prior to 1985, technical work relating to the Internet was carried out in a series of task forces chaired by leading researchers at DARPA and a few universities. In 1985, this activity was placed under the umbrella of a new, loosely organized body — the IETF. Around this time, Kahn and other leaders of the Internet project departed from DARPA, leaving the IETF and its sister organization, the Internet Activities Board (now the Internet Architecture Board, known as the IAB), to chart the future direction of the Internet.

As the Internet grew in popularity and usage, commercial users rapidly began to outnumber academic and government users. In order to create an organization in which commercial, academic and government representatives could collaborate, a non-profit corporation called the Internet Society (ISOC) was formed in 1992 (Lehr 1995, 153; DeNardis 2014, 70). ISOC became the "organizational home" of the IETF in 1996 and still provides administrative, personnel and financial support to the IETF.[30]

Participation in the IETF is, and always has been, on an individual basis, although firms often sponsor attendance and participation by their employees. In recent years, more than a hundred different working groups have been operational within the IETF at any given time (Hoffman 2012), and between 1,200 and 1,500 individuals regularly attend its meetings, which are held three times a year (Contreras 2014). The IETF is famously open and transparent (Whitt 2013; Froomkin 2003; Lessig 2001). Almost all proceedings, documents and records are freely available on the IETF website, and anyone who is interested may join a technical working group. Documents that advance through the "standards track" are based on open consensus processes overseen and managed by a group of semi-elected area directors and other leaders. The IETF standardization process is largely bottom-up, wherein technical proposals are generated by individual participants who must defend and advocate their proposals both in written email communications and at in-person IETF meetings.

While the IETF's open culture and transparent procedures have been applauded (Froomkin 2003), they have also shown weaknesses. Most notably, the speed of standardization at the IETF has flagged, and the organization has become notorious for lengthy technical debates and delays (Simcoe 2007). As discussed below, this slowdown contributed to Tim Berners-Lee's formation of W3C as an independent organization in 1994.

Patents at the IETF

Evolution of the IETF Patent Policy

The IETF's first formal policy regarding patents[31] was adopted in 1992 to accommodate the growing community of commercial Internet users. This policy, largely mirroring the language of the American National Standards Institute's (ANSI's) patent policy,[32] contained a rudimentary FRAND or RF licensing requirement.

Patents played little role in IETF deliberations until 1995, when Motorola disclosed patents claiming features of the PPP[33] Compression Control Protocol (known as CCP, RFC 1962) and PPP Encryption Control Protocol (known as ECP, RFC 1968) (Simcoe 2007).[34] Motorola initially refused to commit to license these patents to users of the PPP standards, leading to significant opposition within the IETF working group.[35] The IETF eventually published the PPP standards with the patented technology, but only after

29 As explained by Lehr (1995, 137), Internet standards tend to support "minimal functionality at least cost," in contrast to hardware-specific standards supporting a range of specialized services.

30 See RFC 2031, "IETF-ISOC Relationship" (1996), https://tools.ietf.org/html/rfc2031.

31 RFC 1310, "The Internet Standards Process" (March 1992), https://tools.ietf.org/html/rfc1310.

32 Although ANSI is not itself an SDO, it accredits US SDOs as developers of American national standards. Among ANSI's requirements for accredited SDOs, which are embodied in its *Due Process Requirements for American National Standards*, are rules regarding the way that accredited SDOs must handle patents held by their participants (see *ANSI Essential Requirements: Due Process Requirements for American National Standards*, ANSI, § 3.1.1 [January 2015]). Although the IETF is not an ANSI-accredited SDO, its first patent policy was borrowed largely from the ANSI *Essential Requirements*.

33 PPP refers to Point-to-Point Protocol. The PPP CCP and PPP ECP are known collectively as the PPP standards.

34 One earlier patent disclosure at the IETF was made in 1993 by the National Institute of Standards and Technology (NIST) relating to a patent covering its Digital Signature Algorithm. However, NIST committed to license the patent to users worldwide on an RF basis, eliminating any serious concern. See Reported Statement from NIST Regarding Use of DSA (23 July 1993), https://datatracker.ietf.org/ipr/449/.

35 See IETF Working Group mail archive at https://groups.google.com/forum/#!msg/info.ietf/raixEKiWbMc/IPK9BQuXjnoJ.

Motorola agreed to offer implementers of the standard licenses on RAND terms.[36]

The PPP incident led the IETF to review and revise its patent policy as part of a 1996 overhaul of its standardization procedures (RFC 2026). The 1996 policy departs from the IETF's earlier RAND/RF licensing commitment; it only requires that participants disclose the existence of known patents covering IETF standards,[37] but not that the patents be licensed on any particular terms. The IETF's current policy (contained in RFC 3979 and subsequent addenda, collectively known as Best Common Practice [BCP] 79) preserves this disclosure-only approach.[38]

The IETF's Preference for RF

Given IETF participants' discomfort with Motorola's RAND licensing proposal for PPP, it may seem curious that the IETF elected to adopt a policy with no licensing commitment at all. That is, the IETF's 1992 policy at least contained an upper bound on royalties charged by participants ("reasonableness"), whereas the 1996 policy gives SEP holders carte blanche to charge anything they wish, or even to withhold licenses entirely.

But this seeming flexibility is, in practice, an illusion. Rather than empower SEP holders to charge high or unreasonable royalties for their patents, it actually discourages them from charging anything at all. How? If an SDO policy expressly permits a SEP holder to charge RAND royalties, then such royalties are effectively condoned by the organization. But if a policy neither permits nor prohibits royalties, then all decisions regarding royalty-bearing technologies will be pushed down to the organization's working groups. As such, the IETF continues to exhibit a strong preference for RF standards. It does so in two ways: through express statements of preference in BCP 79 and elsewhere, and through working group deliberations.

RF Policy Preferences

While the IETF does not require its participants to commit to license their patents on any particular terms, reasonable or otherwise, it does express a preference for RF standards in many contexts. For example, according to Section 8 of BCP 79,

> In general, IETF working groups prefer technologies with no known [patent] claims or, for technologies with claims against them, an offer of royalty-free licensing. But IETF working groups have the discretion to adopt technology with a commitment of fair and non-discriminatory terms, or even with no licensing commitment, if they feel that this technology is superior enough to alternatives with fewer [patent] claims or free licensing to outweigh the potential cost of the licenses.[39]

Thus, the preference for RF standards at the IETF is just that: a preference, and one that is not universally shared. However, the express statement of that preference is telling.

Additional evidence of the IETF community's preference for RF is displayed in connection with specific technology areas, such as Internet security. In these areas, which are viewed as critical for Internet integrity, the institutional preference for RF standards is articulated more strongly:

> An IETF consensus has developed that no mandatory-to-implement security technology can be specified in an IETF specification unless it has no known [patent] claims against it or a royalty-free license is available to implementers of the specification unless there is a very good reason to do so.[40]

Thus, while the IETF lacks strict positive rules requiring RF standards, these statements are reflective of broadly held community norms. Accordingly, while room is left for the IETF to adopt an Internet security standard that is subject to royalties if "there is a very good reason to do so," it does not appear that such a reason has ever been found.

Working Group Deliberations

IETF working groups are charged with considering and evaluating the implications of patent burdens on technologies being considered for standardization.

36 See RFC 1915, "Variance for the PPP Connection Control Protocol and the PPP Encryption Control Protocol" (1996), https://tools.ietf.org/html/rfc1915.

37 As noted in the section "Origins and Growth of the IETF" above, participation in the IETF is on an individual, rather than an organizational, basis. Thus, individual IETF participants must disclose any patents held or controlled by themselves or by their employers or sponsors. RFC 3979, "Intellectual Property Rights in IETF Technology," Sec 6.1 (2005), https://tools.ietf.org/html/rfc3979. However, because individuals must only disclose patents "reasonably and personally" known to them, it is possible that some relevant patents held by an organization may not be required to be disclosed by an individual employee of that organization. The author is unaware of such a situation ever having become an issue at the IETF.

38 IETF patent disclosures are published and archived at www.ietf.org/ipr.

39 RFC 3979, "Intellectual Property Rights in IETF Technology," Sec 6.1 (2005), https://tools.ietf.org/html/rfc3979.

40 Ibid., Sec. 8.

RFC 3669, which offers guidance to IETF working groups, states that

> every working group…needs to take [intellectual property rights] seriously, and consider the needs of the Internet community and the public at large, including possible future implementers and users who will not have participated in the working group process when the standardization is taking place.[41]

In addition to statements of preference in IETF policy documents, IETF participants and working groups exhibit their own preferences for RF standards in the selection of technical proposals for standardization. The fact that patents must be *disclosed* to the IETF early in the standardization process enables participants to evaluate the extent to which patented technologies may be essential to standards under development. If the members of a working group do not wish to include a patented technology in the standard, they have the opportunity to redesign the standard to avoid the relevant patents.

Thus, while explicit group negotiation of patent royalty rates is discouraged,[42] working group members are advised to consider the potential impact of proposed licensing terms on the usefulness of a technology under consideration for standardization.[43] In practice, IETF working group participants have exhibited a keen awareness of which technical proposals are burdened by potential patent royalties and take this information into account when designing standards.[44]

Voluntary Licensing Disclosures

Decisions regarding the inclusion of patented technologies in IETF standards is facilitated by voluntary disclosures that SEP holders may make regarding their licensing intentions. Thus, while patent disclosures at the IETF must contain certain key information such as patent numbers or affected standards, the IETF also permits the disclosure of additional relevant information. Accordingly, many IETF participants make express licensing commitments in their patent disclosures.[45] These can include commitments to license the disclosed SEPs on RAND or RF terms, as well as broad commitments not to assert patents in particular contexts.

Not surprisingly, given IETF's stated preferences, many voluntary licensing commitments indicate that RF licensing of SEPs will be offered. In a study covering the period 2007–2010, Jorge L. Contreras (2013a) analyzed 481 patent disclosures made at the IETF, covering a total of 594 different standards documents. Of these disclosures, 283 (59 percent) contained voluntary commitments to license the disclosed SEPs on RF terms or the equivalent. These data reveal strong community alignment behind the elimination of patent encumbrances on IETF standards.

The strength of the IETF's community norms around RF patent licensing is further exemplified by the agreement even of IETF participants with well-known patent monetizing programs not to assert their SEPs under certain circumstances.[46]

W3C

The Origins of W3C

By the late 1980s, the European Organization for Nuclear Research (CERN) was a key European Internet node (DeNardis 2014, 74). Around 1989 Tim Berners-Lee, a young software engineer at CERN, began work on improving the Internet's user interface to facilitate scientific collaboration and data exchange both within CERN and with external collaborators. In doing so he developed HTTP and HTML,[47] which became the foundational protocols for the World Wide Web. Berners-Lee, heavily influenced by the open source software movement, released his code online in 1991 (Russell 2011).

The graphically oriented World Wide Web was a significant improvement over existing text and directory-based file sharing systems such as Gopher and FTP.

41 RFC 3669, "Guidelines for Working Groups on Intellectual Property Issues" Sec. 5 (2004), https://tools.ietf.org/html/rfc3669#section-5.

42 Potential antitrust concerns arise in the context of such group negotiations. Non-lawyer IETF working group leaders do a good job of curbing these discussions. See, for example, the 2009 email list discussion of the Robust Header Compression standard, in which a working group leader writes, in typical tongue-in-cheek IETF fashion, "please do *not* discuss specific patents/patent claims on the mailing list, as such a discussion might require a number of contributors to unsubscribe and stop contributing. (It might also cause you or your employer to become liable for damages in interesting ways.)…If you want to discuss this, meet in a hallway and make sure no microphones are nearby." See www.ietf.org/mail-archive/web/rohc/current/msg05691.html.

43 See IETF, RFC 3669, "Guidelines for Working Groups on Intellectual Property Issues" at Sec. 5.6 (2004).

44 For examples of potential patent issues considered by IETF working groups, see IETF, RFC 3669 "Guidelines for Working Groups on Intellectual Property Issues" at Sec. 4 (2004) (detailing patent issues arising in connection with standardization efforts for IP Storage, Privacy-Enhanced Mail and public key infrastructure, Virtual Router Redundancy Protocol and Secure Shell).

45 The enforceability of such commitments in the absence of a formal contractual framework is discussed in Contreras (2015a).

46 See, for example, https://datatracker.ietf.org/ipr/2554/, in which Qualcomm commits not to assert SEPs against implementers of IETF RFC 6330 so long as the standard is not implemented in a device that uses a wireless wide-area standard (for example, a mobile phone).

47 HTML is an application of International Organization for Standardization Standard 8879:1986 Information Processing Text and Office Systems; Standard Generalized Markup Language (Berners-Lee and Connolly 1995).

Enthusiasm for the Web grew rapidly among academic researchers. Berners-Lee, aware that researchers were likely to tinker with and improve his original Web protocols, recognized the need to standardize the technology to avoid fragmentation and proliferation of incompatible versions. His first efforts at publishing the Web protocols as standards were made at the IETF.[48] He was discouraged, however, by the slow and contentious deliberations at the IETF, and decided that the Web would best be served by a new and more flexible standardization body (Russell 2011).[49] In 1994 Berners-Lee left CERN for MIT, which became the home of a new SDO devoted to Web standards, W3C. Berners-Lee brought the page descriptor language HTML to W3C, while leaving HTTP at the IETF, where it continues to be maintained.

Soon after MIT became the base for W3C, several other universities in Europe and Asia joined W3C as organizational hosts. W3C received early funding from DARPA and the European Union. It later shifted to a self-sufficient member fee funding model (DeNardis 2014).

Patents and W3C

The Increasing Relevance of Patents to the Web

The open source movement was, to a large extent, a reaction to increases in intellectual property protection for computer software. As noted above, by the late 1980s and 1990s, an increasing number of software-related patents were being issued in the United States and growing numbers of lawsuits were being brought to enforce these patents (Besen and Meurer 2008, chapter 9). In addition, patents purporting to cover various broad categories of Internet technology, including British Telecom's 1989 patent that it claimed to cover the entire hyperlinked Internet, drew increasing press coverage and public concern, along with some ridicule from the technical community.[50] According to Richard Stallman, one of the founders of the "free" software movement, "the worst threat we face comes from software patents" (Stallman 1999).

In 1993, the University of Minnesota, which developed the popular Gopher Internet file sharing system, announced that it would begin to charge commercial users (Russell 2011). This announcement raised concerns among many Internet users, and prompted Berners-Lee to seek assurances from his own employer, CERN, that it would not do the same with the Web (ibid.). Later that year, CERN agreed to contribute its intellectual property rights in the code underlying the Web to the public domain to "further compatibility, common practices, and standards in networking and computer supported collaboration" (CERN 1993).

Given W3C's origins in the scientific research community, the first five years of its existence were relatively free from patent-related controversy. As Berners-Lee (2004) observed of that period:

> Many participants in the original development of the Web knew that they might have sought patents on the work they contributed to W3C, and that they might have tried to secure exclusive access to these innovations or charge licensing fees for their use. However, those who contributed to building the Web in its first decade made the business decision that they, and the entire world, would benefit most by contributing to standards that could be implemented ubiquitously, without royalty payments.

But, as noted in the introduction of this chapter, throughout the 1990s patents were becoming an increasingly important force in the commercial world. Patent concerns finally reached W3C in 1999. That year, Microsoft and Sun Microsystems disclosed patents covering W3C's CSS (cascading style sheets) and XLink technical proposals, respectively, and a small company called Intermind obtained a patent claiming key aspects of W3C's Platform for Privacy Preferences (P3P) standard (Weitzner 2004; Russell 2011). W3C feared that Intermind's royalty demands would chill adoption of the P3P standard. As a result, it engaged a prestigious New York law firm to opine that P3P did not infringe Intermind's patent (Pennie & Edmonds LLP 1999). Eventually, Intermind backed down and P3P was released without the threat of patent infringement. Nevertheless, the Intermind incident caused W3C to re-evaluate its informal "gentlemen's agreement" whereby participants would not seek to patent W3C standards.

W3C's RF Patent Policy

In 1999, W3C began the arduous task of developing a formal patent policy. Daniel J. Weitzner (2004) offers a detailed account of this lengthy and contentious process. The first policy that W3C's drafting group developed included requirements relating both to patent disclosure and patent licensing. The patent licensing provisions were the most controversial because they would have required W3C members to license SEPs to all implementers of W3C standards on RF or RAND terms. The possibility that

48 Berners-Lee submitted a version of HTML for standardization to the IETF in June 1993 (see www.w3.org/MarkUp/draft-ietf-iiir-html-01.txt). The standard was published by the IETF as RFC 1866 in November 1995 (Berners-Lee and Connolly 1995).

49 It has also been suggested that Berners-Lee preferred a standardization process over which he exerted more direct control. In this regard, W3C has been referred to as a "benevolent dictatorship," one in which the ultimate authority lies in the organization's director (Eygedi 2001, 40-41).

50 *British Telecom. v Prodigy Comms.*, 189 F Supp (2d) 101 (SDNY 2002), 217 F Supp (2d) 399 (SDNY 2002).

monetary royalties could be charged on W3C standards alarmed some W3C participants and members of the public, particularly the Open Source Initiative (2001) and other open source software developers and advocates. They claimed that large corporate interests within W3C were attempting to "hijack" the organization and subvert its historically open tradition. W3C received nearly 2,500 public comments on the draft policy, mostly opposing it.

This reaction from the open source community sent W3C back to the drawing board. In 2002, after extensive internal discussion and debate, W3C proposed a new patent policy, this time requiring RF licensing by all members of the W3C working group that developed a standard. Berners-Lee (2004) justified the move to an RF model as follows:

> The open platform of royalty-free standards enabled software companies to profit by selling new products with powerful features, enabled e-commerce companies to profit from services that [sic] on this foundation, and brought social benefits in the non-commercial realm beyond simple economic valuation. By adopting this Patent Policy with its commitment to royalty-free standards for the future, we are laying the foundation for another decade of technical innovation, economic growth, and social advancement.

To accommodate the concerns of some of its corporate members, the W3C policy included an exception which allowed the inclusion of patented technologies in W3C standards, but only after a "Patent Advisory Group" (PAG), comprising representatives of all working group members and the chair of W3C, determined that the patented technology was essential to the standard and could not be worked around. The new version of the patent policy was approved and went into effect in 2004, the tenth anniversary of W3C's formation. The policy remains in effect today with only minor revisions.[51]

The new W3C patent policy was not universally applauded by W3C members, and it has been reported that the RF requirement caused large patent holders such as IBM, SAP and Microsoft to bring standardization proposals to SDOs with more patent-friendly policies (Festa 2003; Russell 2011).[52] Nevertheless, some of these firms eventually expressed support for the policy, acknowledging the growing importance of open source software to the Web ecosystem.

Since W3C's RF policy went into effect, there have been relatively few invocations of the PAG process. One of the first arose in 2003, when a PAG was formed to assess the potential impact of four patents on W3C's draft VoiceXML standard (Voice Browser PAG 2003). The PAG approached the owners of the four patents and received a commitment of RF licensing with respect to two of them, and an assurance that the owner of the third did not consider the patent to be essential to the standard. But Rutgers University, the owner of the fourth patent, did not make any commitment regarding the patent and seemingly reserved its right to seek royalties against implementers of the standard. W3C proceeded to adopt the standard in the face of this threat, and it appears that Rutgers did not actively seek to enforce the patent.

A more contentious incident arose, also in 2003, with respect to a patent held by a small firm called Eolas, which allegedly covered a key aspect of the HTML standard (Weitzner 2004). After Eolas obtained a US$521 million infringement verdict against Microsoft's Internet Explorer browser, W3C convened a PAG to assess the potential impact of the Eolas patent on HTML. As a result of the PAG, W3C petitioned the US Patent and Trademark Office (PTO) to re-examine the Eolas patent. In a letter to the PTO, Berners-Lee (2003) expressed the concerns of the PAG and the broader Web community:

> The impact of the [Eolas] '906 patent reaches far beyond a single vendor and even beyond those who could be alleged to infringe the patent. The existence of the patent and associated licensing demands compels many developers of Web browsers, Web pages, and many other important components of the Web to deviate from the fundamental technical standards that enable the Web to function as a coherent system…
>
> The barriers imposed on the information technology industry by the '906 patent are of such concern because they cause fragmentation in the basic standards that weave the Web together. Denial of access to any particular technology is a problem that engineers can successfully address, provided they have knowledge of the barrier before it becomes part of a standard. However, as the '906 patent threatens widely deployed, standard technology, the damage is magnified. If the '906 patent remains in force, Web page designers and software developers will face a dangerous dilemma. They may comply with globally-

51 See www.w3.org/Consortium/Patent-Policy-20040205/.

52 SDOs face the risk that members will depart with any controversial policy change. Such fears arose in 2007 when the small SDO VITA amended its patent policy to require members holding SEPs to disclose their maximum royalty rates prior to approval of a standard. Despite vigorous opposition, only one member, Motorola, actually withdrew from VITA as a result of the policy change (Contreras 2013a). Similar concerns have been raised in the wake of recent policy amendments by the IEEE.

> recognized Web standards resulting in an inadequate user experience of their content. Or, they may attempt to design to the various work-arounds chosen by different browser developers and face the uncertainly of not knowing who will be able to use their content or applications properly. W3C's development and the industry's acceptance of a single common base of standards for Web infrastructure arose out of a need to avoid just this sort of dilemma. The '906 patent is a substantial setback for global interoperability and the success of the open Web.

The Eolas patent was eventually invalidated by the PTO on the basis of prior art presented by W3C (Weitzner 2004).

Despite these relatively high-profile incidents and the large number and significance of standards published by W3C, only a handful of PAGs have been formed to investigate patents not subject to RF licensing commitments. During the first 10 years of the RF patent policy, a mere 12 PAGs were formed, all of which resolved the relevant issues without serious disruption of W3C's standardization activities (W3C Patent and Standards Interest Group 2013). It thus appears that the RF policy at the W3C has largely been a success.

CONCLUSION: THE LOGIC OF RF

As this chapter shows, the primary SDOs responsible for Internet standards, the IETF and W3C, have evolved strong policies and norms favouring RF standards. This approach has likely contributed to the relatively low level of patent litigation relating to Internet standards in comparison with network standards.

The preference for RF standards at the IETF and W3C can be traced, in part, to the historical origins of these groups in academia and government and their ties to the open source movement. Scotchmer (2006, 307) called the circumstances resulting in the open Internet "one of the most fortunate accidents in industrial history."[53]

But the IETF and W3C today are dominated by private firms that are as motivated by profit as their counterparts in the network space. Their reasons for favouring RF models are not entirely ideological or altruistic. A range of commercial considerations motivate firms to relinquish potentially profitable exploitation of their patent rights in the service of broader commercial goals, such as the seeding of new markets, the establishment of technological leadership and the desire to achieve industry-wide interoperability (Contreras 2015c).

Whatever the reasons for its development, the RF patent landscape of the Internet has yielded significant benefits (Scotchmer 2006; DeNardis 2014). It has enabled substantial innovation and experimentation, it has yielded entirely new industries such as social media and it has facilitated virtually unrestricted market entry and competition.

Defenders of patent monetization argue that a financial return on patents is necessary to fuel innovation and product development in complex and rapidly advancing technologies. There is clearly some truth to this assertion, and a recognition in no less than the US Constitution that patents are intended to promote innovation. However, proponents of strongly monetized patent structures may lose sight of the innovation that could potentially be enabled by *lowering* barriers to technology markets.[54]

Today's debate over SEPs and patent monetization is really just one skirmish in a much larger war over openness and closure in technology networks. Scholars including Larry Lessig (2001; 2006), Jonathan Zittrain (2009), Milton L. Mueller (2002), Tim Wu (2010) and Laura DeNardis (2009; 2014) have warned about the consequences of over-regulating, closing and monetizing the Internet. The open and RF nature of the Internet was not pre-ordained and it may not last forever. Slight changes in history could have sent the Internet off in very different directions. Just as a single meteor or climatic event can shift the course of biological evolution, so can a single judicial decision or regulatory pronouncement change the course of a technology field. It is unlikely that many today would prefer to live in a world in which most content is meted out by commercial networks, as it was in the 1980s under pay services such as America Online (AOL), CompuServe and Prodigy. Could

53 See also Lehr (1995), attributing the success of the Internet in part to "historical accident."

54 In a way, today's patent monetization justifications echo those made by AT&T in the heyday of the telephony monopoly. As Tim Wu (2010) has described it, AT&T justified its state-sanctioned monopoly, in part, by arguing that the resulting rents were plowed back into research and development at facilities like Bell Laboratories, where no fewer than seven Nobel laureates hung their hats and to which we owe the transistor and many other technological marvels. Yet in hindsight, Wu points out, these arguments ring hollow. After all, the basic residential telephone unit remained essentially unchanged for 40 years, notwithstanding the brain trust at Bell Labs. What's more, AT&T imposed a daunting array of intellectual property, regulatory and commercial barriers to block any innovator who sought to improve telephony in the slightest degree (culminating in the notorious "Hush-a-Phone" debacle). When the Federal Communications Commission finally grew skeptical of the monopoly's virtue and ordered the standardization of telephone jacks via the now-ubiquitous RJ-11 connector, an explosion of innovation occurred leading to the introduction of connected devices including fax machines, answering machines and speaker phones (ibid.).

the proliferation of patents on fundamental interoperability standards nudge us back in this direction?[55]

Rapid technical change will occur in the near future with the advent of the Internet of Things, the Smart Grid,[56] 3D printing, wearable devices and other technological advances. Each of these developments will require new standards and common protocols that build on top of the existing Internet infrastructure. Let us hope that these new technologies remain as open to future innovation and competition as the Internet is today.[57]

ACKNOWLEDGEMENTS

The author thanks Scott Bradner and Wendy Seltzer for their thorough background discussions of the IETF and W3C, respectively, as well as an anonymous peer reviewer for numerous helpful comments and suggestions.

AUTHOR'S NOTE

The author serves as a legal adviser to the IETF, but received no compensation from the IETF relating to the preparation of this chapter. This chapter contains no privileged or confidential information. Support for its preparation was provided by the Centre for International Governance Innovation and the Royal Institute of International Affairs (Chatham House).

55 Walter Isaacson (2014) describes a similar alternative pathway that the Internet might have taken had Ted Nelson's system of two-way links prevailed over Berners-Lee's hyperlinks:

> Had Nelson's system of two-way links prevailed, it would have been possible to meter the use of links and allow small automatic payments to accrue to those who produced the content that was used. The entire business of publishing and journalism and blogging would have turned out differently. Producers of digital content could have been compensated in an easy, frictionless manner, permitting a variety of revenue models, including ones that did not depend on being beholden solely to advertisers. Instead the Web became a realm where aggregators could make more money than content producers….But a system of two-way links and micropayments would have required some central coordination and made it hard for the Web to spread wildly, so Berners-Lee resisted the idea.

See also Lisa Larrimore Ouellette's 2015 discussion, "An Alternate History of the Web & Copyright Law," at http://writtendescription.blogspot.com/2016/02/an-alternate-history-of-web-copyright.html.

56 For example, for a description of the influence of telecommunications and electronics producers on discussions of Smart Grid standardization, see Contreras (2012).

57 A group of SDOs led by the IETF, W3C and the IEEE took a tentative step toward formalizing this ethos in 2012 with the publication of the OpenStand "Modern Paradigm for Standards" (see https://open-stand.org/about-us/principles/). The principles espoused by OpenStand include laudable ideals such as cooperation, due process, transparency and consensus. The OpenStand position regarding patents, however, does little other than accept both RF and FRAND licensing models for patented standards.

WORKS CITED

ABA. 2007. *Standards Development Patent Policy Manual*, edited by Jorge L. Contreras. Chicago, IL: ABA Publishing.

Adelman, Martin, Shubha Ghosh, Amy Landers and Toshiko Takenaka. 2011. *Global Issues in Patent Law.* St. Paul, MN: Thompson Reuters.

Baran, Paul. 1964. *On Distributed Communications: I. Introduction to Distributed Communications Networks*. RAND Corporation. www.rand.org/pubs/research_memoranda/RM3420.html.

Baron, Justus and Tim Pohlmann. 2015. "Mapping Standards to Patents using Databases of Declared Standard-Essential Patents and Systems of Technological Classification."

Bekkers, Rudi and Andrew Updegrove. 2012. "A Study of IPR Policies and Practices of a Representative Group of Standard Setting Organizations Worldwide." Presented at National Academies of Science Symposium on Management of IP in Standards-Setting Processes, Session 4. http://sites.nationalacademies.org/xpedio/groups/pgasite/documents/webpage/pga_072197.pdf.

Bekkers, Rudi, Bart Verspagen and Jan Smits. 2002. "Intellectual Property Rights and Standardization: The case of GSM." *Telecommunications Policy* 26: 171–88.

Berners-Lee, Tim. 2003. Letter to Hon. James E. Rogan, Director, U.S. Patent and Trademark Office, www.w3.org/2003/10/27-rogan.html.

———. 2004. "Director's Decision, W3C Patent Policy." www.w3.org/2003/05/12-director-patent-decision-public.html.

Berners-Lee, Tim and Daniel W. Connolly. 1995. RFC 1866 — Hypertext Markup Language — 2.0. www.rfc-editor.org/rfc/rfc1866.txt.

Bessen, James and Michael J. Meurer. 2008. *Patent Failure: How Judges, Bureaucrats, and Lawyers Put Innovators at Risk*. Princeton, NJ: Princeton University Press.

Biddle, Brad, Andrew White and Sean Woods. 2010. "How Many Standards in a Laptop? (And Other Empirical Questions)." Proceedings of the 2010 ITU-T Kaleidoscope Academic Conference, Pune, India, December 13–15.

Blind, Knut, Rudi Bekkers, Yann Dietrich, Eric Iversen, Florian Köhler, Benoît Müller, Tim Pohlmann, Stein Smeets and Jurgen Verweijen. 2011. *Study on the Interplay between Standards and Intellectual Property Rights (IPRs)*. Luxembourg: Publications Office of the European Union.

CERN. 1993. "Statement Concerning CERN W3 Software Release Into Public Domain." https://tenyears-www.web.cern.ch/tenyears-www/Declaration/Page2.html.

Clark, David D. 1992. "A Cloudy Crystal Ball: Visions of the Future (Alternate Title: Apocalypse Now)." Proceedings of the 24th IETF, Cambridge, MA, July 13–17.

Contreras, Jorge L. 2012. "Standards, Patents and the National Smart Grid." *Pace Law Review* 32 (3): 641–75.

———. 2013a. "Technical Standards and *Ex Ante* Disclosure: Results and Analysis of an Empirical Study." *Jurimetrics* 53: 163–211.

———. 2013b. "Fixing FRAND: A Pseudo-Pool Approach to Standards-Based Patent Licensing." *Antitrust Law Journal* 79: 47–97.

———. 2014. "Divergent Patterns of Engagement in Internet Standardization: Japan, Korea and China." *Telecommunications Policy* 30: 916–34.

———. 2015a. "A Market Reliance Theory for FRAND Commitments and other Patent Pledges." *Utah Law Rev*iew 2015: 479–558.

———. 2015b. "A Brief History of FRAND: Analyzing Current Debates in Standard Setting and Antitrust through a Historical Lens." *Antitrust Law Journal* 80: 39–120.

———. 2015c. "Patent Pledges." *Arizona State Law Journal* 47 (3): 543–608.

———. Forthcoming 2016a. "Patents, Technical Standards and Standard-Setting Organizations: A Survey of the Empirical, Legal and Economics Literature." In *Research Handbook on the Economics of Intellectual Property Law, Vol. II — Analytical Methods*, edited by Peter S. Menell and David Schwartz. New York, NY: Edward Elgar.

———. Forthcoming 2016b. "Assertion of Standards-Essential Patents by Non-Practicing Entities." In *Patent Assertion Entities and Competition Policy*, edited by D. Daniel Sokol. New York, NY: Cambridge University Press.

Cowhey, Peter F., Jonathan D. Aronson and John E. Richards. 2006. "The Peculiar Evolution of 3G Wireless Networks: Institutional Logic, Politics and Property Rights." In *How Revolutionary Was the Digital Revolution? National Responses, Market Transitions, and Global Technology*, edited by J. Zysman and A. Newman. Stanford, CA: Stanford University Press.

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

———. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

Egyedi, Tineke M. 2001. *Beyond Consortia, Beyond Standardisation? New Case Material and Policy Threads — Final Report for the European Commission*. October.

Fairfield Resources, Inc. 2007. "Analysis of Patents Declared as Essential to GSM as of June 6, 2007." Working paper, December 31.

Farrell, Joseph, John Hayes, Carl Shapiro and Theresa Sullivan. 2007. "Standard Setting, Patents and Hold-Up." *Antitrust Law Journal* 74: 603–70.

Festa, Paul. 2003. "W3C Makes Patent Ban Final." CNET News, March 21.

Froomkin, Michael. 2003. "Habermas@Discourse.Net: Toward a Critical Theory of Cyberspace." *Harvard Law Review* 116: 749–873.

Galetovic, Alexander, Stephen Haber and Ross Levine. 2015. "An Empirical Examination of Patent Hold-Up." NBER Working Paper 21090. Cambridge, MA: National Bureau of Economic Research.

Gartner Group. 2015. "Gartner Says 6.4 Billion Connected 'Things' Will be in Use in 2016, Up 30 Percent from 2015." Press Release. www.gartner.com/newsroom/id/3165317.

Goodman, David J. and Robert A. Myers. 2005. "3G Cellular Standards and Patents." Proceedings of IEEE 2005 International Conference on Wireless Networks, Communications and Mobile Computing.

Hafner, Katie and Matthew Lyon. 1996. *Where Wizards Stay Up Late: The Origins of the Internet*. New York, NY: Simon & Schuster.

Hesse, Renata. 2012. Remarks at the ITU-T Patent Roundtable: Six "Small" Proposals for SDOs Before Lunch. October 10. www.justice.gov/atr/public/speeches/287855.pdf.

Hoffman, Paul, ed. 2012. *The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force*. www.ietf.org/tao.html.

Isaacson, Walter. 2014. *The Innovators: How a Group of Hackers, Geniuses, and Geeks Created the Digital Revolution*. New York, NY: Simon & Schuster.

Kushida, Kenji E. 2008. "Wireless Bound and Unbound: The Politics Shaping Cellular Markets in Japan and South Korea." *Journal of Information Technology & Politics* 5 (2): 231–54.

Lehr, William. 1995. "Compatibility Standards and Interoperabilty: Lessons from the Internet." In *Standards Policy for Information Infrastructure*, edited by Brian Kahin and Janet Abbate, 121–47. Cambridge, MA: MIT Press.

Lemley, Mark A. 2002. "Intellectual Property Rights and Standard-Setting Organizations." *California Law Review* 90 (6): 1889–980.

Lemley, Mark A. and Carl Shapiro. 2007. "Patent Holdup and Royalty Stacking." *Texas Law Rev*iew 85: 1991–2049.

Lessig, Larry. 2001. *The Future of Ideas: The Fate of the Commons in a Connected World*. 1st ed. New York, NY: Random House.

———. 2006. *Code — Version 2.0*. New York, NY: Basic Books.

Lundqvist, Björn. 2014. *Standardization Under EU Competition Rules and US Antitrust Laws*. Cheltenham, UK: Edward Elgar.

Mueller, Milton L. 2002. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press.

Nickerson, Jeffrey V. and Michael zur Muehlen. 2006. "The Ecology of Standards Processes: Insights from Internet Standard Making." *MIS Quarterly* 30: 467–88.

Open Source Initiative. 2001. OSI Letter of comment to W3C's Proposed RAND Policy. November 13. https://lists.w3.org/Archives/Public/www-voice/2001OctDec/0037.html.

Pennie & Edmonds LLP. 1999. "Analysis of P3P and U.S. Patent 5,862,325." www.w3.org/TR/1999/NOTE-P3P-analysis-19991027.

Russell, Andrew L. 2011. "Constructing Legitimacy: The W3C's Patent Policy." In *Opening Standards*, edited by Laura DeNardis, 159–76. Cambridge, MA: MIT Press.

———. 2014. *Open Standards and the Digital Age: History, Ideology, and Networks*. New York, NY: Cambridge University Press.

Rustad, Michael L. 2014. *Global Internet Law*. Minneapolis, MN: West Academic Publishing.

Scotchmer, Suzanne. 2006. *Innovation and Incentives*. Cambridge, MA: MIT Press.

Segalier, Stephen. 1998. *Nerds 2.0.1: A Brief History of the Internet*. New York, NY: TV Books.

Shapiro, Carl and Hal R. Varian. 1999. *Information Rules: A Strategic Guide to the Network Economy*. Boston, MA: Harvard Business School Press.

Shurmer, Mark and Gary Lea. 1995. "Telecommunications Standardization and Intellectual Property Rights: A Fundamental Dilemma?" In *Standards Policy for Information Infrastructure*, edited by Brian Kahin and Janet Abbate, 378–404. Cambridge, MA: MIT Press.

Simcoe, Timothy. 2007. "Delay and de jure Standardization: Exploring the Slowdown in Internet Standards Development." In *Standards and Public Policy*, edited by Shane Greenstein and Victor Stango, 260–95. Cambridge, UK: Cambridge University Press.

Stallman, Richard. 1999. "The GNU Operating System and the Free Software Movement." In *Open Sources: Voices from the Open Source Revolution*, edited by Chris DiBona, Sam Ockman and Mark Stone. O'Reilly & Associates.

US Department of Justice and US FTC. 2007. *Antitrust Enforcement and Intellectual Property Rights: Promoting Innovation and Competition*. Washington, DC.

Voice Browser PAG. 2003. "Voice Browser PAG Report." www.w3.org/2003/06/VBPAG-Report.html.

W3C Patent and Standards Interest Group. 2013. "Continued Maintenance of W3C's Patent Policy." www.w3.org/2004/pp/psig/.

Weitzner, Daniel J. 2004. "Standards, Patents and the Dynamics of Innovation on the World Wide Web." www.w3.org/2004/10/patents-standards-innovation.html.

Whitt, Richard S. 2013. "A Deference to Protocol: Fashioning a Three-Dimensional Public Policy Framework for the Internet Age." *Cardozo Arts & Entertainment Law Journal* 31 (3): 689–768.

Wu, Tim. 2010. *The Master Switch: The Rise and Fall of Information Empires*. New York, NY: Vintage Books.

Zittrain, Jonathan. 2009. *The Future of the Internet — And How to Stop It*. New Haven, CT: Yale University Press.

ABOUT THE AUTHOR

Jorge L. Contreras is associate professor of law at the University of Utah's S. J. Quinney College of Law, and a senior policy fellow at American University Washington College of Law. He writes and speaks frequently on topics including technical standards, patent litigation and antitrust law. He serves as co-chair of the American Bar Association's (ABA's) Technical Standardization Committee, and as a member of the American National Standards Institute Intellectual Property Rights Policy Committee, the Advisory Council of National Institutes of Health's (NIH's) National Center for Advancing Translational Science and NIH's Council of Councils. He edited the ABA's *Technical Standards Patent Policy Manual* (2007) and is the editor of the forthcoming *Cambridge Handbook of Technical Standardization Law* (2 vols.). Jorge's work has appeared in publications including *Science*, *Nature*, *Telecommunications Policy*, *Standards Engineering*, *IEEE Internet Computing*, *American University Law Review, Antitrust Law Journal, Berkeley Technology Law Journal*, *Jurimetrics* and *Harvard Journal of Law and Technology*. He is the founding editor of Social Science Research Network's *Law, Policy and Economics of Technical Standards eJournal*, and was the winner (with co-authors) of the Standards Engineering Society's 2011 and 2015 scholarly paper competitions. In addition to his academic work, Jorge represents select clients, such as the Internet Engineering Task Force, on matters relating to technology licensing and standards, and has served as a testifying expert and arbitrator in complex international intellectual property disputes. Prior to entering academia, he was a partner in the Boston, Washington and London offices of the international law firm Wilmer Cutler Pickering Hale and Dorr LLP. He is an honours graduate of Rice University (B.A., B.S.E.E.) and Harvard Law School (J.D.), and was a fellow of the Berkman Center for Internet and Society at Harvard Law School.

CHAPTER THREE:
STANDARDS, PATENTS AND NATIONAL COMPETITIVENESS

Michael Murphree and Dan Breznitz

ACRONYMS

3C	content, computers and communications
AVS	Audio Video Standard
CD	compact disc
CDMA	Code Division Multiple Access
DVD	digital video disc
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobiles
IBM	International Business Machines Corporation
IGRS	Intelligent Grouping and Resource Sharing
IP	intellectual property
JVC	Victor Company of Japan
MIIT	Ministry of Industry and Information Technology (China)
MOU	memorandum of understanding
MPEG	Moving Picture Experts Group
MS-DOS	Microsoft Disk Operating System
PC	personal computer
RAND	reasonable and non-discriminatory
SEPs	standards-essential patents
USB	universal serial bus
VHS	Video Home System

INTRODUCTION

Technology standards are fascinating. They are inscrutable and dense, accessible only to engineers and intellectual property (IP) lawyers, seemingly far outside the realm of daily life. At the same time, they are central to modern daily life. From your morning coffee (graded according to a standardized scale of colour, quality and roast), to your email inbox check (enabled by a dizzying array of protocols set by individual firms and international technology associations), to your commute to work (powered by gasoline rated according to standards set by sovereign governments), life is governed by standards. Were it not for standards, it would be impossible — without extreme costs in terms of time and effort — to compare products, utilize networked technologies or even shop in a grocery store with confidence. Standards ensure product compatibility (essential for the functioning of telecommunications, audio, video and information technology) and facilitate information transfer. When a product is standardized, it is clear to a prospective buyer or user what they are acquiring, as well as its capabilities.

In technology products, standards ensure compatibility across brands and devices (Braunstein and White 1985). Before standardization takes place, there can be multiple protocols for different products, making them incompatible (Besen and Johnson 1986). With standardization, a consumer can purchase a variety of devices from multiple vendors and brands knowing they will work together. The reader may recall a time before the universal serial bus (USB) standard, when computer accessories used many different types of connectors. Not every brand or type of computer on the market included all of the necessary plug types, meaning the user had to either purchase adaptors or carefully check for compatibility before purchasing a computer peripheral. With the USB standard, users know that accessories will always be compatible, whatever brand they purchase.[1]

Despite their ubiquity in our lives, technology standards are still a mystery. Most people neither know what they contain nor how they are created. Yet their importance goes beyond facilitating modern life. Standards create markets for technology goods and services, and set the terms of competition in those markets. This chapter specifically looks at one aspect of standardization — the inclusion of essential IP, usually referred to as standards-essential patents (SEPs). Within the hundreds of pages of documentation for a standard, the clauses concerning SEPs help determine the fate of technologies, markets, firms and even countries in the global economy. This chapter examines the intersection of technology standards and IP and explains the impact SEPs have on the development of technology markets and industries in different countries.

SEPs determine the costs for firms to participate in markets for standardized technologies. They do so in two ways. First, firms that own the rights to SEPs have a cost advantage in the market over non-SEP holders (Bekkers, Dysters and Verspagen 2002). Unlike firms on the outside, SEP holders will owe no licensing fees, or lower ones, when they produce standards-compliant products. Second, holders of SEPs have a closer understanding of the specific technical features of a standard and thus a greater advantage in setting the technology trend for the next generation of standards, helping to perpetuate competitive advantage (Correia de Brito and Pelkmans 2012).

At a macro scale, different countries in the world economy have different positions in this system, and hence different perspectives on the normative role for IP in standards. All else equal, developed countries usually support "hard" IP

1 An interesting exception to this trend are Apple products, which frequently use different standards in order to force users to purchase only Apple products. This strategy can increase revenues by locking users in to a given vendor's products but can also backfire if the products are not sufficiently differentiated and valuable to a consumer to encourage them to inhabit this isolated market. Despite the unique hardware standards it adopts, even Apple understands the de facto Microsoft Office standards for word processing and spreadsheets. Accordingly, Apple includes these Microsoft applications with its computers in order to ensure Apple users can easily share documents with personal computer (PC) users.

norms in standards. This is an extension of their national laws concerning IP. IP is property and thus the bearer has the right to dispose of it as they see fit, whether by restricting access to it or setting the price at which it may be used (Simpkin 2010). Developing countries, which — thanks to the global fragmentation of production — are major manufacturers of technology products that conform to established technology standards, are in a difficult position. In order to produce goods for which there is global demand, they must produce standards-compliant products. However, doing so exposes the firms to requirements to pay royalties for the SEPs in standardized technologies. This increases their costs and lowers profit margins, thus reducing the resources available to invest in research and development that could, perhaps, contribute to the next generation of technology. Accordingly, emerging economies, most notably China, are increasingly pushing for new norms governing SEPs (Maskus and Merrill 2013). China's approach — setting standards with free or nominally priced IP — is highlighted here.

This chapter first defines technology standards and SEPs, and the roles they play in determining markets for technology goods and services. It then turns to two case studies. The first looks at the role that SEPs played in early mobile telecommunications standards in Europe and the United States. This case shows the manner in which hard enforcement of IP rights shaped the markets for these technologies. The second case study examines two standardization efforts in China, highlighting the challenge that licensing fees for SEPs pose to Chinese firms and the efforts made in Chinese standardization to change the norms governing IP in standards. The chapter then concludes with implications for the future of SEP norms and public policy-governing standards.

DEFINING TECHNOLOGY STANDARDS AND SEPs

Technology standards are defined as formal written protocols, developed by consensus or a modified consensus principle in a formal or ad hoc body, that serve as a platform for interoperability and comparability and on which other applications and innovations can be built (American National Standards Institute 2013). This somewhat complex definition encompasses both varieties of standards: de jure (set through binding political processes) and de facto (set by enterprises or private bodies that have achieved market dominance that forces competing standards to exit). Both de jure and de facto standards can be set by either individual private parties or alliances, or by government or international organizations. Usually, the drafting of a standard takes place in a working group, is voted on by a technical committee and is finally adopted by the entire standardization body (International Organization for Standardization n.d.).

Although standards are usually considered public goods, because the adherence to the standard by one firm does not preclude its adoption or utilization by another, they should actually be considered "semi-public" goods (Kindleberger 1983). All firms are able to benefit from standardization but those actively involved in setting the standard and contributing essential technologies benefit even more than those who simply use the standard. The degree of benefit a firm receives from a standard depends on its position either as a creator/contributor or as an adopter of the standard.

Standards have several impacts on technology development and marketing once they are set. First, standards will "freeze" the development of technology. This does not mean innovation or technology development stops. Rather, the freeze means the standard codifies the state of the art at that point, amalgamating knowledge into a platform on which other peripheral and related innovations can be built (ibid.; Besen and Johnson 1986; Ernst 2009; Ernst 2011). Second, the setting of a standard effectively precludes the development of alternative technologies — whatever their technical or commercial merit. Once a standard is set, firms must ensure their products conform to the standard, lest they face a declining market share. The third impact of standards is to shift the basis of market competition. Once a standard is set and all firms are able to utilize it, competition no longer involves novelty or difference but rather becomes based on price (Farrell and Saloner 1985; Berg 1988; Berg 1990; Berg and Schummy 1990; Özsomer and Cavusgil 2000; Yoo, Lyytinen and Yang 2005).

All three of these principles can be seen in the case of the de facto standard for video cassettes in the 1980s and 1990s (Cusumano, Mylonadis and Rosenbloom 1992). In the 1970s, Sony first introduced a video recording cassette under the brand name Betamax. Within a year, a competing standard format, Video Home System — VHS — was offered by the Victor Company of Japan (JVC). Although Betamax enjoyed first-mover advantage and arguably offered better picture quality, by the early 1980s, VHS had emerged as the dominant standard. VHS won the competition over Betamax because its creator — JVC — was willing to widely and inexpensively license the technology. As more firms offered VHS players, there were lower prices and more content available. Users increasingly adopted VHS. Once VHS achieved critical mass, Betamax users became "orphans," with limited choice of content (Özsomer and Cavusgil 2000). Once VHS won the standards competition, the technology was essentially frozen. Firms were able to produce the technology — utilize the standard — and make improvements on it, such as higher-quality or longer-running cassettes. However, the standardized technology would remain largely unchanged until it was supplanted by an entirely different technology 20 years later — the digital video disc (DVD). Competition among VHS-player

manufacturers shifted to price. Since all devices performed the same function, consumer interest shifted to price and away from unique features. The same trend would occur with DVD players once they emerged from competition among advanced VHS and video compact disc players.

The market impact of standards — and by extension the broader impact on firms and national economies — is often a feature of the embedded IP. An SEP is a patent whose technological scope must be violated if a user creates a standards-compliant technology (American National Standards Institute 2016). The European Telecommunications Standards Institute (ETSI) further clarifies that essentiality means it is impossible on technical — as opposed to commercial — grounds, given the current state of technology, to make or use standards-compliant technology without infringing on that particular IP (ETSI 2016). Similarly, Jay P. Kesan and Carol M. Hayes (2014) define SEPs as technologically essential patents, where essentiality is tightly bound with the interoperability focus inherent in a standard. To illustrate, consider an electric plug. If all — or most — of the firms in a given industry opt to use a specific type of plug for charging devices, the plug shape is a de facto standard. If the design of this plug is covered by a patent, any firm making products compatible with that plug would be violating this proprietary technology. Thus, the patent in question would be essential to the de facto standard.

While early technological standards often had dozens or hundreds of patents considered essential, today standards often list thousands of essential patents. SEPs are intended to be so basic to the technology in a standard that it is impossible to "innovate around" the patents to produce a roughly compatible or equivalent product that does not violate the patent (Dolmans 2002; ETSI 2016). Rather than violate IP, which would undermine the incentive to invent, standards bodies provide options for holders of SEPs to declare and benefit from widespread adoption of their technology.

Any actor wishing to adopt a standard or make standards-compliant products will have to license the patents in question. This process poses several potential risks in standardization. First, an IP holder might declare that it has essential IP but refuse to license the technology (Bekkers and West 2009). If this occurs while a standard is being developed, the developers must attempt to find a way around the patent or else the entire standard can be blocked. Second, an IP holder might wait until after a standard has been developed to declare that the standard as proposed actually infringes on their patents. If the firm again refuses to license their IP, this is called "patent holdup" and can prevent the implementation of a standard (ETSI 2016). A firm under the same circumstances can offer to license but only under highly restrictive or expensive terms with negative effects on standard adoption and the profitability of firms making standards-compliant products. A third threat is that an IP holder will transfer the patents to a third party that refuses to acknowledge or accept the licensing agreements made by the previous owner (Arthur 2012). This last occurrence has sparked numerous lawsuits as new IP holders — such as Google after purchasing Motorola Mobility's patents — change the agreed-upon licensing terms and increase fees.

In almost all cases, standards-development bodies and national governments enforce IP law in the case of technology standards. Patents are IP, and must be protected or else, proponents argue, there would be no incentive for firms or individuals to innovate (Simpkin 2010). Patents are necessary to offer a reward for taking the risk of invention — even if those patents can determine the fate of a technology standard. Since standards offer so many advantages to consumers in clarity of choice and lower prices, it stands to reason that they should be developed. If a standard involves SEPs, then a licensing arrangement must be made. The general norm is known as RAND: reasonable and non-discriminatory (Van Eecke and Truyens 2009). SEP holders are expected to license their patents on a non-discriminatory basis — all users have a right to license the technology — and in exchange for a reasonable royalty. This norm is broadly upheld in the United States and Europe (ibid.; American National Standards Institute 2008).

A major exception, however, has occurred in the case of China. There, the government has attempted to set rules for technology standardization that weaken the norm of hard IP protection (Breznitz and Murphree 2013). China's government does not suggest that patents are unimportant or that they should be invalidated. Instead, standards-development organizations are encouraged to include SEPs offered on a royalty-free or nominal basis before considering patented technologies or SEP-relevant protocol submissions from firms interested in maximizing the returns from licensing (ibid). The objective is to encourage firms to offer their IP inexpensively in exchange for broad promotion of the technology standard — with the idea that a larger user base would ensure both licensing revenues and income from sales of standards-compliant products.

HOW STANDARDS AND SEPs SHAPE MARKETS

With this understanding of standards and SEPs, it is possible to go into greater depth on how these shape markets. Standardization research argues that there are three stages of competition in standardized technologies: pre-standardization, standardization and post-standardization (Besen and Johnson 1986). In the pre-standardization era, a variety of competing technologies or formats arise. In this stage, competition is between the technologies themselves over which offers the best quality, greatest ease of use or other features. The development of the modern PC

industry illustrates this stage. Until 1984, there were at least four major PC standards: International Business Machines Corporation (IBM), Apple, UNIX and CSIS. All four competed to offer the most satisfactory user experience (Apple) or the greatest utility (IBM). All were incompatible, because the software for one PC system could not run on another. Each also used unique peripheral hardware, thus making shopping difficult. Users of one firm's system were effectively locked into a closed monopoly market — with the accompanying higher prices.

The standard was set when the impasse between the four technology platforms was broken open through the combination of IBM's decision to use a third-party's operating system — Microsoft Disk Operating System (MS-DOS) — and the piracy of IBM's Basic Input/Output System by Taiwanese computer hardware manufacturing firms. With "PC clones" available — computing hardware with similar capabilities, and all able to run the same software, thanks to MS-DOS — consumers were able to choose among competing brands without worrying about incompatible software. As more and more users adopted the IBM PC standard, it achieved critical mass in the market, forcing out the competing standards — except Apple, which retained a niche market.

Once the standard was established, PC manufacturers and brands now had to compete on price. Increased competition for users and the availability of standardized components drove down prices, further encouraging adoption. The PC industry, to this day, is mostly a highly price-sensitive competitive environment in which makers of general use PCs must produce as inexpensively as possible to support sales. Most users no longer care about the brand of the PC because they are largely interchangeable.

While standardization changes the overall dynamics of market competition from features to price, the rewards of that competition are heavily influenced by SEPs. Once a standard is adopted and the list of SEPs determined, the firms that contributed them are able to demand royalties. While this is normally done in accordance with the RAND principle, there is no clear definition of a reasonable royalty. In the DVD standard, the SEPs were held by a group of European, American and Japanese firms including Toshiba, Matsushita, JVC, Mitsubishi, Hitachi, Time Warner, Philips, Sony and Pioneer. As with VHS, DVD was an open standard in that any firm wishing to do so could produce DVD players and discs. However, they would be required to pay royalties to these firms, set at roughly US$20 per DVD player in 2004 (*People's Daily* 2004; Linden 2004). When DVD players were first produced, this seemed a reasonable amount. However, as the wholesale price of DVD players fell in the early 2000s, the royalty became the single largest cost in production, severely limiting the profits for manufacturers while providing a steady source of income to SEP holders. For firms hoping to leapfrog technologies or catch up through advanced manufacturing, the cost of royalties limited the ability to marshal capital. For firms hoping to secure their position in the next generation of standards, the royalties offered a source of income for investment in research and development.

Further, it is common practice for SEP holders to share their IP with other SEP holders through cross-licensing (Bekkers and West 2009). Cross-licensing grants SEP holders largely royalty-free access to the standard. Effectively, SEP holders can thus produce standards-compliant goods at a far lower price than firms without SEPs. This cost advantage can be used to undercut the prices of non-SEP-holding competitors or to provide an even greater source of profits. It can thus be seen that SEPs significantly impact the distribution of gains from standardization.

To illustrate the principles of technology standards and SEPs in market creation, consider the examples of two standards: first, the setting and performance of mobile telephony standards in Europe and the United States in the 1980s and 1990s, and second, more recent Chinese attempts at standardization. In these examples, the role of SEPs was quite different, greatly shaping the outcomes for the standards. In the case of mobile telephony, limited licensing of SEPs helped determine the eligible players in the market — thus determining winners and losers before market competition had even begun. For Chinese standards, a bitter lesson in the costs of SEPs would lead to attempts to change the norms governing IP. Given the vested interests of established technology players, Chinese standards makers came to believe the only means of improving their competitive situation would be to create technologically competitive Chinese standards as an alternative to global standards with "expensive" IP. The idea was to force a change in the norms governing valuation of IP without violating the norm of IP itself. In effect, SEPs would still be accepted but the pricing norm would switch from an arbitrarily defined RAND licence to nominally priced sharing of IP to encourage adoption and dissemination of a standard and standards-compliant technologies.

MOBILE TELEPHONY STANDARDS

The world's first truly global telecommunications standard was the Global System for Mobiles, or GSM, developed by a consortium of European firms under the aegis of two bodies: the Groupe Speciale Mobile and (later) ETSI (Bekkers, Verspagen and Smits 2002). In the 1980s, the Scandinavian countries, Germany, France and Italy had developed four individual and incompatible mobile telephony systems, creating highly fragmented national markets (Funk 2002). As a result, French mobile handsets, for example, became useless once a user crossed the border into Germany. To solve the problem of incompatibility, in 1982, telecommunications operators across Europe signed

a memorandum of understanding (MOU) pushing for a single pan-European standard to replace the incompatible national standards. This MOU would form the basis of the Groupe Speciale Mobile that would later develop the GSM standard.

Rather than allow firms to develop competing standards, ETSI would use national-level representation for voting on protocols and IP policies (Brenton 1990). This system was to ensure that all of the member states would feel included in the development effort and encourage their national firms to adopt the standard. It was also to provide a means for smaller member states to air their concerns before the standard would be completed. However, as the voting only required a supermajority, it was possible to override the concerns of resistant countries in order to facilitate moving forward with development and adoption of the standard.

Once a single pan-European standard was in place, global adoption quickly followed (Funk 1998, 2002; Funk and Methe 2001). National telecommunications ministries and phone companies chose the technology because there were many participants (all of the major European telecommunications firms) offering compatible infrastructure and handset technologies. The competition on a common platform meant devices were less expensive. It also meant there was already a large user base, further encouraging adoption. At GSM's peak in 2005, 75 percent of the worldwide mobile industry used the standard (Bekkers and Updegrove 2012).

For IP, utopian ideals of a completely royalty-free standard initially struggled. Although the 1982 MOU recommended all SEPs be made available on a royalty-free basis, the French and German governments pushed for GSM to adopt their technologies based on the RAND policy for SEP inclusion (Bekkers, Dysters and Verspagen 2002). In contrast, Ericsson of Sweden offered another approach to mobile telephony on a royalty-free basis — one using non-proprietary technology. Once it was adopted, this royalty-free core helped to keep overall royalty rates low. The lower rates, in addition to the the advantages of the large user base, would further encourage worldwide adoption of the standard.

By 1998, GSM would only list 380 SEPs, some of which were duplicates due to their being filed in multiple jurisdictions (Bekkers and Updegrove 2012). Ericsson had very little proprietary technology in GSM. It chose instead to seek revenues by selling its equipment and handsets. Having created the technology core, Ericsson would enjoy a competitive advantage in making compliant technologies.

The single largest SEP holder would be Motorola (ibid.). Unlike Ericsson, which sought to earn revenues through sale of hardware — a pattern common among Chinese firms, as discussed below — Motorola sought to maximize its royalty returns. Motorola's technology was essential to the GSM protocols, but the company refused to even accept RAND principles. Motorola demanded the right to set royalty rates on a bilateral basis with any firm adopting GSM and to be able to discriminate among the firms that would be allowed to license its technology. Some European firms would be unable to produce GSM equipment when Motorola refused to license. For those that did secure a licence, Motorola's royalty rates ranged from 10 to 13 percent of the wholesale price of GSM products (Bekkers and West 2009). This and other licensing fees increased costs to non-favoured firms. Motorola and other leading GSM developers entered into cross-licensing agreements, giving themselves largely royalty-free access to the standard (Bekkers, Dysters and Verspagen 2002).

In the competing Code Division Multiple Access (CDMA) standard, the lead developer, Qualcomm, adopted a very different approach from Ericsson's. By the mid-1990s, Qualcomm was aggressively seeking to exit the infrastructure and handset industries. Without a competitive advantage in producing hardware, Qualcomm sought to maximize revenues through licensing its technology. The CDMA standard was based heavily on SEPs held by Qualcomm. While emphasizing licensing revenues, Qualcomm's approach to IP was quite open when it was approached by representatives from Korea's Samsung (Yoo, Lyytinen and Yang 2005). Whereas the GSM standard's leadership had not allowed Samsung to participate in developing or adjusting protocols or including new SEPs, Qualcomm welcomed Samsung's assistance. Samsung was able to include its IP in the CDMA standard. The market result was adoption of CDMA, rather than GSM, in Korea.

In the case of GSM, rules governing SEPs determined the market in two ways. Thanks to Ericsson's offer of royalty-free technology, overall costs were kept lower than they would have been had the German and French proposals — based on licensing patents — been adopted. However, Motorola's insistence on discriminating among licensees and controlling the rates for each licensee raised costs for all but the core developers of the standard. Those who contributed to the development of GSM stood to benefit far more than others, helping them earn greater profits and setting the stage for the next generation of telephony standards. In the case of CDMA, the willingness of Qualcomm to open the standard to Samsung led to the adoption of a CDMA monopoly in Korea and to helping Samsung develop core innovation capabilities it would use in future generations of mobile telephony. Both the GSM and the CDMA standard involved the use of SEPs. In both cases, not all firms from all countries were allowed to participate in standards development or to produce technology on the same terms. Firms that had not contributed to the development of either standard — for example, other Chinese telecommunications equipment

firms such as Julong or Potevio — would have to pay the required SEP licensing fees to those standards' SEP holders. Unlike Samsung (which enjoyed preferential IP access) or the GSM developers (with their patent-sharing agreements), such firms were at a cost disadvantage — one that would limit their abilities to invest in technology and create an unequal distribution of opportunity in the global economy.

CHINESE TECHNOLOGY STANDARDS AND SEPs

Developing-country firms face a very different environment than do established technology giants in Western and Organisation for Economic Co-operation and Development member countries. They often have weaker technology development capabilities and are attempting to engage in technology catch-up or leapfrogging. In some circumstances, the openness of technology standards with RAND-based licensing enables firms to make rapid increases in their technology capabilities (Blind and Jungmittag 2005). So long as a firm has sufficient capital to pay the licensing fees, it is able to access and utilize the technology and the patents embedded in a standard — not only to make the standards-compliant products but also to study and improve upon them. This access is an enormous advantage. Non-standardized technologies containing proprietary technology are not so open. Outside a standard with the RAND norms, an IP holder is free to fully block access to a technology, thus creating a true monopoly. When firms cannot access a technology in order to study, reverse engineer or improve upon it, any attempts they might make to technologically upgrade or catch up will be stymied.

Standards are more open, thanks to the RAND norm. Nonetheless, the opening of standards on its own is no panacea. As noted above, the conditions under which SEPs are licensed determines the structure and terms of competitive markets for standardized technologies. The licensing fees for developing compliant technologies can be onerous to manufacturing firms forced to pay full price. In the first decade of the 2000s, Chinese DVD manufacturers noted that the royalty costs were by far the largest single-cost item in production (Cai 2006; Chen 2008; Ding 2009). Even as the wholesale price of DVD players fell, and the prices of many components as well, the licensing fees remained constant, cutting into the already-thin margins of Chinese manufacturers.

One way to address this competitive disadvantage is to change the norms governing SEPs. Rather than allowing firms to restrict access — as Motorola did with GSM, in the case above — or to maximize unit profits through licensing — as happened with Qualcomm's CDMA standard — SEP policy can be designed to favour the Ericsson approach. Here, technology is licensed on a royalty-free basis and firms compete through manufacturing and sales of products, rather than through IP. For emerging economies, this approach complements their existing competitive strengths as manufacturers. It would lower their input costs while still offering the large consumer base advantages of standardized technologies.

To illustrate this effect, consider the case of audio-video encoding standards. One of the licence items in DVD players was for the MPEG-2 audio-video encoding standard. AV encoding standards convert analog sound or light waves into digital format (1s and 0s) and convert the digital format into analog for playback. The MPEG standards are created by the Moving Pictures Experts Group, a committee established in 1988 to coordinate the development of standards for audio and video (MPEG 2010).

The MPEG-2 standard was the de facto industry standard for all digital media in the 1990s and first few years of the 2000s until it was replaced by MPEG-4, also known as H.264, in March 2003. The standard was used for compact disc (CD) and DVD players, and early Internet video and music file and transmission formats. Under the terms of MPEG's SEP licensing arrangement, all devices compatible with MPEG-2 owed US$2.50 in licensing fees (Kanellos 2004). Fees were also owed for producers of CDs and DVDs. Chinese manufacturers, who by the early 2000s were producing over 70 percent of the world's DVD players, were heavily squeezed by these and other SEP licensing fees (Linden 2004). Chinese manufacturers and researchers studying MPEG-2 and H.264 claimed that of the hundreds of SEPs in the standards, most were technologically unnecessary. The Chinese claimed many of the patents were only incrementally different from other patents in the pool or entirely unnecessary for producing technologies that complied with the standard. Accordingly — the Chinese firms argued — the patent pool contained a large number of patents that they were obliged to license but which were unnecessarily raising their costs.

Once a standard is set, however, it is extremely difficult to replace, due to the power of the network effect. When a critical mass of users and suppliers exists for the standard, little space remains for a competing standard at the same level of technology. To help overcome the cost difficulties facing Chinese manufacturers, China's Ministry of Industry and Information Technology (MIIT) initiated a program to create an inexpensive next-generation audio-video-encoding standard.[2] Using contributions from government research institutes, university and industry labs, a Chinese alternative called AVS (Audio Video Standard) was published in 2005. Using a different approach — and hence not infringing on foreign patents — AVS was able to achieve encoding and compression efficiencies comparable

2 In-person interviews conducted by authors, Beijing, June and July 2012.

to H.264 (AVS 2012). Unlike the development of H.264, universities and government research institutes played a more significant role in AVS, contributing roughly half of the SEPs.

AVS's development alliance claimed adherence to basic RAND principles. However, the group in practice favoured royalty-free SEPs or submissions from firms that agreed to include patents in its patent pool rather than to negotiate licences on a bilateral basis (AVS 2004).[3] The AVS alliance strictly examined claims of essentiality, eventually including only 50 patents in its patent pool, versus nearly 1,000 for H.264. The patent pool was designed to reduce SEP licensing costs. The AVS alliance had also announced the licensing fee in advance — US$0.12 per device. Firms with SEPs were unlikely to make large amounts of money from licensing fees. The intention was to encourage widespread adoption of the standard and for the contributing firms to make revenues by producing and selling products rather than by licensing IP. Although the causal relationship is unclear, Chinese industry representatives and academics claim that the low price for AVS forced the MPEG-Licensing Authority to set a far lower royalty rate for H.264. Even with more SEPs than MPEG-2, the licence rate fell to US$0.15 from $2.50.[4] With lower licensing fees — whether for AVS or H.264 — Chinese manufacturers could produce standards-compliant products on terms far less onerous than demanded in the past. This would improve their profitability and ability to save and invest in future technologies.

Apart from creating alternatives to established technology standards in order to encourage lower licensing fees, Chinese firms and research institutions are actively seeking to set technology standards both domestically and worldwide for technologies that are still in the pre-standardization phase. One such initiative is the Intelligent Grouping and Resource Sharing (IGRS) standard being developed for the Internet of Things (IGRS 2012a). The IGRS standard's first form enables resource sharing among mobile phones, computers, televisions and cable receivers over short distances. Later developments have expanded the capabilities and range of IGRS to enable resource sharing and seamless communication among compatible devices at the metropolitan level. While today's telecommunications standards differ from those of wireless information-processing devices, such as laptops operating on Wi-Fi, IGRS hopes all devices can use the same protocols and communicate smoothly and efficiently. IGRS device networks are designed to be automatic, integrating new devices without needing intervention from service managers or information technology departments. Whenever IGRS devices are within range of one another, they will automatically connect and begin resource sharing as needed. Thus a phone's processing power could be greatly enhanced by resource sharing with a nearby computer. IGRS is not a dream of the Chinese alone; its protocols formed the basis for the international 3C convergence standard[5] adopted in 2012.

Showing the extent to which Chinese firms hope to change norms governing IP in standards to better their revenue and profit margins, IGRS was started by Chinese manufacturers, not research institutes. Although the IGRS working group was officially created by MIIT in 2003, the technology development had begun in leading firms such as Lenovo. After the working group convened, Lenovo and several other firms worked for 18 months on the protocols for the standard, presenting the results to MIIT in 2005. Participation in the working group remained limited, however, as it was widely seen as Lenovo's standard.[6] Other firms involved in development, including Great Wall, Konka, TCL and Hisense, were reluctant to declare or share their potential SEPs for fear of giving them away to their main competitors. To encourage further participation in the standard, Lenovo was formally removed from official leadership of the working group and a new IGRS corporate entity — similar to the legally separate licensing authorities of many other global standards — would be responsible for licensing and certification of standards-compliant products. Membership grew from 59 to 170 members by June 2012 (IGRS 2012b).

The SEP rules for the IGRS standard are much like those in AVS — built upon Chinese manufacturers' experience with the licensing of SEPs for earlier global standards. First, to prevent bilateral negotiations in which one party might be at significant disadvantage, SEPs included in IGRS must be licensed on a non-discriminatory basis (IGRS 2005). Firms unwilling to accept this condition cannot have their patents included in the standard. Further, any firm wishing to include technology in IGRS must fully disclose all potentially relevant patents. They are not permitted to declare essential patents *ex post*.

Further, similar to AVS, IGRS created a patent pool to facilitate both the licensing of the SEPs and the sharing of SEPs among participating firms. Firms whose patents are included in the pool enjoy "preferential treatment in using other units' patents" (IGRS 2015). Further, the patent pool's single licence is to be inexpensive. While there is no formal rule mandating nominal pricing, IGRS's members see it as in their interest to keep licensing rates low. Doing so is to encourage other Chinese firms — and manufacturers worldwide — to adopt this standard, in the hopes of building critical mass and ensuring lock-in. However, the emphasis for the member firms remains on increasing their market size for compliant products — not on maximizing licensing revenues.

3 Ibid.

4 Ibid.

5 The 3 Cs of convergence are content, computers and communications.

6 In-person interviews conducted by authors, Beijing, March 2012.

CONCLUSION

The development of globally accepted technology standards has been a boon for firms and consumers in developed and developing countries alike. However, the gains of these advantages are distributed unevenly thanks to the influence of SEPs and the varying terms under which they are licensed. Even when SEPs are licensed on a non-discriminatory basis, the rewards are unevenly distributed. Firms with large collections of SEPs enjoy royalty-free access to the standard due to their ability to enter patent-sharing agreements with other SEP holders. In contrast, those on the outside face a cost disadvantage because they must pay royalties for each standards-compatible product they produce.

In response, some emerging country governments, most notably China, have begun challenging the norms of independently determined "reasonableness" in licensing rates. Since technology standards effectively prevent the emergence of competing products — at a given level of technology — would-be market participants are obligated to compete on the terms set by the holders of SEPs. In China, standardization efforts over the past 15 years have emphasized a narrow definition of essentiality in the interest of limiting the size of the patent pool involved in a standard. By keeping the number of SEPs to a minimum, licensing arrangements should be simpler to navigate.

More importantly, standardization efforts in China have attempted to reshape norms concerning the licensing of SEPs. In principle, as with Ericsson's decision concerning GSM, IP should be licensed on a royalty-free basis. When firms submit proposals for the protocols of a standard, the terms under which they intend to license the technology are considered alongside technical merit. Where the best technology is not available on a royalty-free basis, the standards-development working groups attempt to create licensing patent pools available at nominal rates. This compromise approach is intended to reward innovative effort by allowing firms to receive royalties for their IP but also to encourage earnings through production of standards-compliant products. Ideally, the low royalty rates and widespread production will reduce costs for the technology, facilitating wide adoption.

Writ large, the Chinese approach is intended to show it is possible to protect and honour IP without making it a primary source of revenue. The challenge for foreign firms interested in pushing their technologies as part of Chinese standards is that these norms conflict with Western principles of hard IP rights in which IP holders are free to dispose of their property as they see fit. There is also a challenge and question as to whether leading Western multinationals will accept these terms for SEPs. To date, many firms have been reluctant to participate in Chinese standards-development efforts for fear of losing control over their IP. At the same time, however, some Western firms — most famously Apple — have publicly come out in favour of at least compulsory licensing for patents that might be used to obstruct the rollout or dissemination of a standard. This support shows there is potential for broader acceptance of the "Chinese" approach to SEPs.

Should Chinese standards prove their technological merit and competitiveness with foreign alternatives in the pre-standardization phase, it is possible that these new norms of less expensive IP may take root. This would benefit manufacturers and producers of standards-compliant goods and services. Those firms with production capability and cost controls will be better suited to benefit from this system than firms accustomed to partial, or full, reliance on licensing as a means of revenue generation.

Policy makers in different countries naturally act in the interest of their national economies. These differing visions have now spilled over into technology standardization. In international trade agreements, US negotiators push for protection of IP because this benefits US firms. In contrast, Chinese firms — which specialize in production — emphasize that IP should be widely available on favourable terms. In other emerging economies, this perspective might be welcomed. In India, for instance, there is a thriving generic pharmaceuticals industry. These firms compete not on licensing or technology but rather on production efficiency. As manufacturing and dissemination are the source of value, rather than licensing fees, such firms might be more open to the inexpensive IP approach. Smaller emerging economies with strong manufacturing sectors, such as Vietnam or Indonesia, would also stand to benefit from the lower costs created through an alternate SEP-valuation regime. For countries that utilize, rather than produce, standards-compliant products, the lower licensing fees could mean wider availability of and lower prices for these products.

While the Chinese approach is far from universally accepted, it does provide an alternative perspective on SEPs. Without rushing to make judgments, business leaders and policy makers in both emerging and developed countries should consider the developments in international standardization coming from China. Such consideration will allow negotiators to speak more frankly and clearly, thereby helping to foster more productive negotiations in which both sides understand the other and are thus better able to reach accommodation.

WORKS CITED

American National Standards Institute. 2013. "General Overview: What is a Standard." www.ansi.org/about_ansi/faqs/faqs.aspx#.UcWxc23hcfQ.

———. 2016. "3.0 Normative American National Standards Policies." In *ANSI Essential Requirements: Due process requirements for American National Standards*, 10. Washington, DC: American National Standards Institute. https://share.ansi.org/shared%20documents/Standards%20Activities/American%20National%20Standards/Procedures,%20Guides,%20and%20Forms/2016_ANSI_Essential_Requirements.pdf.

Arthur, Charles. 2012. "Google's Motorola takeover could trigger fresh patents battle with Apple." *The Guardian*, February 14. www.theguardian.com/technology/2012/feb/14/google-motorola-mobility-apple-patents.

AVS. 2004. *Constitution of the Audio Video Coding Standard Working Group of China*. Beijing, China.

———. 2012. "Audio Video Coding Standard Workgroup of China." www.avs.org.cn/en/.

Bekkers, Rudi, Geert Dysters and Bart Verspagen. 2002. "Intellectual property rights, strategic technology agreements and market structure: the case of GSM." *Research Policy* 31 (7): 1141–61.

Bekkers, Rudi and Andy Updegrove. 2012. "A study of IPR policies and practices of a representative group of Standards Setting Organizations worldwide." Presentation at the National Academies of Science, Washington, DC, October 3-4. http://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_072702.pdf.

Bekkers, Rudi, Bart Verspagen and Jan Smits. 2002. "Intellectual Property Rights and Standardization: The Case of GSM." *Telecommunications Policy* 26: 171–88.

Bekkers, Rudi and Joel West. 2009. "The limits to IPR standardization policies as evidenced by strategic patenting in UMTS." *Telecommunications Policy* 33: 80–97.

Berg, J. L. 1990. "Findings and Recommendations." In *An Analysis of the Information Technology Standardization Process*, edited by J. L. Berg and H. Schummy, 7–18. New York, NY: Elsevier Science Publishing Co.

Berg, J. L. and H. Schummy, eds. 1990. *An Analysis of the Information Technology Standardization Process*. New York, NY: Elsevier Science Publishing Co.

Berg, S. V. 1988. "Technical Standards and Technological Change in the Telecommunications Industry." Public Utility Research Center. Gainesville, FL: University of Florida.

Besen, Stanley and Leland Johnson. 1986. *Compatibility Standards, Competition, and Innovation in the Broadcasting Industry*. Santa Monica, CA: RAND Publishing.

Blind, Knut and Andre Jungmittag. 2005. "Trade and the impact of innovations and standards: the case of Germany and the UK." *Applied Economics* 37 (12): 1385–98.

Braunstein, Y. M. and L. J. White. 1985. "Setting Technical Compatibility Standards: An Economic Analysis." *Antitrust Bulletin* 30 (2): 337–56.

Brenton, M. E. 1990. "The Role of ETSI in IT Standardization." In *An Analysis of the Information Technology Standardization Process: Proceedings of the International Symposium on Information Technology Standardization held in Braunschweig, FRG, 4–7 July 1989*, edited by John L. Bergand Harald Schumny, 49–52. Amsterdam, the Netherlands: Elsevier Science Publishing.

Breznitz, Dan and Michael Murphree. 2013. "The Rise of China in Technology Standards: New Norms in Old Institutions." Research report prepared on behalf of the United States-China Economic and Security Review Commission, January 26. www.uscc.gov/sites/default/files/Research/RiseofChinainTechnologyStandards.pdf.

Cai, W. 2006. "Guochan Languang Gaoqing Dieji Dijia Jiaomai Guanwang Zhezhong (Domestic Blue Laser High Definition Disc Player Low Price Peddling Creates a Wait and See Attitude)." *Nanfang Ribao*, Guangzhou, China.

Chen, H. 2008. "Guang Gu Jiang Zao Shi Jie Shou Pi NVD 10 Yue Fen Shang Shi Ji Jie 1600 Yuan (Optics Valley to Create the World's First NVD — October Release Will Cost 1600 RMB)." *Chang Jiang Commercial Paper.*

Correia de Brito, Anabela and Jacques Pelkmans. 2012. "Pre-empting Technical Barriers in the Single Market." CEPS Policy Brief, No. 277, July 11.

Cusumano, M. A., Y. Mylonadis and R. S. Rosenbloom. 1992. "Strategic Maneuvering and mass-market dynamics: The triumph of VHS over Beta." *Business History Review* 66: 51–95.

Ding, I. 2009. "The Blu-ray Challenge in China." *China International Business*. Beijing, China: Zhong Guo Shang Wu Bu Guo Ji Shang Bao She.

Dolmans, Maurits. 2002. "EU Standardization: IPR Policies and RAND Licensing." (Cleary, Gottlieb, Steen and Hamilton of Brussels), DoJ/FTC Hearings on Competition and IP Comparative Law Topics — Other Jurisdictions.

Ernst, D. 2009. Challenges for Standards and Innovation Policies in the Emerging Global Knowledge Economy. *Standards and Innovation Policy in the Global Knowledge Economy*. National Bureau of Asian Research.

———. 2011. *Indigenous Innovation and Globalization: Challenges for China's Standardization System*. Honolulu, HI: East West Center.

ETSI. 2016. "Annex 6: ETSI Intellectual Property Rights Policy." ETSI Rules of Procedure. Brussels, Belgium: ETSI.

Farrell, Joseph and Garth Saloner. 1985. "Standardization, Compatibility and Innovation." *The RAND Journal of Economics* 16 (1): 70–83.

Funk, Jeffrey L. 1998. "Competition Between Regional Standards and the Success and Failure of Firms in the world-wide Mobile Communication Market." *Telecommunications Policy* 22 (4/5): 419–41.

———. 2002. *Global Competition Between and Within Standards: The Case of Mobile Phones*. New York, NY: Palgrave.

Funk, J. and D. T. Methe. 2001. "Market and Community Based Mechanisms in the Creation and Diffusion of Global Industry Standards: the case of mobile communication." *Research Policy* 30 (4): 589–610.

IGRS. 2005. "Organization Constitution of IGRS." Beijing, China: IGRS Alliance.

———. 2012a. "IGRS Background." Beijing, China: IGRS Alliance. www.igrs.org/templates/T_newslist_en/index.aspx?nodeid=133.

———. 2012b. "IGRS: Our Members." Beijing, China: IGRS Alliance. www.igrs.org/templates/T_newslist_en/index.aspx?nodeid=82.

———. 2015. "How to Join." Beijing, China: IGRS Alliance. www.igrs.org/templates/T_newslist_en/index.aspx?nodeid=111.

International Organization for Standardization. n.d. "How we develop standards." www.iso.org/developing-standards.html.

Kanellos, M. 2004. "DVD Player Profits down to $1." CNET.com, August 9.

Kesan, Jay P. and Carol M. Hayes. 2014. "FRAND's Forever: Standards, Patent Transfers, and Licensing Commitments." *Indiana Law Journal* 89 (1): 231–314.

Kindleberger, Charles P. 1983. "Standards as Public, Collective and Private Goods." *Kyklos* 36 (3): 377–96.

Linden, Greg. 2004. "China Standard Time: A Study in Strategic Industrial Policy." *Business and Politics* 6 (3).

Maskus, Keith E. and Stephen A. Merrill, eds. 2013. *Patent Challenges for Standard-Setting in the Global Economy: Lessons from Information and Communication Technology.* Washington, DC: National Academies.

MPEG. 2010. "About MPEG." Moving Pictures Expert Group. http://mpeg.chiariglione.org/about_mpeg.htm.

Özsomer, A. and S. T. Cavusgil. 2000. "The Effects of Technology Standards on the Structure of the Global PC Industry." *European Journal of Marketing* 34 (9/10): 1199–1220.

People's Daily. 2004. "EVD players not selling as expected in China." *People's Daily Online* (Beijing, China), January 10.

Simpkin, Julie. 2010. "Introduction to Patents." British Library Business and IP Centre. www.bl.uk/reshelp/pdfs/patents.pdf.

Van Eecke, Patrick and Maarten Truyens. 2009. "Standardization in the European Information and Technology Sector: Official Procedures on the Verge of Being Overhauled." *Shidler Journal of Law, Commerce & Technology* 11.

Yoo, Youngjin, Kalle Lyytinen and Heedong Yang. 2005. "The role of standards in innovation and diffusion of broadband mobile services: The case of South Korea." *Journal of Strategic Information Systems* 14: 323–53.

ABOUT THE AUTHORS

Michael Murphree is assistant professor of international business in the Darla Moore School of Business at the University of South Carolina. Michael's primary research interests include globalization, industrialization and economic upgrading, innovation in emerging economies, technology standards, and intellectual property rights. His research considers China in comparative perspective with other emerging economies and the developed West. He has four years' field research experience in China and speaks fluent Mandarin. Michael's work has been published in the *International Journal of Innovation and Regional Development*, *Harvard Business Review*, *Journal of Technology Transfer*, *Research Policy* and *Cardozo Law Review De Novo*, as well as in a book, a chapter and numerous commissioned reports. His first book, co-authored with Dan Breznitz, *The Run of the Red Queen: Government, Innovation, Globalization, and Economic Growth in China*, won the 2012 British International Studies Association (BISA) Susan Strange Book Prize as the year's best book in international studies.

Dan Breznitz is professor and Munk Chair of Innovation Studies and co-director of the Innovation Policy Lab at the Munk School of the University of Toronto. Dan is known worldwide as an expert on rapid-innovation-based industries and their globalization and for his pioneering research on the distributional impact of innovation policies. He has been an adviser on science, technology and innovation policies to multinational corporations, governments and international organizations, in addition to serving on several boards. Among his scholarly awards are the 2008 American Political Science Association's Don K. Price Award (for the year's best book on science, technology and environmental politics) and the 2012 BISA Susan Strange Book Prize, with co-author Michael Murphree. His policy work has been recognized by multiple awards, and in 2008 he was selected as a Sloan Foundation Industry Studies Fellow. In an earlier life Dan founded and served as chief executive officer of a small software company.

CHAPTER FOUR:
LOOKING BACK ON THE FIRST ROUND OF NEW gTLD APPLICATIONS: IMPLICATIONS FOR THE FUTURE OF DOMAIN NAME REGULATION

Jacqueline D. Lipton

INTRODUCTION

In 2012, the Internet Corporation for Assigned Names and Numbers (ICANN) opened the door to a new procedure that enabled applications for new generic top-level domains (gTLDs), that is, applications to run a registry for new strings to the right of the "dot" in a domain name. A domain name registry is a database of domain names and associated registrant information in a particular gTLD space.

Applications were made for 1,930 new gTLDs, of which 803 had been granted at the time of writing. Some applications were withdrawn, some were not approved, and some are still in process. The next round of applications for new gTLDs has not yet been opened.

This interlude between the first and second round invites consideration of some of the lessons learned from the first round, with particular reference to the protection of trademarks and freedom of expression. ICANN itself is evaluating the initial process with a view to streamlining the procedures the next time around.

This chapter focuses on specific situations that arose under the first process, with particular reference to balancing interests in trademarks against interests in free expression. It is not offered as a statistical overview of the process; it is, rather, a more impressionistic reflection on some of the key issues implicated in the balance of proprietary and expressive interests online. Specifically, it addresses the question of whether the advantages of the new gTLD system outweigh its costs in the new domain spaces, given the significant resources expended by applicants and opposers in the context of the application process.

THE NEW gTLD PROCESS: BACKGROUND AND UNDERLYING POLICIES

It seems almost a misnomer to refer to this program as "new" given that the window for new applications opened and closed in 2012, but applications are still being processed. However, it is the first iteration of a program that may have a significant impact on how business is conducted online. It is unclear how significant the new domain names will be in practice, given Internet users' tendency to rely on search engines to find online information and given how prominent the .com gTLD remains. Nevertheless, a number of entities have expended, and continue to expend, significant resources in applying for, and subsequently supporting or opposing applications for, new gTLDs.

First, a word on terminology. The acronym "gTLD" stands, as noted, for "generic top-level domain," which in simple terms means the alphanumeric string to the right of the dot in the domain name. Prior to the new gTLD process, ICANN authorized a number of entities around the world to maintain registries so one could register domain names in the second level of the gTLD, or to the left of the dot. The number of gTLDs available prior to the new program was 22, including the ever-popular .com, .net, .biz and .org, which are open-use domains. Other gTLDs were limited to particular types of industry or institutions, such as .edu for American universities and the country-specific suffixes, such as .ca or .ru.

In these original gTLDs, entities desiring a Web presence within a gTLD apply to an ICANN-authorized registry for a domain name that incorporates the relevant gTLD; for example, Nike Inc. registered nike.com.

While multiple registries administer one or more of the existing gTLDs, the new gTLD program makes it possible for an entity to operate as the sole registry for a new gTLD. Thus, the European Broadcasting Commission now runs the registry for .eurovision and the British broadcasting company BSkyB administers .sky (Register.eu 2015).

The policy aims of the new gTLD program are to increase competition and to avoid scarcity in domain spaces. ICANN began to formulate the program around 2005, with input from a multi-stakeholder process. It developed an applicant guidebook for the program and opened the doors to applications in 2012.

In formulating the new process, ICANN was sensitive to concerns about protecting intellectual property rights in new gTLD strings, as well as attempting to avoid improper use of new gTLDs with a view to protecting various interests, such as culturally specific terms, competing brand names and geographically relevant terms. In its *gTLD Applicant Guidebook*, ICANN (2011) articulated the following four specific grounds for objection to an application for a new gTLD: "(a) string confusion, (b) legal rights, (c) limited public interest, and, (d) community" (ibid., module 3.2.1). String confusion contemplates that the applied-for gTLD is too similar to an existing TLD or another applied-for gTLD. Legal rights objections refer to infringements of existing legal rights of the objector, which naturally include trademark rights. Limited public-interest objection applies when a string is "contrary to generally accepted legal norms of morality and public order that are recognized under principles of international law" (ibid.). Community objection relates to substantial opposition from a significant proportion of a community to which the gTLD might be explicitly or implicitly targeted. The government advisory committee (GAC) to ICANN has been extremely active in the area of community objections during the first round of applications.[1]

The guidebook puts in place specific procedures to oppose the granting of a new gTLD application. A number of

1 See https://gacweb.icann.org/display/gacweb/Governmental+Advisory+Committee.

applications were challenged. Some challenges are still in process. Challenges have been largely decided by arbitrators who have some familiarity with resolving domain name disputes under the Uniform Domain Name Dispute Resolution Policy (UDRP) in existing domain spaces. The GAC and other parties have also made representations to ICANN in the course of the process to clarify the rules applying to first-round applications.[2]

The following discussion focuses on four specific classes of concerns that have arisen in the new gTLD space: "gripe sites" (i.e., criticism sites) under new gTLDs, generic versus proprietary TLDs, closed versus open gTLDs, and geographically significant and other "public interest" forms of gTLDs. Before considering those categories of contentious applications, it is worth briefly summarizing how the balance of rights and interests in existing domain names (domains registered in the second level of pre-existing gTLDs) have been dealt with both legally and as a matter of market practice.

DISPUTES IN SECOND-LEVEL DOMAINS

Obviously, the introduction of the new gTLD process did not raise the prospect of balancing trademark rights and other important interests in the domain space for the first time. Registered domain names have grown exponentially over the years, as have the number of disputes, particularly since the advent of the UDRP, which makes the management of these conflicts fast, inexpensive and global. Despite the UDRP's success and popularity as a mechanism for resolving disputes about competing interests in the domain space, it is important to bear in mind that the system does not oust the jurisdiction of national courts. Domestic laws, including trademark laws, can still be applied to domain name disputes in appropriate contexts. The same is true of new gTLDs. Online activities, including uses of domains in the new gTLD spaces, will still be subject to national laws, however the ICANN dispute-resolution processes develop and however market practices develop. While this chapter focuses on ICANN and international market practices, the spectre of domestic litigation is still very real in both existing and new gTLD spaces.

The UDRP was implemented by ICANN in 1999, largely as an attempt to prohibit cybersquatting: registering a domain name corresponding with someone else's trademark in order to profit in bad faith from the domain name, either by offering it for sale to the trademark holder or to a competitor, or otherwise disrupting the trademark holder's business (ICANN 1999, section 4a). However, soon the UDRP was being applied to a variety of situations that did not necessarily fit the traditional cybersquatting mould. The UDRP has been applied to disputes involving unauthorized fan webpages, gripe sites, parody websites and commentary websites. These disputes have emphasized the importance of balancing a trademark holder's proprietary interests against the ability of individuals to criticize or comment on the subject of the domain name. Ideally, trademark-based regulations should not quell freedom of expression. This has always been a challenge for domestic trademark laws, and naturally affects the regulation of domain names based on trademarks. A detailed consideration of how disputes involving free speech versus trademark rights tend to be resolved by both domestic courts and UDRP arbitrators is beyond the scope of this chapter; however, there is a growing body of scholarship available to those interested (for example, Lipton 2008; 2010; Lindsay 2007).

The World Intellectual Property Organization (WIPO), whose arbitrators hear the most UDRP disputes, has also helpfully provided, and continually updates, a summary of the consensus views by arbitrators on particular types of disputes (for example, disputes involving personal names, disputes involving gripe sites) (WIPO 2011). For example, one consensus view on gripe sites is that:

> The right to criticize does not necessarily extend to registering and using a domain name that is identical or confusingly similar to the complainant's trademark. That is especially the case if the respondent is using the trademark alone as the domain name (*i.e.*, <trademark.tld>) as that may be understood by Internet users as impersonating the trademark owner. (WIPO 2011, section 2.4)

While the WIPO overview summaries theoretically do not hold precedential value because the rules of stare decisis do not apply to UDRP arbitrations, they offer useful guidelines about which rights and interests are typically prioritized above others in existing domain spaces. Those views might well inform the determinations of similar disputes in new gTLD spaces, and have certainly informed ICANN-authorized arbitrators dealing with disputes as to who has the right to a new gTLD.

Similar issues may well arise in new gTLD spaces as those that have arisen previously under existing gTLDs. Hypothetically, if a dissatisfied customer wanted to criticize a particular hotel franchise under the proposed .hotel gTLD using the "franchisename.hotel" domain,

2 See https://newgtlds.icann.org/en/program-status/odr/independent. This chapter does not provide a detailed summary of the application process, nor of the opposition procedures, but rather focuses on specific issues that have arisen in the context of the first round of applications. Readers interested in more details of the process, including the innovation of adding an independent objector as an ICANN-appointed officer empowered to make objections to particular applications and the auction process for disputed domain names, should consult ICANN's website at https://newgtlds.icann.org/en/applicants/auctions. ICANN maintains and publishes voluminous records of all aspects of the new gTLD process, including issues that will be reviewed prior to opening the second round of applications.

and was successful in securing the domain name, would the franchise be able to secure a transfer or cancellation of the domain name? The WIPO consensus view cited above suggests that there is something special about the "trademark.tld" versions of trademarks within a domain space. Would this apply to new gTLDs as well as existing and extremely well-known gTLDs, such as .com? This remains to be seen in practice, but the current WIPO consensus views may be particularly useful in resolving these kinds of disputes.

GRIPE SITES UNDER THE NEW gTLD SYSTEM

Some issues arising in the new gTLD spaces will, of course, be quite different from those arising in the pre-existing system. For example, some new registries will operate as closed registries, meaning that the applicant for the gTLD will not open registrations in the second-level domains to third parties. Thus, for example, if our hypothetical hotel franchise in the previous paragraph applied for a new gTLD comprising its trademark (".franchisename") and elected to operate it as a closed registry, it could ensure that disgruntled customers could not use any of the second-level domains under the gTLD for gripe sites. Disgruntled customers could still set up criticism websites under other gTLDs, like "franchisename.com" or "franchisename.biz" if those domain names were available. It could also register "franchisename.sucks" under the recently granted (and somewhat controversial) new .sucks registry (see Kay 2015).

The .sucks registry in particular — the registry is run by a Canadian corporation, Vox Populi — opens a whole new can of worms for the domain name system. Previously, the registration of a second-level domain name including a pejorative such as "sucks" (for example, franchisenamesucks.com) was generally unobjectionable as long as the use was not commercial and was for a legitimate gripe site, and not an attempt to deceive customers (WIPO 2008). Trademark owners were always free to register pejorative versions of their brand names for themselves, and often did, as defensive registrations to prevent others from using those names (Kay 2015). Those registrations are generally inexpensive under the existing systems because of the competition among registries, which keep registration prices low.

However, registries that control pejorative domain extensions such as .sucks, for example, could charge much higher fees for certain types of registration. At the time of writing, Vox Populi has actually implemented a pricing scheme that attributes higher values to certain kinds of domain spaces, seeking to onsell those names to registry services that will profit from selling third-level domains in the relevant domain space. Some premium non-trademarked terms, such as "life.sucks" or "divorce.sucks," are suggested for onsell at higher prices than standard terms under Vox Populi's current plans, such that a purchaser could then operate a third-level domain registry for customers interested in registering names such as "my.life.sucks." Vox Populi also suggests that some "market premium names" will be released for significantly higher prices than other terms. Vox Populi also offers the ability to block the use of market premium names at a lower rate.

Ultimately, of course, the market will decide what price tag, if any, to place on these kinds of domains. However, to the extent that pejorative terms in domains are regarded as useful online forums, the costs of speech could increase. It is simply too early to know for sure how problematic, or helpful, such gTLDs might be, assuming most want the Internet to be an inexpensive and efficient forum for both speech and commerce.

It may be that the market continues to place its faith in existing gTLD spaces and these newer gTLDs will not come into widespread use, but, again, it is too early to gauge the popularity of any given new gTLD space.

GENERIC VERSUS PROPRIETARY gTLDs

Outside of concerns about specific new gTLDs, general concerns have arisen about different categories of gTLDs. One of the distinctions, implicit in the discussion of the .sucks registry, is that some gTLDs are generic terms, whereas others connote proprietary terms (trademarks, business names). Generic terms include general words and phrases that might be applicable to a number of commercial interests, such as .hotel, .public or .free. Proprietary/trademark gTLDs, on the other hand, correspond to individual trademarks or business names — .google, for example.

Some terms correspond with both trademarks and generic words simultaneously. For example, "Amazon" is a geographical term when applied to the river but a trademark term when applied to the online retailer of that name. "Delta" is a generic word when applied to a geographical feature and a trademark when applied to the airline or the faucet company.

The ICANN guidebook contains some guidelines for considering the balance between trademark interests in a potential new gTLD and other competing interests, such as those of governments that may have an interest in specific geographical regions. The community objection (see above) is an obvious example of an attempt to strike this balance in practice. However, it is difficult to formulate a clear rule that will apply fairly in all situations. Amazon is a particularly interesting example in that more than one national government has objected to the granting of the .amazon gTLD, which was withdrawn from the first-round process. The GAC objected to the granting of the application because of concerns raised by Brazil and Peru. However, the online retailer intends to continue fighting

for the gTLD. In a letter to ICANN, the co-chairs of the US Congressional Trademark Caucus, J. Randy Forbes and Suzan DelBene, argued that neither Brazil nor Peru had legal right to the term Amazon and that the gTLD should be granted to the online retailer consistent with ICANN's stated policies (Ribeiro 2015).

While Amazon is a geographic term, the majority of generic terms do not correspond with geographic regions or geographic features as regards gTLDs. Thus, the potential concern about a private entity monopolizing a term does not necessarily have an obvious champion in terms of opposition during the application process. There are few who would have the wherewithal or knowledge to raise opposition. Private entities such as Amazon and Google applied for a number of generic terms such as .free and .public (Amazon) and .search (Google) in the first round. Objections to these applications came both from the GAC, on public-policy grounds, and also from other commercial entities who were concerned about the monopolization of those domains. The GAC issued a communiqué from Beijing on April 11, 2013, in which it suggested that safeguards be implemented for applications for certain categories of generic terms, including terms pertaining to children (for example, .kid), the environment (.earth), financial issues (.capital), gambling (.bet), charity (.care), intellectual property (.film), professional services (.doctor), corporate identifiers (.gmbh), generic geographic terms (.city) and "inherently governmental functions" (.army) (see ICANN 2013). Private objections were also made to businesses operating closed registries for generic terms. For example, Microsoft objected to Amazon and Google's respective applications for large numbers of generic terms that they intended to run as closed private registries. Microsoft's concern was that if Amazon, for example, monopolized the .book domain space for its own proprietary innovations, it would give them an unfair advantage in the marketplace.

ICANN ultimately called for submissions from the general community in response to objections to closed registers for generic terms, and ultimately decided, contrary to the provisions of the original guidebook (or at least not addressed by those provisions), that generic terms had to be operated as open registries (Burke 2014). The result is that successful applicants for generic terms as gTLDs are required to allow third parties to register in the second-level domains under that gTLD.

CLOSED VERSUS OPEN gTLDs

The move to distinguish between closed and open gTLDs was controversial, particularly as individual entities had expended significant funds in applying for "generic term" gTLDs that they intended to operate as closed domains. For example, Amazon had wanted to operate a closed registry for the gTLD .author. Amazon could have used that gTLD to set up webpages promoting its own authors, or providing services to new authors, or simply creating fan sites for established authors. Similarly, Google wanted to operate a closed registry for the .search gTLD. However, concern was raised about corporations monopolizing generic terms like these.[3]

The problem of closed versus open registries for generic terms as TLDs is even more complex than these two simple examples may suggest. While some terms are clearly generic, others are only generic in a certain context (delta, for example). Thus, even with a policy that does not allow closed registries for generic terms, ICANN and its authorized arbitrators are still faced with the problem of determining when a term is generic or proprietary. A policy that does not allow Amazon to monopolize the .book space might make sense, but it seems more problematic to determine whether a company such as Delta Airlines or Delta Faucet should, theoretically, be disallowed from operating a closed registry for a .delta domain. Of course, the delta example also raises the issue of multiple trademark holders each claiming the right to run a closed registry under the gTLD string that corresponds with its trademark.

With respect to generic domain names, in the case of multiple applications for the same gTLD, ICANN incorporated an auction procedure in its initial guidebook to determine who should be granted the domain name. The prices at which the names are ultimately sold at auction are additional to the original application fees, which were already close to US$200,000 per application (US$185,000 plus associated expenses). Some recent auction results underscore how valuable certain generic domains are deemed to be in the marketplace; .app was auctioned for just over US$25,000,000, for example.

Once a domain name application is successful, the registry will have significant discretion how to implement it and how much to charge for second-level domains. The .sucks example above illustrates how lucrative some successful applicants expect certain second-level domains to be in practice. Charleston Road Registry, the new owners of the .app gTLD, obviously plans to profit from running an open registry for the gTLD. Interestingly, Charleston Road Registry is a wholly owned subsidiary of Google. In the wake of the determination that generic terms could not be operated as closed registries, Google clearly plans to try its hand at profiting from registering second-level domains as a registry for new gTLDs.

While companies such as Google and Amazon are not able to pursue some of their earlier plans to establish innovative services within closed registries for certain new gTLDs, they are certainly exploring the option of extending into

3 At the time of writing, applications have not been finalized and there are no known outcomes on bids.

the domain name registration business. It remains to be seen whether these companies are able to profit in an already crowded domain name registration market.

GEOGRAPHICALLY SIGNIFICANT TERMS

As noted above, geographically significant terms have proved to be a particularly difficult case in the new gTLD space. Deliberations over the ability of private entities to run registries under such gTLDs have been time consuming and cost intensive. Additionally, even where a private entity is granted the right to run a registry for a geographically significant term, presumably most, if not all, such registries would have to be open on the basis that the term is, at least in some respects, generic. The .patagonia gTLD, for example, although initially applied for by the Patagonia sporting-goods company as a closed registry, is in fact being operated as an open registry by the Instra Corporation, an Australian domain name registry business. When Patagonia initially applied for the string, objections were raised by the governments of Chile and Argentina, and by ICANN's independent objector, an individual intended to represent the public interest. The company ultimately withdrew its application.

Geographically significant terms have also been problematic under the pre-existing gTLD system, given that the main dispute-resolution procedure for most existing domain names (i.e., the UDRP) prioritizes trademark interests over many other rights. The WIPO consensus document dealing with common issues arising in UDRP disputes notes that, generally, geographic terms cannot be protected under the UDRP unless they also comply with trademarks (WIPO 2011). It has proved difficult for the legal authority of a particular geographic region to establish unregistered trademark rights in jurisdictions where that authority has not registered a trademark (ibid.).

Thus, the various stakeholders in the global domain name community cannot glean much useful information from the pre-existing system as to how best to deal with geographically significant new gTLD applications. The result of several of the first-round applications for such TLDs has been that the terms in question are not used at all (for example, .amazon). The expenditure of significant resources in applications and objections to such applications could be regarded as wasteful in situations where a prospective gTLD is not approved for anyone's use. The lesson learned from the first round of applications may, in fact, be that corporations whose trademarks happen to correspond with geographical terms are simply out of luck with respect to new gTLDs corresponding with their trademarks, and should not apply for the gTLD in the first place unless they are prepared to run an open registry. Many such corporations probably do not want to go to the trouble of running an open registry, and it may defeat their purposes for applying for the gTLD in the first place.

Even when corporations are prepared to run open registries, objections to such applications may still be made by community groups, governments, the GAC and the independent objector, consistent with the policies set out in the original ICANN guidebook. For the near future, it is likely that applications for geographically significant terms under the new gTLD program will continue to be a costly and risky proposition.

Interestingly, the problems may not be so severe for gTLDs corresponding with personal names. Despite the fact that personal names (of celebrities, politicians, athletes, etc.) have raised particular concerns in pre-existing domain spaces, this is not likely to be the case under the new gTLD program. Many individuals have complained about registrations of .com names corresponding with their personal names by fans, cybersquatters and those who seek to criticize them (Lipton 2008; 2010). These disputes tend to arise under the UDRP because it is the fastest, most inexpensive and most effective way for an individual to deal with what they perceive as unfair practices involving personal names. The WIPO consensus document discusses personal names in much the same manner as geographical terms: they are only protectable under the UDRP if they correspond with trademark rights (WIPO 2011, section 1.6). However, unlike geographical terms, many names of well-known individuals have been regarded by UDRP arbitrators as comprising trademarks (ibid.).

Under the new gTLD system, it is unlikely that anyone would go to the trouble of seeking to apply for an entire domain name registry, and incurring the resultant costs, with respect to a personal name. While some surnames are so popular that it may be worth running a registry (for example, .smith, .jones, .wang), the idea of paying upwards of US$200,000 for an application to run a registry for a person's full name, such as ".hillaryclinton," seems unlikely.

CONCLUSION

While the discussion above is not comprehensive, it has highlighted some of the more significant issues that have arisen during the first round of applications for new gTLDs. Principles developed in relation to dispute resolution over names registered in pre-existing gTLD spaces have been helpful in foreseeing and resolving some of these issues. Some novel issues have arisen as well. It is too early to gauge the overall likely impact of this "new" gTLD program on use of proprietary terms and on freedom of expression in cyberspace. However, some areas bear close scrutiny in coming years, in particular with respect to the second round of applications.

The present gTLD program significantly moves the regulatory focus in the domain space away from old-fashioned cybersquatting to other concerns, such as wasted resources in cyberspace. From a public-policy perspective, the early days of the domain name system illustrated a regulatory focus on those who registered second-level domain names corresponding with well-known trademarks, with a view to profit from trading in or exploiting the marks. The UDRP was largely implemented to provide an efficient mechanism for trademark holders to protect their intellectual property rights in the digital environment. However, the new gTLD system is not particularly concerned with cybersquatting for much the same reason that personal name strings are not particularly problematic: it is simply too expensive for an applicant to target an individual or trademark holder by applying for a new gTLD string corresponding to the relevant alphanumeric string. Moreover, such an application would not likely be successful because of the pre-grant opposition procedures, under which an affected person or trademark holder could readily oppose the grant. And of course, cybersquatting in the second level of any newly granted gTLDs would be effectively handled under existing dispute-resolution mechanisms, such as the UDRP.

Unlike the pre-existing gTLD system, however, the present system creates the potential for significant amounts of wasted time and resources in the initial application procedures. Because of the costs of applications (with no guarantee of success) and the often lengthy and costly opposition procedures — and given the possibility of a competing application for the same string, which can result in an auction — hundreds of thousands of dollars can easily be incurred in a new gTLD application. ICANN's willingness to change the rules during the process (as it did when it disallowed closed registries for generic terms) also adds to the risk of wasted resources if an applied-for name is no longer desirable to the original applicant following a rule change.

While many business entities applied for new gTLDs, a number of them may not be so keen in the next round. Two of the leading applicants, Amazon and Google, were surprised by the objections to their proposals to run closed registries for certain generic terms in the new gTLD space. While they comprised a significant number of the applications, they (along with others who may have harboured similar business plans) will not likely be in the market for new gTLDs in the second round. The big winners seem to be those who seek to run competitive registries in new generic spaces. This will undoubtedly expand the domain name system and make more domains available in second-level spaces, likely at competitive prices.

However, a new registry that controls an entire gTLD will not be under the same competitive pressures as a registry that competes with other registries for services involving second-level domains in existing gTLD spaces, such as .com. For example, while multiple entities provide services to register second-level domains in the .com space, the only registry administering the second level of the .patagonia space is Instra, and, perhaps more worryingly, the only registry administering the .sucks space is Vox Populi. The latter is already suggesting that it will engage in a pricing model that attributes more value, and more cost, to certain terms in second-level spaces. It remains to be seen whether pricing models that attribute high values to certain domains are viable in the marketplace, or whether they are of little interest to anyone other than, perhaps, a trademark holder seeking to defensively register second-level domains to prevent gripe sites. Defensive registrations increase the costs of commercial practices online and may ultimately amount to little more than wasted resources, which are eventually passed on to consumers.

Individual governments, the GAC and the independent objector have led the charge with respect to preventing the granting of certain gTLD applications in situations where no one other than the applicant is likely to want the gTLD in question. Does this amount to wasteful activity and wasted online resources (the lack of domain names that otherwise would have been granted and used for commercial, social or generally communicative purposes)? It is simply not clear. Corporations such as Google and Amazon appear to have no shortage of domain names to use for their various business services, but, in contrast, governments like those of Brazil and Peru do not seem to have plans for an application for the .amazon gTLD.

Domain names are unquestionably big business. The exponentially increasing number of UDRP disputes every year attests to that, alongside the willingness of many entities to apply for and expend additional resources defending oppositions or bidding at domain name auctions for new gTLDs. The question remains as to whether the advantages of the new gTLD system outweigh its costs. At the end of the first application round, when all the applications have been dealt with, will the gTLD program look more like an exercise in wasted resources than an important cyberspace innovation? What will the level of interest in a second-round application process look like, and how much might the rules change before then? It is too early to tell with any degree of certainty. Because many of the high-profile disputes, disagreements and uncertainties under the first round are highly case-specific to the parties involved, it will be difficult to extrapolate any general principles about the benefits and challenges inherent in the system. Some issues are clear: closed registries for generic terms in the new gTLD spaces have proved problematic in practice, and geographical terms are highly problematic, with no clear uniform rules forthcoming, in particular in cases where geographical terms correspond with valuable trademarks.

Many trademark holders did not apply for gTLDs corresponding with their marks in the first round, either waiting to see how the system worked out or feeling that it was a wasteful and unnecessary expenditure of resources.

The way the application process has unfolded in recent years is unlikely to make any of those businesses more interested in applying for their trademarks as new gTLDs in subsequent rounds. Again, ICANN has given the cyberspace law and policy community much food for thought, and some interesting current and forthcoming challenges about balancing commercial interests and freedom of expression in the domain space.

WORKS CITED

Burke, Molly. 2014. "How to Turn a Closed Generic gTLD into a Restricted One." CircleID, June 11. www.circleid.com/posts/20140611_the_case_for_turning_closed_generic_tlds_into_restricted_tlds/.

ICANN. 1999. "Uniform Domain Name Dispute Resolution Policy." October 24. www.icann.org/resources/pages/policy-2012-02-25-en.

———. 2011. *gTLD Applicant Guidebook*. May 30. https://archive.icann.org/en/topics/new-gtlds/rfp-clean-30may11-en.pdf.

———. 2013. "GAC Communiqué — Beijing, People's Republic of China." April 11. www.icann.org/en/system/files/correspondence/gac-to-board-11apr13-en.pdf.

Kay, Roger. 2015 "Saga of .Sucks Domain Generates Laughter, Agony." Forbes.com, June 29. www.forbes.com/sites/rogerkay/2015/06/29/saga-of-sucks-domain-generates-laughter-agony/.

Lindsay, David. 2007. *International Domain Name Law: ICANN and the UDRP.* Oxford, UK: Hart Publishing.

Lipton, Jacqueline. 2008. "Celebrity in Cyberspace: A Personality Rights Paradigm for a New Personal Domain Name Dispute Resolution Policy." *Washington and Lee Law Review* 65 (4): 1445–528.

———. 2010. *Internet Domain Names, Trademarks, and Free Speech.* Cheltenham, UK: Edward Elgar.

Register.eu. 2015. "The New gTLDs: Some Could Make You Blush!" www.register.eu/en/news/the-new-gtlds-some-could-make-you-blush.

Ribeiro, John. 2015. "US Lawmakers Back Amazon.com's Bid for .amazon Domain." *PC World*, June 24. www.pcworld.com/article/2940032/us-lawmakers-back-amazoncoms-bid-for-amazon-gtld.html.

WIPO. 2008.*Sermo, Inc. v. CatalystMD. LLC*, Case No. D2008-0647, July 2. www.wipo.int/amc/en/domains/decisions/html/2008/d2008-0647.html.

———. 2011. "WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Second Edition (WIPO Overview 2.0)." www.wipo.int/amc/en/domains/search/overview2.0/.

ABOUT THE AUTHOR

Jacqueline Lipton holds the Baker Botts Chair in Law at the University of Houston Law Center and is a visiting lecturer at the University of Akron School of Law. She holds Ph.D.s in law from Cambridge University (UK) and Griffith University (Australia). She is widely published internationally in the areas of Internet governance, domestic and international intellectual property, privacy law and secured finance law.

CHAPTER FIVE:
THE DIGITAL TRADE IMBALANCE AND ITS IMPLICATIONS FOR INTERNET GOVERNANCE

Susan Ariel Aaronson

ACRONYMS

ACTA	Anti-Counterfeiting Trade Agreement
ECIPE	European Centre for International Political Economy
EDRi	European Digital Rights network
EFF	Electronic Frontier Foundation
EOP	Executive Office of the President
EUA	European University Association
FTA	free trade agreement
GATS	General Agreement on Trade in Services
ICT	information and communications technology
IPR	intellectual property rights
ITA	International Technology Agreement
MIIT	Ministry of Industry and Information Technology (China)
NGO	non-governmental organization
NSA	National Security Agency
NTIA	National Telecommunications and Information Administration
OECD	Organisation for Economic Co-operation and Development
TiSA	Trade in Services Agreement
TLDs	top-level domains
TPP	Trans-Pacific Partnership
TTIP	Transatlantic Trade and Investment Partnership
UAE	United Arab Emirates
USITC	United States International Trade Commission
USTR	United States Trade Representative
WTO	World Trade Organization

INTRODUCTION

In many countries today, leaders see lagging (or no) growth, sagging employment and rising underemployment (Lagarde 2015; Easterly and Pennings 2013). While they recognize that the Internet is not a magic bullet, these leaders believe that the Internet, and its associated digital technologies (products and services that facilitate the creation, storage, analysis and sharing of data and information), might be a potential economic saviour (Chakravorti, Tunnard and Chaturvedi 2015; *The Economist* 2014). These leaders have seen the Internet transform what firms do as well as how they do it (Organisation for Economic Co-operation and Development [OECD] 2013a) and they are optimistic about the promise of new digital technologies, including mobile telephony and the "Internet of Things." They hope that these digital technologies will bring expanded growth, higher productivity, more and better jobs and greater purchasing power for their citizens.[1]

According to the consulting firm McKinsey, in 2010, the Internet contributed on average 3.4 percent of GDP for the 13 countries it surveyed. McKinsey also found that for the 4,800 small and mid-size enterprises surveyed, the Internet and associated technologies created 2.6 jobs for each job lost. Moreover, some 75 percent of the Internet's benefit has gone to traditional industries through efficiency gains and expanded markets (McKinsey Global Institute 2011). The United Nations Conference on Trade and Development (2015, 21-22) asserts that many studies have shown that the Internet improved consumer welfare as well as labour productivity.

The Internet and associated digital technologies have made it cheaper and easier to trade information; to collaborate and work across borders; and to fund and sell goods and services (Manyika et al. 2014; eBay Inc. 2014). Growth in global markets for digital technologies is likely to continue because some 61 percent of the world's population has yet to go online (Meeker 2015; Meeker 2014; World Bank 2014, 7).

Digital technologies can also enhance human welfare. The World Bank found that "rapid penetration of digital technologies is changing the lives of the poor" (World Bank 2014, 2). These technologies have empowered small farmers to search and sell in more markets and to interact with government without travelling long distances, visiting multiple government offices or paying bribes (ibid.). Scholars have found that Internet usage is positively correlated with happiness (Penard, Poussing and Suire 2013). A forthcoming study of 700,000 Israelis found that Internet use increases life satisfaction and it is especially helpful to the poor, disabled and elderly (Lissitsa and Chachasvil-Bolotin 2016).

Nonetheless, digital technologies also bring costs. Because Internet technologies have transformed how goods and services are produced and delivered, some job sectors have already become obsolete and others will be transformed. Citizens might lose jobs, businesses and incomes. Digital technologies might also have unanticipated side effects, one example being increased social and economic disparities.

1 According to the US International Trade Commission (USITC), higher productivity in digitally intensive industries due to the Internet increases output in these industries while it simultaneously lowers production costs and consumer prices. These gains spill over to the rest of the economy and lead to economy-wide effects. Higher demand for workers in the digitally intensive industries drives up wages in the labour market and draws workers from other sectors of the economy; it can also increase aggregate employment as more workers are brought into the labour force. The productivity-based reductions in costs translate into lower prices for consumers, which increases the purchasing power of their wages (USITC 2014, 20).

Although more people can now participate in trade, the Internet has also facilitated cross-border trade in drugs, money laundering and other underground activities. The same technologies that help citizens collaborate to influence and monitor government have also made it easier for governments to monitor their citizens (World Bank 2014, 6, 12).

Despite these costs to the economy and human welfare, policy makers across the world are trying to encourage the development and use of digital technologies. For example, China, the European Union, Singapore and Sweden have digital agendas that include investments in related infrastructure and robust government support for research (USITC 2014; European Union 2014). But leaders might not find it easy to develop digital prowess. One country, the United States, has a huge competitive advantage in digital technology. Ranked by market capitalization, the United States is home to 11 of the 15 largest Internet-related businesses (Apple, Google, Facebook, Amazon, eBay, Priceline, Salesforce, Yahoo, Netflix, LinkedIn and Twitter) while China is home to four (Alibaba, Tencent, Baidu and JD.com). No companies from Brazil, Canada, the EU 28, India, Japan or Korea crack the top 15 (Meeker 2015, 6). Officials outside of the United States worry that US (and, to a lesser extent, Chinese) Internet behemoths have too much influence and market share, and the ability to quash local competitors.

In order to develop or maintain healthy firms that focus on digital technologies, policy makers must first create an effective enabling environment, including competition (antitrust), educational, human rights and infrastructural policies. Policy makers want to encourage the rule of law online and prevent unlawful behaviour such as the dissemination of hate speech or child pornography, fraud, identity theft, cyber attacks and money laundering (Council of Europe 2014, 7). However, by restricting data flows and competition between firms, policy makers might retard technological innovation and the Internet's "generativity." They might also reduce the ability of firms to aggregate services and data analytics through cloud services and the potential of the Internet to provide information globally. Finally, such strategies could affect Internet governance. According to Jonah Force Hill (2014, 4), "restricted routing…may be technically infeasible without initiating a significant overhaul of the Internet's core architecture and governance systems, which itself would have significant negative effects."

In their efforts to create such an environment, these officials might sometimes take steps that could discriminate against foreign market actors, and in so doing, distort trade. These actions can have unintended consequences for the stability and integrity of the Internet (Daigle 2015). In May 2015 alone, several governments announced such policies. France, Germany and the United Kingdom asked Twitter, Facebook and Google to pre-emptively remove content considered extremist (Fairless 2014; Hirst 2015). The Israeli Foreign Ministry asked global platforms to take down Holocaust denial and anti-Semitic websites identified from the results of searches throughout the Internet (Jewish Telegraphic Agency 2015; Ronen 2015; *Jerusalem Post* 2015). In addition, the Chinese Ministry of Industry and Information Technology (MIIT) announced that domain name registrars in China would be forbidden from selling domain names in top-level domains (TLDs) not approved by the Chinese government. Registries and registrars will also be required to have a physical presence in China to comply with the regulation. These actions resonated throughout the Internet as a whole. Radio Free Asia reported that the US-based domain-name registry XYZ.com agreed to ban domain names based on the 12,000 words banned by the Chinese government. In so doing, the firm and the Chinese government undermine freedom of expression in both the United States and China while making it harder for Beijing-based activists to transcend China's Great Firewall (Radio Free Asia 2015).[2]

Governments are not only attempting to nurture local competitors, disadvantage foreign ones and regulate the Internet within their borders but also acting to protect their constituents from perceived harm. With the revelations of former US National Security Agency (NSA) contractor Edward Snowden and others, people around the world learned that the United States and its intelligence partners in the Five Eyes (Australia, Canada, New Zealand and the United Kingdom) were monitoring their communications. In many countries, citizens and policy makers have called for greater restrictions on cross-border information flows in the belief that data kept at home will be more secure and that local suppliers are more trustworthy.[3] For example, India required major Internet companies to locate servers in the country; Canada and Korea required that certain types of data must be stored in the country; and Brazil required federal agencies to use only Brazilian data storage, telecommunications and information technology services for national security reasons (Edgerton and Robertson 2014; Chander and Le 2014; USITC 2013; Kommerskollegium 2014). Officials and citizens are not only worried about the privacy of their communications; they also fear that they have become too dependent upon US companies for web services (which must comply with

2 By July 2015, the MIIT will not allow registries not approved by the Chinese government to operate or sell domains in China. Some analysts fear that only Chinese companies will gain approval, but it remains to be seen. Kevin Murphy (2015) offers one perspective, versus a more sanguine James Seng (2015). Murphy notes that thus far there are 14 TLDs on the approved list, all of which are operated by Chinese registries. The list does not include the TLDs ".com" or ".net" nor does it contain any country-code TLDs other than "cn."

3 Australia, Canada, New Zealand, the United Kingdom and the United States have been sharing signals intelligence since World War II (Kozner 2013; BBC 2014).

US rules on privacy and national security).[4] As well, they are concerned that the United States continues to dominate not only the Internet economy but also global Internet governance institutions in ways that could benefit US interests or companies. Global Internet governance reflects the influential role of US early web actors who wanted an ad hoc, multistakeholder, bottom-up and self-regulatory approach to Internet governance (EurActiv.com 2010; 2013).

The United States has responded vigorously and often without nuance to efforts by governments to create the domestic-enabling context. In recent years, many US executives and policy makers have labelled other governments' efforts to restrict information flows "digital protectionism" (BSA 2015; Business Roundtable 2012). Their concern is understandable. The stakes are huge: US firms in digitally intensive industries sold $935.2 billion in products and services online in 2012, including $222.9 billion in exports; they purchased $471.4 billion in products and services online in 2012, including $106.2 billion in imports (USITC 2014, 5). The USITC estimates that digital trade in certain digitally intensive industries resulted in an estimated 3.4 percent to 4.8 percent increase in US GDP ($517.1–$710.7 billion in 2011; ibid., 1). *The Wall Street Journal* described US efforts to thwart digital protectionism as a battle, noting that it would affect Internet governance (Fairless 2014). The United States' determination to use trade agreements and policies to govern cross-border flows and to reduce digital protectionism stems from an imbalance between the Internet power and influence it holds and the Internet power and influence of other nations.

This chapter will examine how governments use trade agreements and policies to address cross-border Internet issues, focusing on the imbalance between America's zeal for free-flow rules and other countries' ambivalence toward such rules. It will show that while trade agreements are logical venues for governing information flows, they might not be the best places to address these issues unless policy makers also include language designed to enhance human welfare, Internet operability and the rule of law. This chapter uses the word "Internet" as shorthand for advanced digital technologies and services that greatly facilitate the creation, storage, analysis and sharing of data and information (World Bank 2014, 4). Digital trade policies can be defined as domestic, regional or international principles, policies or rules designed to encourage the cross-border flow of information, products or services delivered online. The chapter uses the USITC's (2013, 5-1-5-2) definition of digital protectionism: barriers or impediments to digital trade, including censorship, filtering, localization measures and regulations to protect privacy.

4 See *Inside US Trade* (2014a). On the Trade in Services Agreement (TiSA) negotiations, please see Australian Government (2014). On the Transatlantic Trade and Investment Partnership (TTIP), see http://ec.europa.eu/trade/policy/in-focus/ttip/, and on the Trans-Pacific Partnership (TPP), see www.dfat.gov.au/fta/tpp/.

The chapter begins with an explanation of the importance of information flows to the Internet and Internet governance, then moves to the debates over various trade agreements, concentrating on issues where the United States and its trade partners have failed to find common ground. It then examines whether policies adopted to nurture digital firms at the national level or policies adopted to achieve important national policy goals are truly "protectionist," that is, designed to distort trade between foreign and domestic producers. Next, the chapter focuses on some of the problems "netizens," policy makers and businesses might encounter as a result of policy makers' increasing reliance upon trade policy as a tool to govern cross-border information flows. After focusing on the costs and benefits of using trade policies and agreements, the chapter concludes with policy recommendations.

WHY TURN TO TRADE AGREEMENTS AND POLICIES TO REGULATE THE INTERNET?

The Relationship of the Internet to Information Flows

The Internet and related technologies are built on information flows. The consulting firm McKinsey (2014) notes there was an 18-fold increase in cross-border Internet traffic between 2005 and 2012. Cross-border information flows are also the fastest growing component of trade. Using International Monetary Fund data from 2008 to 2012, economist Michael Mandel (2013) found that such flows increased 49 percent, while trade in goods and services grew some 2.4 percent. Digitization of goods (such as music and movies) is changing the mix of flows, transforming global logistics and enabling new and smaller players to participate in trade (McKinsey Global Institute 2014, 2-3; eBay Inc. 2014).

Policy makers can do a lot to hamper or encourage cross-border information flows. Individuals and firms move data from a location in one country with one set of rules to another location with another set of rules. If policy makers could devise shared rules to encourage the free flow of information, they would facilitate interoperability among legal regimes. More people would have greater access to information and more information would be created and exchanged (Manyika et al. 2014; Tietje 2011).

However, policy makers are struggling to find ways to ensure that the rules governing cross-border information work effectively across nations and systems, reflecting the ideal of the global interoperable Internet. Citizens and policy makers around the world disagree on how and where to regulate cross-border information issues such as intellectual property, privacy, cyber security and censorship (Castro and Atkinson 2014, 2; World Bank 2014; Daigle 2015). Although governments might share

the Internet, countries have different ideas regarding the role governments should play online. Moreover, countries have different ideas as to how and where to regulate cross-border information flows in the interests of their citizens and firms.

Domestic Needs versus the Internet's Global Public Goods Nature

Some nations, such as Brazil and India, believe that governments should do more to exercise direction over the Internet. Often officials in these countries argue that greater government control will help them to provide public goods online, such as education or health care, and to foster innovation and economic growth. Other governments, such as China and Russia, want a rethink of Internet governance and propose greater international control over the Internet. And still other governments, such as Vietnam, are just beginning to set the ground rules for the Internet within their countries (Aaronson with Townes 2012, 3 fns 10–16).

Governments might have good reasons for restricting information flows but doing so could result in unanticipated negative side effects on the Internet as well as on economic growth. Economists generally agree that information is a global public good that governments should provide and regulate effectively. When states restrict the free flow of information, they shrink access to information, which can reduce economic growth, productivity and innovation, not just in their own country but globally (Maskus and Reichman 2004, 284-85; Khan 2009). Moreover, when officials place limitations on which firms can participate in the network, they might reduce the overall size of the network, which also could raise costs (Hill 2014, 32; Daigle 2015).

Meanwhile, when government officials retain and control access to large amounts of information about their citizens, they might undermine human rights (Chander and Le 2014; Pearce 2014). Individuals who feel that their privacy is not respected might be more reluctant to engage in free speech, participate in politics or search for information, because such activities could make them targets of government monitoring. In contrast, individuals who have some control over their information might be more willing to share it (Powles 2015). According to the UN Special Representative on the Right to Freedom of Opinion and Expression, Frank La Rue, "Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas…Surveillance takes away people's ability to be anonymous." He added that "restrictions on anonymity have a chilling effect, dissuading the free expression of information and ideas...exacerbating social inequalities" (La Rue 2013, 13, #49, #20).

Why Have Governments Used Trade Agreements to Regulate Information Flows?

Trade agreements and policies could provide a framework to govern cross-border information flows. First, policy makers recognize that when we travel the information superhighway, we are often trading. Second, officials understand that digital trade creates wealth. However, officials can only create that wealth if nation states can find common ground not only on the rules governing their obligations (what nations must do to encourage trade) but also on the exceptions to the rules (when nations can breach their obligations and how they must engage in trade policy making when doing so).

The most important and internationally accepted trade agreement, the World Trade Organization (WTO), already governs digital trade to some extent (Burri forthcoming). The WTO has 162 member states that agree to adhere to its rules and to bring disputes that they cannot settle to its binding system of dispute resolution. The WTO and other trade agreements have a long history of promoting trust between buyers and sellers who do not know each other (Büthe and Milner 2008; Simmons, Dobbin and Garrett 2007). When we go online, just as when we trade, we operate on trust. Producers and consumers of information often do not know each other. Thus, Internet producers and consumers must trust that others will protect confidential personal or business information.

The WTO contains several agreements covering issues affecting digital trade. They include the Information Technology Agreement, which eliminates duties for trade in digital products;[5] the Agreement on Trade-Related Aspects of Intellectual Property Rights, which protects trade-related intellectual property pertinent to information technology, such as computer programs;[6] and the General Agreement on Trade in Services (GATS), which has chapters on financial services, telecommunications and e-commerce, all of which relate to cross-border information flows. However, for purposes of brevity, we focus on the e-commerce chapters of GATS (as well as the free trade agreements [FTAs] discussed below), as they are most relevant regarding cross-border information flows.

5 The Ministerial Declaration on Trade in Information Technology Products (known as the International Technology Agreement [ITA]) was concluded by 29 participants at the Singapore Ministerial Conference in December 1996. The agreement has been signed by some 81 countries representing about 97 percent of world trade in information technology products. The ITA provides for participants to completely eliminate duties on information technology products covered by the agreement. In July 2015, the signatories expanded the ITA list (WTO 2015a; Office of the United States Trade Representative [USTR] 2015a; see also https://ustr.gov/sites/default/files/ITA-expansion-product-list-2015.pdf).

6 See also www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm and www.wto.org/english/tratop_e/trips_e/tripfq_e.htm.

The GATS e-commerce chapter sets rules governing how nations can trade services that are electronically delivered. These rules also delineate exceptions: how and when signatory nations can restrict trade in the interest of protecting public health, public morals, privacy, national security or intellectual property, as long as such restrictions are necessary and proportionate, and do not discriminate among WTO member states (Goldsmith and Wu 2006; Mattoo and Schuknecht 2000).

However, the language in the chapter predates the World Wide Web, the Internet, mobile and cloud computing, and the Internet of Things, among other developments. Member states designed the GATS language to ensure it would remain relevant as technology changed but several member states have said that they need clarification on specific points and want to update these rules to avoid misunderstanding.[7] For example, in 2011, the United States wrote that the WTO must update its work program (and ultimately the system of rules) on electronic commerce "if the WTO is to remain relevant to the innovative technologies and business models that can support economic growth and opportunity" (WTO 2011). The United States also expressed concerns that governments still lack guidance as to whether electronic commerce should be governed by WTO commitments under trade in goods or services and if these rules could cover the mobile Internet and cloud computing (ibid.). The WTO Deputy Director-General Harsha V. Singh (2013) admitted that "the issues we need to address at the WTO are fairly distinct and legalistic, including, for example, classification dilemmas, the implications of technological neutrality for the trade rules, when does a 'challenge' or 'obstacle' to e-commerce also fit within our definitions of a restriction on trade." Academics and business leaders have also argued that the WTO's rules are incomplete, out of date and in need of clarification (Burri 2013; Makiyama 2011; National Board of Trade, Sweden 2012).

Meanwhile, although the GATS states nothing explicitly about information flows, WTO members have begun to apply these obligations when settling disputes about cross-border information flows (Wunsch-Vincent 2006; Goldsmith and Wu 2006). The WTO's Dispute Settlement Body has adjudicated two trade disputes related to information flows. After Antigua challenged the United States' ban on Internet gambling, the WTO ruled that governments could restrict service exports to protect public morals if these barriers were necessary, proportionate and non-discriminatory (not discriminating between foreign and domestic providers).[8] The WTO's Appellate Body also examined China's restrictions on publications and audiovisual products, noting that commitments for distribution of audiovisual products must extend to the distribution of such products by the Internet.[9] However, neither dispute has provided clarity regarding key issues such as whether governments can, for example, restrict sales of offensive items such as Nazi memorabilia or if they can censor and filter websites (Mattoo and Schuknecht 2000, 19-20; Mattoo and Wunsch-Vincent 2004; Goldsmith and Wu 2006; Santoro and Goldberg 2009). Until members challenge these policies in a trade dispute or negotiate new rules, we will not have clarity on why, how and when governments can restrict cross-border flows (Aaronson with Townes 2012).

THE ROLE OF THE UNITED STATES

History

The United States was the first nation to include provisions related to cross-border information flows in its trade agreements, as well as the first to use trade policies to govern cross-border information flows. Some 20 years later, America remains the most vociferous booster of trade agreements as a tool to advance the benefits of the Internet internationally.

In 1997, President Bill Clinton announced a "Framework for Global Electronic Commerce," which focused on private sector leadership; a limited role for government intervention, including on cross-border flows; strategies designed to encourage global e-commerce; and provisions on privacy and security. It states, "The US government supports the broadest possible free flow of information across international borders…The Administration...will develop an informal dialogue with key trading partners… to ensure that differences in national regulation...do not serve as disguised trade barriers" (Executive Office of the President [EOP] 1997).

The Clinton administration had some success in its drive to set rules governing e-commerce and data flows. President Clinton directed the USTR to make the Internet a tariff-free zone and to secure new agreements to make electronic commerce a seamless global marketplace. The members of the WTO agreed to a temporary moratorium on taxes on cross-border data flows, which they have continued to renew.[10] The president directed the Department of Commerce to develop a uniform international commercial legal framework that recognizes, facilitates and enforces electronic transactions worldwide, and to work with the private sector to develop national online privacy standards (ibid.).

7 See Marchetti and Roy (2013); news items during the WTO's 2013 Forum (WTO 2013a; 2013b); and for an example of a misunderstanding, "GATS: Fact and Fiction" (WTO n.d.).

8 See www.wto.org/english/tratop_e/dispu_e/dispu_e.htm#disputes, Case 285.

9 See www.wto.org/english/tratop_e/dispu_e/dispu_e.htm#disputes, Case 363.

10 On OECD, see its action plan for electronic commerce (1998); see also www.wto.org/english/tratop_e/dda_e/status_e/ecom_e.htm.

In the years that followed, the United States signed bilateral agreements with the Netherlands, Japan, France, Ireland and Korea to remove barriers to e-commerce. It and other members of the OECD endorsed a global action plan for electronic commerce in 1999, which had been put forward by various international business groups. Policy makers hoped that the action plan would build trust, establish ground rules for e-commerce and maximize the benefits of electronic commerce (Alliance for Global Business 1999). The OECD also developed widely accepted privacy principles and principles for Internet governance (OECD 2011a; 2011b; 2013b).

The Bush administration (2000–2008) included e-commerce chapters in many of its FTAs, but the language did not keep up to date with the rapidly moving Internet world. The Bush administration, like the Clinton administration before it, did not foresee that other nations would become increasingly competitive, and at times interventionist, in the Internet sector. More people from more countries were going online and building domestic companies to serve local Internet needs. While US companies (and, to a lesser extent, European companies) still dominated Internet searches and social networking, other companies outside of the United States found a niche in providing services, cyber security, apps or games.[11] Meanwhile, policy makers from many of these countries were increasingly determined to control the Internet within their borders and to facilitate the rise of domestic Internet firms. Australia, China, India, Russia, Thailand, Turkey and the United Arab Emirates (UAE), as examples, restricted or blocked information flows in the first decade of the twenty-first century (Hindley and Makiyama 2009; Meier and Worth 2010). These governments cited a wide range of reasons for their actions: some sought to protect their citizens from harm; others aimed to prevent their citizens from organizing online. Still others acted to restrict information flows to encourage local Internet development (Aaronson with Townes 2012, 3).

Whatever the rationale, executives from many US-based Internet companies saw in these actions a threat to their bottom lines. They argued that when governments restricted information flows, companies had fewer viewers and customers for their sites, content and apps. Moreover, executives from these companies recognized that their future growth would lie outside the United States and the European Union. Internet analyst Mary Meeker notes that 79 percent of the users of the top 10 Internet platforms come from outside the United States. Facebook provides a good example. In 2008, some 50 percent of Facebook users were outside the United States; by 2013, 86 percent of its users lived abroad (Meeker 2014; 2015). These executives demanded that officials do a better job of limiting digital protectionism, which they often saw as any restriction on data flows. For example, Google used the research of the Open Network Initiative (a Canadian think tank) to document how more than 40 governments instituted broad-scale restrictions of information flows.[12] Google reported that governments were using opaque regulation, wholesale blocking of services, bias against foreign competitors and other strategies that could violate international trade rules under the WTO (Google 2010, 6–11).

In 2009, new US President Barack Obama's administration made digital trade a major trade issue. Obama's team was particularly attuned to the importance of digital technologies for economic growth and determined to respond to policies that influential US Internet companies deemed protectionist. In 2010, the Department of Commerce asked firms to describe the restrictions they encountered. Some of the firms and associations took an interesting stance, essentially, warning that people who live in glass houses should not throw stones. They noted that the United States also had various rationales to restrict information flows. They suggested that the government should adopt a more principled approach by linking an open Internet, information flows and human rights.[13] Unfortunately, the United States did not use this feedback to develop a more coherent approach — one that would link openness, interoperability and Internet resiliency to economic growth and the protection of digital rights online (Aaronson 2015).

In 2011, Obama administration officials promised to put forward provisions in trade agreements that would encourage information flows while simultaneously limiting how and when governments could restrict such flows and favour domestic firms. They began at the WTO (2012a; 2012b).[14] In 2011, as part of Doha Round negotiations to reduce trade barriers related to the cross-border flow of services such as banking, the United States and the European Union proposed that members agree not to block Internet service providers or to impede the free flow of information online. The United States also wanted members to use the WTO venue to discuss information flows, cyber security and privacy as related issues. But

11 See http://mashable.com/2013/10/28/google-monthly-traffic/; the Internet map (http://internet-map.net/); and the Internet timeline (www.infoplease.com/ipa/A0193167.html). See also *The Economist* (2014).

12 See Google (2010, 5-6; 2011). On the Open Network Initiative, see https://opennet.net/about-oni.

13 Federal Register: The Daily Journal of the United States Government (2010); for the comments, see National Telecommunications and Information Administration ([NTIA] 2010a). For examples of comments showing the lack of consistency in US policies and actions, see NTIA (2010b, 9-10, 23; 2010c, 17, 22-23).

14 However, discussions on free flow might be revived as part of a plurilateral agreement on the liberalization of services (www.ecipe.org/media/media_hit_pdfs/ecipe-esf-seminar-in-brussels.pdf). See also Martin (2012) and Palmer (2012).

other member states did not respond enthusiastically to this proposal.[15]

Hence, the United States turned to bilateral and regional trade agreements. In 2012, the United States and the Republic of Korea became the first states to include specific language related to the free flow of information in the electronic commerce chapter of their FTA. Article 15.8 of the agreement says that "the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."[16] However, this provision does not forbid the use of such barriers, nor does it define necessary or unnecessary barriers. In short, the language is not actionable. In addition, the agreement did not clarify whether legitimate online exceptions to free flow, such as cyber security measures or privacy regulations, are necessary or not. It is unclear whether one party could use this language to challenge another party's use of such barriers (Aaronson with Townes 2012).

After Korea, the Obama administration decided to make the language in its future agreements binding (*countries must or shall do x* instead of *countries shall endeavour to do x*) and disputable (one state may challenge another country's policies as trade distorting). In this way, the United States would have greater leverage to ensure that barriers to information flows would be limited. The United States achieved binding language in trade agreements with 11 countries in the TPP. It is currently negotiating with 28 countries in the TTIP and with the European Union's 28 members and with 23 other members of the WTO in the TiSA negotiation. If these agreements are approved and go into effect, they will cover most of the world's leading Internet providers and netizens and have significant effects on Internet openness and governance.

Government officials have negotiated trade agreements in secret for centuries (Aaronson and Moore 2013). But this strategy aroused significant opposition from many individuals active in Internet governance. As noted earlier, the Internet has long been administered by experts, companies, governments and individual volunteers working collaboratively in a transparent manner. Understandably, these individuals were uncomfortable with the notion that governments were negotiating regulations that could dramatically affect the Internet — without transparency and without direct involvement from a diverse group of stakeholders.

Critics of US efforts to use trade policies to address these issues based their analysis on newpaper reports and leaked text provided by the media and transparency organizations such as Wikipedia. These leaked documents provide some insights into what the negotiators are discussing and where they are finding stumbling blocks. However, because they contain so much bracketed text, we can only guess at potential compromises. As a result, with the exception of the TPP, which has been posted online,[17] the analysis that follows is based on speeches and publications by trade officials, leaks and news reports.

US Objectives

The United States is clearly the main driver of efforts to use trade agreements for both facilitating information flows and governing cross-border information flows. The US government tends to make a strictly economic case for such policies rather than to argue that such provisions might contribute to improved governance, digital rights and Internet operability.

For example, on May 1, 2015, Deputy USTR Ambassador Robert Holleyman II gave a speech in which he explained why the Obama administration made "promoting the digital economy a key component of its trade agenda." He stated that the United States has 12 priorities for its digital trade agenda. First, the government wants trade policies to help the Internet remain free and open; hence, customs duties on digital products should be prohibited. He stressed that the United States' trading partners should refrain from discriminating against the digital products of foreign providers and collaborate to develop rules to prevent not only discriminatory and protectionist barriers to cross-border data flows, but also forced localization or requirements that companies build data centres in every market they serve (Holleyman 2015).

In addition, the United States wants its trade partners to explicitly state that they will not require companies to transfer their technology, production processes or other proprietary information to persons in their respective territories, and also to make binding commitments ensuring that they will not require companies to purchase and utilize local technology. Thus, the US government wants trade agreements to reduce opportunities for digital protectionism, data localization or favouritism. Nonetheless, it also wants trade agreements to build trust online. It wants provisions to ensure that companies and consumers develop and use technologically neutral signatures and authentication methods, provide enforceable consumer protections, safeguard network competition, foster innovative and effective encryption, and never block companies from using encryption. Holleyman suggested that language in the agreement

15 The WTO's GATS sets limits as to when governments could block services (such as Internet services), but it is vague: Members can only invoke this exception to the rule "where a genuine and sufficiently serious threat is posed to one of the fundamental interests of society." GATS (19) 33 ILM, 1167, Article XIV, n. 5. On US and EU proposal forbidding blocking, see *Inside US Trade* (2011a).

16 US/Korea FTA, chapter 15, article 15.8, "Electronic Commerce," www.ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text.

17 https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text

should be technologically neutral so that the agreements could apply to future innovative digital products and services as well as to new business models and services that might emerge, unless a specific negotiated exception applied (ibid.).

Ambassador Holleyman stressed that the United States would push for every one of these 12 priorities in the TPP, TTIP and TiSA, although he said nothing about how America's trade-negotiating partners were responding to these priorities or why they might not share them (ibid.). Moreover, Holleyman's speech and other government documents reveal that the administration continues to make a narrow case for rules governing cross-border information flows. It could, for example, better explain the link between Internet freedom and Internet openness by showing how Internet openness might foster economic development. However, the United States and its allies have not figured out how to help governments devise an appropriate regulatory context to support Internet freedom and openness or what the rule of law means online. As a result, US policies to promote cross-border information flows seem disconnected from policies to sustain the open Internet (Aaronson with Townes 2012, 21).

THE THREE AGREEMENTS: TPP, TTIP AND TiSA

TPP

The TPP is the first trade agreement to include binding commitments on cross-border information flows and to limit digital protectionism. Moreover, the agreement contains transparency requirements that could bring much-needed openness, due process and increased political participation to trade (and Internet-related) policy making in countries such as Vietnam. The TPP could play an important role in encouraging cross-border information flows and in providing tools to challenge censorship and filtering. But the TPP can have those effects only if the agreement goes into effect and other countries such as Indonesia, South Korea and Thailand sign on; policy makers use its provisions to maintain Internet openness and challenge Internet censorship and filtering as barriers to trade; and other nations build on the TPP's language in their FTAs or at the WTO.

To understand the TPP's scope and potential, it is necessary to first understand the role of services (such as e-commerce) in the TPP. The services chapter (chapter 10) first defines services and service suppliers and delineates how cross-border services can be regulated. It defines service suppliers as individuals or firms that supply services across borders. Service suppliers do not need to interact financially with their consumers, and thus include firms that provide e-commerce services for free (such as Dropbox, Facebook, Google and free apps). The TPP defines cross-border services (such as e-commerce) as services delivered from one party into another party's territory, services produced in the territory of one party and delivered to a person living in another territory, or services provided by a national of one territory to a party in another territory. Hence, the rules governing services encompass both Internet service providers and Internet users.

However, the language in the TPP's e-commerce chapter (chapter 14) raises two important questions: Do the rules cover *all* cross-border information flows by *all* Internet actors? Does the chapter apply to both suppliers and consumers of digital transmissions? The USTR says yes, based on the content of the services chapter. However, the language in the e-commerce chapter raises questions: its key text related to information flows is article 14.11, which notes that "each party shall allow the cross-border transfer of information by electronic means…when this activity is for the conduct of the business of a covered person." But some information flows are not for the conduct of the business of a covered person — they do not involve the exchange of money. A covered person is defined in article 14.1 as an investment, investor or service supplier. The agreement only mentions users in article 14.8, where it recognizes the benefits of protecting users' personal information. Like the United States, the government of Australia describes the benefits to business and does not mention users in general: "For the first time in a trade agreement, the TPP countries will guarantee the free flow of data across borders for service suppliers and investors as part of their business activity. This 'movement of information' or 'data flow' is relevant to all kinds of businesses…TPP countries have retained the ability to maintain and amend regulations related to data flows, but have undertaken to do so in a way that does not create barriers to trade" (Australian Government 2015).

Trade agreements generally focus on business, so this focus is not unusual. However, the language in the TPP differs from that of the FTA with Korea, which although not binding, did not limit the chapter to "covered persons." In fact, in a side letter to the Korean trade minister, the USTR noted that the agreement applies to Internet users. Why was this side letter and language necessary for Korea but not for the TPP? More importantly, given its arguments that the agreement helps support the open Internet (not just for business but for all users), the USTR must clarify how Internet users in general, rather than just business users, benefit from this language.

The TPP includes very specific language related to privacy of consumers. In earlier FTAs, such as US-Korea, the parties simply stated that they recognized "the importance of maintaining and adopting transparent and effective measures to protect consumers" and agreed to cooperate to enforce laws and enhance consumer welfare. However, the TPP parties agreed to new and enhanced

privacy rules. Article 14.7 requires the parties to "adopt or maintain consumer protection laws." Moreover, the TPP nations made it clear that privacy is important to maintaining trust online, in article 14.8: "Each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce." They will publish information on personal privacy protection and "endeavor to adopt non-discriminatory practices." Finally, the countries agreed to develop mechanisms to promote compatibility among different privacy regimes. With this language, the parties were able to find common ground on the "free flow" language that could satisfy nations with strong domestic (or principal regulations) on privacy, such as Australia, as well as nations with more voluntary approaches, such as the United States.

The agreement clearly limits data protectionism. As the government of Australia noted, "TPP countries cannot force businesses to build data storage centres or use local computing facilities in TPP markets. TPP countries have committed not to impose these kinds of 'localisation' requirements on computing facilities — providing certainty to businesses as they look to optimise investment decisions" (Australian Government 2015, 1).

In addition to its language encouraging digital trade, reducing digital protectionism and protecting privacy, the TPP has language supportive of the open Internet. First, article 14.4, "Non-Discriminatory Treatment of Digital Products," includes binding language that prohibits parties from favouring domestic products and their creators and owners or from discriminating between products or producers from home versus abroad. However, governments are still allowed to provide subsidies or grants to their own producers or creators. Moreover, article 14.10 builds on long-standing principles for Internet governance designed to empower consumers. Thus, the parties recognize the benefits of consumers being able to make their own choices, to connect their own devices to the network and to access information on the network management practices of their Internet access service suppliers. Although it is one of the few sections where the TPP actually discusses Internet users, the language is not binding upon governments.

The TPP recognizes that there are times when nations must breach their obligations and provides guidelines as to when and how in its "exceptions." The USTR notes that "the General Exceptions chapter ensures that the United States and the other TPP Parties" are guaranteed "the full right to regulate in the public interest, including for national security and other policy reasons" (USTR 2015b). The TPP incorporates the general exceptions delineated in GATS in its chapter 29. This language could be useful to individuals and firms concerned about the trade implications of censorship and filtering. If a government censors or filters, it might cause rerouting of information flows and such actions often distort trade between entities within and among nations. Hence, one TPP party could use the agreement to challenge censorship or filtering in nations that might do so in a discriminatory manner. The two nations that have some record of censorship and filtering, Malaysia and Vietnam, were given two years to revise their policies, after which period they could be subject to such challenges.

The binding language in the TPP's e-commerce chapter is disputable under the rules in chapter 28. The law firm Covington and Burling also notes that "a government measure that violates a commitment in the e-commerce chapter might also violate an investment commitment in Chapter 9, and to that extent could be subject to investor-state dispute settlement" (Hansen and Slater 2015).

What Does the TPP Mean for Future Trade Agreements and Internet Governance?

The TPP will have an impact on Internet governance simply because it covers so many Internet providers and users and because its commitments will affect how governments can behave when regulating cross-border information flows. The TPP parties have a population of some 800 million people, or 11.4 percent of the world's total. Many of these individuals are already active on the Internet. Moreover, the TPP includes important and growing markets for digital products and services in countries such as Vietnam. Colombia, Indonesia, the Philippines, South Korea, Taiwan and Thailand have expressed interest in joining the TPP should it come into effect (Bryson and Nelson 2015). Moreover, if the TPP is approved, it could alter how non-signatories deal with cross-border information flows — they would have to comply with the TPP rules when they exchange information with the TPP parties. Finally, the United States will want to use the TPP as a guidepost for other trade agreements, including the TTIP and the TiSA under negotiation. Other governments, too, will need to consider this language and what it means for their firms' cross-border flows. However, the United States might be overselling the benefits of the agreement to the Internet — just as critics might be exaggerating its costs to the Internet and Internet governance.

The Response to the TPP: Key Concerns

Many netizens did not greet the TPP with a parade along their Twitter feeds (or any other virtual Main Street). Instead, they signalled disaster. For example, Boing Boing reported that activists have concluded that the TPP "spells doom for free speech online" (Doctorow 2015). *The Guardian* headlined that "Wikileaks release of TPP deal text stokes 'freedom of expression' fears among activists" (Thielman 2015). The Electronic Frontier Foundation (EFF) blogged, "Open access isn't explicitly covered…But that doesn't mean that they [the TPP and its proponents] won't have a negative impact on those seeking to publish or use open

access materials." The blogger warned that individuals that seek to circumvent paywalls could be accused of civil or criminal offences (Malcolm 2015). Meanwhile, Evan Greer (2015), campaign director of the Internet activist group Fight for the Future, argued that the TPP threatens basic access to information: "The agreement poses a grave threat to our basic right to access information and express ourselves on the Web and could easily be abused to criminalize common online activities and enforce widespread Internet censorship." The website Expose the TPP (n.d.) came to the most radical conclusion, noting the agreement "would undermine Internet Freedom."

These analysts based their concerns on the intellectual property provisions. The United States and Japan (and, to a lesser extent, Australia) want to protect and enhance online copyright, believing that strong copyright protections further innovation, which is a key factor in the competitiveness of these nations (IP Commission 2013). But as activist Evan Greer (2015) notes, this extensive regime of copyright enforcement "has been repeatedly co-opted by special interests to censor legitimate content from the web and to discourage free expression." These critics stress that the TPP would force the adoption of the US approach, which they believe does not provide due process to individuals who allegedly breach online copyright. Moreover, they note that, if approved, the TPP would require countries such as Chile (which has established a judicial notice-and-takedown regime) to change to the US system (which, they argue, provides less protection to Internet users' expression and privacy). Finally, they stress that signatories would be required to adopt criminal sanctions for copyright infringement that occurs without a commercial motivation. These critics also argue that users could be jailed or hit with debilitating fines over file sharing or have their property or domains seized even without a formal complaint from the copyright holder (EFF 2015; New 2014).

Some critics of the TPP make economic and human welfare arguments against the TPP and online copyright. They stress that the current approach to protecting online copyright is too biased toward the needs of copyright owners and could reduce innovation by stifling opportunities to explore and develop new models that exploit the Internet and digital services (Samuel 2011). TPP critics have concluded that the current approach to protecting online copyright might be counterproductive: it neither enhances human welfare nor encourages innovation.

Proponents, in turn, argue that critics misunderstand the objectives and side effects of the online copyright language in the TPP. They maintain that the TPP's approach is balanced because it allows the dissemination of content and protects individuals who want to access that content online with exceptions and limitations for "fair use" — criticism, commentary, news reporting, teaching, scholarship and research — hence, non-commercial sharing would not be criminalized (Holleyman 2015). Given the importance of this debate, policy makers should carefully consider the current strategy and ask if it is the most appropriate approach for nations with inadequate governance, funds and will to protect intellectual property rights (IPR). They should also examine if it truly enhances human welfare and encourages innovation in the digital age.

Opponents have also expressed concerns about the e-commerce chapter and cyber security. The chapter says that governments cannot force suppliers to give up their source codes to foreign governments, even for national security reasons. The TPP prohibits signer countries from asking software companies for access to their source codes. According to cyber security expert Stewart Baker (2015), "Right now, this is a measure US software companies want," because they provide the bulk of mass market software in the market. "But that's likely to change, especially given the ease of entry into smart phone app markets. We're going to want protection against the introduction of malware into such software. The question of source code inspection is a tough one. If other countries can inspect US source code, they'll find it easier to spot security flaws, so the US government would like to keep other countries from doing that. But I doubt US security agencies are comfortable letting Vietnam write apps that end up on the phones of their employees without the ability to inspect the source" (ibid.). These provisions could, indeed, undermine cyber security efforts. Moreover, it is interesting that the agreement bans spam (unsolicited commercial electronic messages or communications), but says nothing about banning malware. Yet, malware is an equally important trade issue. Malware can be redefined as malicious cross-border information flows. Malware not only damages business but has significant negative effects on human rights. When business or home computers are infected, users are less able to use their computers in the manner to which they are accustomed. They may experience slower computer performance, systems problems and cyber insecurity. US trade agreements have included voluntary language on cyber security writ large; it seems strange to address cyber theft but not to try to address malware.

TPP critics have also implied that the disappointing language of the TPP stems from an undemocratic process that favoured business at the expense of netizens. They might be confusing process and outcome. In June 2015, the website Intellectual Property Watch obtained some 400 pages of email traffic between the USTR and officials and industry advisers related to the TPP. Although most of the content of the emails is blacked out, these emails provide insights into how the USTR develops policy, whom USTR staff talk to and what information they provide. The emails reveal that the USTR is often receptive to business interests and that at times firms even draft language for the USTR.

However, the released emails do not include emails to non-business representatives, such as members of Congress or academics and civil society groups concerned about IPR. Thus we cannot say that the USTR did not consult with or consider opinions of individuals critical of the US approach to protecting online IPR (New 2015).

Although the critics are probably right that the process was not sufficiently transparent, they are exaggerating the effects upon Internet operability and freedom. Firms such as Google, eBay, Walmart and Citigroup also have a stake in maintaining an open and stable Internet. While these firms do not speak for netizens, netizens are their clients; these firms share their need for rule of law online as well as for limits to censorship, filtering and protectionist policies.

Finally, critics condemn the agreement because it was negotiated in secret. While the critics are quite right to note that the process of negotiating the TPP did not engender trust, the critics should keep in mind that the United States and its negotiating partners have not figured out how to update trade negotiations (which requires trust among negotiating partners) and operate with the transparency necessary for good governance in the Internet age (which requires greater openness and dialogue with the public).

Moreover, the critics have not carefully reviewed the transparency chapter. While it is ironic that an agreement negotiated in secret could promote transparent accountable governance, the transparency chapter is likely to have such an effect on how the 12 countries regulate the Internet, for the following reasons. Chapter 26 requires government officials to "ensure that its laws, regulations, procedures and administrative rulings are promptly published and allow individuals to comment on these measures." The parties shall "consider comments received during the comment period." Hence, the parties must take the comments into account. In addition, each party shall provide "reasonable opportunities" to present their concerns with regulations and administrative proceedings. Article 26.4 notes that each party shall establish or maintain judicial or administrative tribunals to review administrative actions and allow the parties affected by such actions opportunities to support or defend their positions. Finally, these review bodies must provide decisions based on evidence and submissions of record. In short, the agreement requires due process and political participation in the regulatory process. To put it differently, the TPP can advance access to information, due process and political participation for Internet and other types of regulation. Moreover, previous studies have shown that such improvements in governance related to trade issues can spill into the polity as a whole (Aaronson and Abouharb 2011).

Trade agreements such as the TPP are complicated and legalistic. They are easy to demonize and hard to understand. To fully understand the potential impact of the TPP, critics should examine the agreement in its entirety as well as the individual chapters. In so doing, critics can more accurately assess its implication on Internet norms of open access, free flow of information, interoperability and multi-stakeholderism. These critics should also consider the motivations of governments as well as the limitations of international trade agreements. Alas, few are willing to take these steps because both proponents and critics have exaggerated the benefits and costs of the TPP.

TTIP

The United States and the 28 countries of the European Union have been negotiating a free trade agreement since 2013. The two trade giants are leaders of the information economy as well as advocates of the multistakeholder approach to Internet governance. Unfortunately, US and EU policy makers have not reconciled their approach to trade policy making with the more transparent and multisectoral approach to Internet governance. The European Union has been significantly more open than the United States about the talks. The European Union has published many of its negotiating positions and their rationales online. However, as of January 2016, it has not yet posted documents for the e-commerce provisions.[18]

The public debate on the free-flow provisions in the TTIP has taken on a different tone than that surrounding the TPP provisions. European and US citizens and non-governmental organizations (NGOs) have expressed concerns about the agreement's potential effect on IPR reform on privacy and other human rights, as well as about the negotiations' effects on public services and governance (European University Association [EUA] 2014; EUA 2015; European Digital Rights [EDRi] 2015; Aaronson 2015; Bridges 2014). European citizens and policy makers are worried that the trade agreement could undermine the European Union's commitment to its citizens' online privacy. An Austrian law student, Max Schrems, brought these concerns to the European Court of Justice and ultimately the court ruled that the US approach to protecting privacy was inadequate. As of January 2016, the two countries have not found common ground on how to bolster the US system so that it meets European data protection standards (Wilhelm 2015).

Public support for strong data protection has a long and proud history in the European Union. Europeans view privacy as a vital human and consumer right. All 28 EU member states are also members of the Council of Europe, a group of 47 European countries, and as such, they are required under human rights law to secure the protection

18 See http://ec.europa.eu/trade/policy/in-focus/ttip/documents-and-events/#eu-position and http://trade.ec.europa.eu/doclib/press/index.cfm?id=1230.

of personal data.[19] Every EU citizen has the right to personal data protection and firms can only collect that data under specific conditions.[20] The European Union also requires member states to investigate privacy violations.[21] The European Commission's Directive on Data Protection, which went into effect in October 1998, prohibits the transfer of personal data to non-EU countries that do not meet the European Union's "adequacy" standard for privacy protection. The European Union requires other countries to create independent government data protection agencies and to register databases with those agencies; in some instances, the commission must grant prior approval before personal data processing begins. To bridge these differences in regulatory strategy, the US Department of Commerce, in consultation with the European Commission, developed a "Safe Harbor Framework" that certifies that US companies meet the European Commission's requirements (Export.gov 2013).

Surprisingly, given its strong commitment to privacy, the European Commission (the executive branch of the European Union) has included only aspirational language on privacy in its FTAs. For example, in its agreement with Korea, chapter 6 refers to trade in data, and article 7.43 of the services chapter says that each party should reaffirm its commitment to protecting fundamental rights and freedoms of individuals and adopt adequate safeguards to the protection of privacy (European Union 2011). Moreover, neither the European Union nor Canada included binding privacy provisions in their recent trade agreement, which was completed in 2014 but is not yet approved.[22]

Although the European Union has not used trade agreements to disseminate its approach to privacy, the EU Directive has had an effect on trade. Some nations, such as India and China, are weighing how to make their laws interoperable with EU privacy provisions.[23] Meanwhile, other countries, such as the Philippines, have adopted EU data protection policies.[24] The European Union would like to make its regulations on data protection global, which could have huge consequences for firms built on the mass acquisition of personal data, such as Facebook, Google and so on. Such companies would have to change their business models.

Currently, companies such as Facebook are free to users, but under the terms of its agreement with its users, Facebook uses their data "for internal operations, including troubleshooting, data analysis, testing, research and service improvement" (quoted in Frizell 2014). When data leaves the company, Facebook says it makes the data anonymous, making it impossible for outside researchers to track down individual Facebook users (ibid.). Not surprisingly, given the import of firms that use the free business model to the US economy, the United States has opposed any efforts to mandate a specific approach to data protection (Aaronson with Townes 2012). The Safe Harbor system had several problems. It was built on trust but many Europeans were not sure they could trust the big firms that provided them with social networking, web search and other services. Second, Safe Harbor did not provide them with a strong system of enforcement. If companies in the Safe Harbor failed to comply with their rulings, an independent body could report these cases to either the Federal Trade Commission or the US Department of Transportation, depending on the sector, both of which have legal powers and can impose effective sanctions to oblige them to comply (European Commission — Justice 2012). According to the European Commission, serious cases of non-compliance will result in companies being struck off the Department of Commerce's list, which means that they will no longer receive data transfers from the European Union under the "safe harbor" arrangement. Moreover, if the system doesn't work the European Union could repudiate the entire Safe Harbor Framework (European Commission — Justice 2015c).

Despite public concerns and litigation, the European Union has not had to repudiate Safe Harbor but instead to remake it. In 2011, the European Commission decided to update its data protection rules to meet changes in technology and increased public concern about privacy (European Commission 2011). After obtaining extensive public comment, the European Commission released its proposed regulation in January 2012. This regulation includes language granting a right to be forgotten (meaning

19 The Council of Europe promotes common and democratic principles based on the European Convention on Human Rights and other reference texts on the protection of individuals. It is also home to the European Court of Human Rights, which clarifies European law related to human rights (Rihter 2011).

20 The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention No. 108") requires that personal data be processed fairly and securely for specified purposes on a legitimate basis only, and establishes that everyone has the right to know, access and rectify their personal data processed by third parties or to erase personal data that has been processed without authorization. The European Union has not, however, devised an action plan for implementing Convention 108. See http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm.

21 See http://ec.europa.eu/justice/policies/privacy/docs/guide/guide-ukingdom_en.pdf and http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm.

22 See http://trade.ec.europa.eu/doclib/docs/2014/september/tradoc_152806.pdf.

23 Interview with Rosa Barcelo, privacy coordinator, policy coordinator, European Commission, DG CONNECT, July 24, 2012. Also see Shaffer (2000).

24 Regarding Philippine adoption of legislation, based on the EU Data Protection Directive 95/46/EC and accords with APEC policies, see Nepomuceno (2012).

companies must delete data at the request of consumers), language stating that individuals must directly give their consent for data processing, rules requiring that individuals have easier access to their own data and rules obligating companies and organizations to notify individuals of serious data breaches without undue delay. The commission also noted that the new regulation could help businesses by replacing the patchwork of national rules, which, in turn, would lower costs (Gardner 2013; see also European Commission 2014a).

But in 2013 netizens learned that they could trust neither their leaders' nor their service providers' assurances that their personal data was truly safe. Edward Snowden revealed that many of the companies that were certified to meet EU standards by the Safe Harbor Framework were in fact providing personal data to the US government.[25] Many European officials and senior EU leaders responded angrily to these allegations. Within days of the revelations, the EU parliament announced an investigation, the German prosecutor general began looking into espionage charges (*Spiegel Online International* 2013), and German Chancellor Angela Merkel expressed her support for tougher rules governing the privacy of European citizens' data (Traynor 2013; Travis 2013). French President François Hollande flirted with the idea of calling off negotiations for the TTIP (Price 2013) as the French government weighed a tax on cross-border data flows.[26] President Toomas Hendryk Ilves of Estonia argued that the right response to these revelations should be to create a secure "European cloud" with high data protection standards (Charlemagne 2013; Ermert 2013). Some European NGOs and policy makers said that because the US could not be trusted to protect privacy, the EU should not negotiate free flow of data provisions in the TTIP.[27] Although it soon became clear that the United Kingdom, France, Germany, and other European nations also had surveillance programs with extraterritorial reach, the US became the poster child for a lack of respect for privacy and human rights (Bendrath 2014; EDRi 2015).

US and EU policy makers recognized that if they wanted to include provisions for free flow of information in TTIP they had to change how the two trade giants interacted on privacy issues. First, the EU and the US set up a working group on privacy, which provided answers to EU questions about the reach, methods and effectiveness of the NSA's programs (Litt 2013).[28] Second, the US Department of Commerce took steps to show that the Safe Harbor Framework was effective, and that US companies that violated these policies would be punished. The US Federal Trade Commission doubled enforcement actions against 14 companies that claimed to participate in the Safe Harbor Framework but had not renewed their certifications under the program (*Daily News* 2013; *Inside US Trade* 2014c). The United States also reassured businesses that they remained committed to a voluntary — rather than a top-down regulatory — approach to privacy. Third, the European Commission made it clear, repeatedly, that the European Union would ensure its citizens had a very high level of data protection, put individuals in control of their own data, and provide for greater legal and practical certainty for economic operators and public authorities. The European Commission insisted that "data protection in the European Union is a fundamental right" (European Council 2015). Finally, the EU parliament voted in favour of the revised data protection rules in 2014. Parliamentarians agreed that non-European companies would have to fully meet the EU data protection law when offering goods and services to European consumers (European Commission 2014a).

In March 2015, the European Comission's Council of Ministers expressed its support for the regulation and for the establishment of a "one-stop-shop" mechanism to deal with violations of the data protection regulations. They noted, "The one-stop-shop mechanism should only play a role in important cross-border cases and will provide for cooperation and joint-decision making between several data protection authorities concerned....The text clarifies that the jointly agreed decision will be adopted by the data protection authority best placed to deliver the most effective protection from the perspective of the data subject, who must give consent" (European Council 2015). As of January 18, 2016, the European Union's data protection regulation has not been approved. Nonetheless, the European Union states, "We are confident that we will be able to say that the EU remains the global gold standard in the protection of personal data" (European Commission — Justice 2015a; 2015b).

Meanwhile, the two trade giants tried to improve and strengthen the Safe Harbor Framework for the exchange of personal data for commercial purposes, as they also negotiated a framework agreement that would apply to personal data transferred between the European Union and the United States for law enforcement purposes. The European Union has insisted, and US policy makers have reportedly agreed, that the United States will grant EU citizens the same privacy rights as US citizens (*Inside*

25 See www.theguardian.com/world/the-nsa-files; www.theguardian.com/world/2013/dec/29/der-spiegel-nsa-hacking-unit-tao; and www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining.

26 The French Ministries of Finance and Economic Regeneration commissioned a study aimed at fighting tax piracy in cyberspace that was published before the Snowden revelations in January 2013. The tax could serve as a prod to data localization because it is designed to tax companies that use French citizens' information (De Filippi 2013).

27 Internet and Jurisdiction Observatory (2013; 4, fns 71–73); *Daily News* (2014); *Inside US Trade* (2013).

28 On the working group's activities and findings, see Council of the European Union (2013).

US Trade 2014c; European Commission 2013b; European Commission 2014b). However, while the European Union's approach might protect EU citizens and facilitate data exchange between the United States and the European Union, it would do little for citizens of other nations. Nor did it clarify whether the United States would view privacy regulations as legitimate exceptions to the free flow of information or address the broader issue of how to deal with the multiplicity of privacy strategies among US and EU trade partners (Bendrath 2014; Aaronson with Townes 2012).

However, these reforms could not save Safe Harbor and they continue to bedevil the TTIP negotiations. On October 6, 2015, the European Court of Justice released its decision on the Schrems case and found that the "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising" privacy and that the Safe Harbor scheme "enables interference by US public authorities with the fundamental rights of persons" (Wilhelm 2015). The court struck down the Safe Harbor Framework. The European Union also announced that "transfers that are still taking place under the Safe Harbour decision are considered unlawful" (ibid.). It set a deadline of January 30, 2016, for a solution to US-EU data flows (ibid.). As of this writing, data transmissions from the United States and the European Union continue, although such transmissions are essentially illegal. Nonetheless, some 4,000 US companies continue to rely on the Safe Harbor Framework.[29] In December 2015, the US Department of Commerce website noted that despite the court's decision, "the Department of Commerce will continue to administer the Safe Harbor program, including processing submissions for self-certification to the Safe Harbor Framework" (US Department of Commerce 2015).

European policy makers have developed guidance for firms on how companies can comply in the interim as the two develop a new approach to Safe Harbor (European Commission — Justice 2015c). According to EU Justice Minister Vera Jourová (2015), "The U.S. has already committed to stronger oversight by the Department of Commerce, [and to] stronger cooperation between European Data Protection Authorities and the Federal Trade Commission. This will transform the system from a purely self-regulating one to an oversight system that is more responsive as well as pro-active. We are also working with the U.S. to put into place an annual joint review mechanism that will cover all aspects of the functioning of the new framework, including the use of exemptions for law enforcement and national security grounds." Meanwhile, companies are finding ways to meet the demands of their European customers. For example, Microsoft announced that, starting in 2016, it will allow European customers to store cloud data on German servers. Under German law, Microsoft would be unable to access its customers' data unless their customers explicitly authorized it or Deutsche Telekom approved a request to access the data. Microsoft frames it as a way to keep Europeans' data beyond the reach of US intelligence agencies (Segal 2015).

The court's decision provides an opportunity to rethink how the two trade giants deal with this issue. Some argue that those negotiations should form the basis of a new approach to protecting privacy. They want any new approach to include obligations on the necessary oversight of access by public authorities, as well as on transparency, proportionality and redress mechanisms (Sayer 2015). However, there is little evidence that either side was thinking creatively about how to merge the two different approaches.

Privacy is not the only issue troubling the TTIP's digital trade negotiations. The negotiators from the United States and the European Union have also struggled to address issues on online intellectual property protection in the TTIP. NGOs in the European Union and the United States have argued that the potential trade agreement would replicate the hated Anti-Counterfeiting Trade Agreement (ACTA). The United States, Japan and other countries negotiated ACTA to create an international legal framework that could prevent commercial-scale counterfeiting and piracy. To many observers, ACTA focused too much on enforcement and too little on protecting the due process rights of users. The EU parliament rejected ACTA after massive off-line and online protests.[30] In the wake of criticisms that the TTIP would replicate ACTA, the European Commission stated that neither ACTA's provisions on IPR enforcement in the digital environment nor those on criminal sanctions would be included in the negotiations (Cirlig 2014; European Commission 2013a). However, many NGOs were not reassured. They argued that IPR should not be included in the TTIP; they noted that the European Union is currently updating its approach to copyright to fit the digital age and that adding these issues to the TTIP would pre-empt that process (EDRi 2015).

With the completion of the TPP, European policy makers are under greater pressure to finalize TTIP e-commerce negotiations. The TPP provides a model as to how they could draft shared provisions, but it is probably not the best template to meet the needs and values of the United States and the EU 28. However, if the two trade giants cannot find a way forward, they will be less likely to find common ground internationally or to ensure that Western norms become the standards for global information flows.

29 See http://safeharbor.export.gov/list.aspx for a searchable list.

30 Australia, Canada, Japan, Korea, Morocco, New Zealand, Singapore and the United States signed ACTA on October 1, 2011. The EU Parliament rejected the agreement. See https://ustr.gov/acta and www.eff.org/issues/acta.

TiSA

As noted above, although the 162 member states of the WTO apply WTO rules to information flows, these rules have not kept pace with new technologies. In 1995, the signatories of the GATS agreed to negotiate new rules to govern internationally traded services, including banking, telecommunications, computer, tourism and professional services. They also agreed that their negotiations would be "technology neutral," in recognition that no one could predict how technologies would change the economics of providing such services. Finally, they committed to ensuring that the service suppliers of other members could use public telecommunications systems to provide cross-border information flows and to access data stored or contained in databases in the territory of another signatory nation (Holleyman 2015). In 2011, some 50 members of the WTO (the 28 countries of the EU and 23 others) agreed to negotiate an agreement about trade in services — TiSA — that would include new rules on e-commerce. According to the European Union, the WTO members negotiating TiSA hope that other WTO members will join in the talks or the agreement when it is signed and that then TiSA "could be turned into a broader WTO agreement."[31] The negotiations officially began in 2013. These negotiating nations represent 70 percent of global services traded (*Inside US Trade* 2011b; Australian Government 2014). The negotiators have focused on electronic authentication, trust services, cross-border information flows, localization requirements, privacy protection and cloud computing (WTO 2015b). The United States and the European Union have been the leading demandeurs of these provisions.[32] However, as the negotiations proceeded, participants disagreed about the relationship between data flows, data protectionism and privacy. The European Union, Australia and other governments wanted data transfers to be subject to rules consistent with international agreements and in no way to alter domestic laws (*Inside US Trade* 2014b; *Inside US Trade* 2014d; Third World Network 2015).

In April 2014, the international transparency organization WikiLeaks leaked the financial services chapter. It contains language calling for the free flow of data and vague wording on data protection. One clause supposedly states, "No Party shall take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means, into and out of its territory, for data processing...Nothing in this paragraph restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of this Agreement" (WikiLeaks 2014).

WikiLeaks also leaked the e-commerce chapter in June 2015. It is undated and so it is unknown whether the version is relatively current. The leak has pages of bracketed text where nations propose alternative language. However, the leaked chapter reveals that nations are trying to set rules governing the free flow of information with clear exceptions to meet important domestic regulatory objectives. The leaked version shows that participating governments for the most part accept the notion that data should flow freely across borders, with a few exceptions. It also shows that many participating nations have expressed concerns or proposed alternative language about the need to protect IPR, privacy, consumers, cultural diversity and fiscal data. The leaked draft also has language stating that no party shall give priority or preferential treatment to domestic suppliers; language banning customs duties on cross-border information flows; language banning data localization or server localization requirements; and even language about international cooperation on cross-border information regulatory issues. Several governments proposed wording that governments should not be precluded from taking action to promote their security interests. Again, it is important to note that these provisions might not be accurate or up to date.[33]

Some analysts have misrepresented some of the texts, perhaps because the documents are complicated or because these analysts misunderstand how trade agreements work. For example, WikiLeaks describes the e-commerce chapter as designed to create "an international legal regime which aims to deregulate and privatize the supply of services — which account for the majority of the economy across TiSA." However, the texts say nothing about privatizing and deregulating the supply of services; instead, they are designed to open up services markets (which are often highly protected monopolies) to foreign providers. Many services (for example, postal, water or banking services) are quasi-public goods; hence, many governments have long-standing monopolies or oligopolies providing these services or closely regulate the providers of such services. Consumers of such quasi-public goods may well benefit from greater competition if such competition is regulated effectively. However, it is not easy to effectively regulate business, and it is even harder to regulate rapidly changing sectors such as digital technologies. The leaked text on "domestic regulation" states that "parties recognize the right to regulate, and to introduce new regulations, on the supply of services within their territories in order to meet national policy objectives." In addition, the leaked document shows that several states are calling for clearer language on the right to regulate in the public interest. Thus, it looks like the negotiating parties have little

31 See ec.europa.eu/trade/policy/in-focus/tisa/ and ec.europa.eu/trade/policy/in-focus/tisa/questions-and-answers/.

32 The EU negotiating mandate is at http://data.consilium.europa.eu/doc/document/ST-6891-2013-ADD-1-DCL-1/en/pdf; for the EU view of TiSA, see http://trade.ec.europa.eu/doclib/press/index.cfm?id=1273.

33 February 2014 bracketed draft of TiSA (e-commerce chapter). WikiLeaks calls it 2014 but the document is dated 2013. See https://wikileaks.org/TiSA/ecommerce/TiSA%20Annex%20on%20Electronic%20Commerce.pdf.

interest in deregulation per se, although they do want to find common approaches to regulation.[34]

TiSA demonstrates that governments have significantly different opinions about their appropriate roles in regulating the Internet and in providing online services, especially services with a public goods nature such as education. Meanwhile, critics of the e-commerce chapter are understandably concerned that TiSA could undermine rather than support the open, international nature of the Internet. These critics have focused on the substance of the agreement as well as on the strategy for negotiation. For example, staff at the Canadian Internet Policy and Public Interest Clinic state that the agreement does not sufficiently ensure net neutrality, privacy and freedom of expression. They argue that governments can use data localization to preserve privacy and freedom of expression (as in protecting citizens' right to be forgotten). Moreover, they point out that the agreement is being negotiated in secret and that there is "minimal to no input from public interest and civil society groups" (Israel n.d., 1; see also James 2015; Kelsey and Kilic 2014). Hence, because trade negotiations are between governments, they argue that such negotiations are illegitimate because groups representing netizen interests are not directly involved as they are in other venues for Internet governance.

As noted earlier, the European Commission has heard its citizens' concerns about data protection and the right to be forgotten, especially in the wake of ACTA and Edward Snowden's revelations.[35] EU negotiators have tried to finesse the EU and US approaches in TiSA. In December 2014, the EU's trade spokesperson noted that only one of the participants had "proposed two provisions that should ensure free data flows and prohibit requirements to store data locally" (quoted in Ermert 2014). The commission also underlined that "such provisions should be without prejudice to data protection requirements" (ibid.). Hence, the commission recognizes the need for clarity, noting privacy is a general "exception" in GATS. The "EU has asked for further clarification on these proposals and made it very clear that it cannot and will not agree to any language that could potentially prevent the EU from enforcing its own data protection standards" (ibid.). The spokesperson also noted that the GATS data protection standards, which include an exemption for future data protection measures "not inconsistent with the provisions of this Agreement," have thus far, according to the commission, "never led to any WTO country, either formally or informally, challenging EU rules on data protection [or any other country's system of data protection]" (ibid.). But the commission acknowledged that it will have "to analyse very carefully how any data transfer obligations in TiSA interact with that existing exception" (ibid.).

As with the TPP, the leaked draft of the TiSA e-commerce chapter includes language on spam, in article 5. The negotiators also included language stating that no party may require the transfer of or access to source code, again similar to the TPP's. And finally, like the TPP, the draft text does not discuss cyber security or malware explicitly. Although the negotiators are making progress, it looks like TiSA will not be completed in the next few years.

DIGITAL PROTECTIONISM: WHY, WHAT AND HOW

The United States has conflicting objectives regarding its many actions and policies concerning the Internet. On the one hand, it wants to encourage a vibrant global Internet with few barriers to entry. On the other hand, it wants to preserve the country's Internet dominance, which is clearly declining as more firms from other nations develop digital prowess and as users (the key demandeurs of digital goods and services) come from populous developing countries such as Indonesia and China. Not surprisingly, more than any other nation, the United States has made fighting digital protectionism a key element of its trade and national security strategy. In fact, in its 2015 national security strategy, the White House argued that "the United States has a special responsibility to lead a networked world. Prosperity and security increasingly depend on an open, interoperable, secure, and reliable Internet…. Jobs will also grow as we expand our work with trading partners to eliminate barriers to the full deployment of US innovation in the digital space" (EOP 2015, 12, 15). The United States closely monitors practices by other governments that it calls protectionist and generally uses naming and shaming to get other governments to change their behaviour. But other governments do not appear convinced that their actions are "protectionist" and that such practices will affect the vitality and stability of the Internet as a whole.

In 2014, at the behest of Congress, the USITC (2014) examined global use of trade-distorting strategies and found that 49 nations have adopted "digital protectionist" policies such as censorship, filtering, localization measures and regulations to protect privacy or ensure cyber stability. Countries adopt such policies for a wide range of reasons — for example, to nurture local Internet producers, protect their citizens' data, monitor their citizens' data or obtain economic advantage. Some states have also adopted local content requirements that stipulate that the products a foreign enterprise sells into a country's market (for example, automobiles, wind turbines, telecommunications equipment, etc.) must include a certain percentage of

34 I am grateful to Ted Alden (2015) of the Council on Foreign Relations for reminding me of this point. See also WikiLeaks (2015, article 4).

35 As an example, two-thirds of the respondents (67 percent) of a March 2015 Eurobarometer survey of 28,000 EU citizens said that they are worried about having no control over the information they provide online (European Commission — Justice 2015a).

domestically produced components. These officials are also responding to online theft of intellectual property; the growth of sophisticated malware; and the challenges involved in regulating the flow, storage and analysis of data. They have adopted rules, laws or policies that limit the storage, movement or processing of data to specific geographies and jurisdictions, or that limit the companies that can manage data, based upon the company's nation of incorporation or principal sites of operations and management (USITC 2013; USITC 2014; Chander and Le 2014).

Meanwhile, many governments see data localization as a strategy to protect their citizens from harm. Policy makers from these nations argue that by keeping data stored within national jurisdictions, or by prohibiting data from travelling through the territory or infrastructure of "untrustworthy" nations or technology companies, data will be better protected (Castro and McQuinn 2015; Hill 2014). Moreover, some governments use data localization policies as a more efficient means of ensuring that they can easily obtain information about potential criminal activities, to avoid having to go through cumbersome legal processes. These governments complain that the process by which they request data from US firms (the rules of which are generally negotiated between the United States and foreign governments and then ratified in a mutual legal assistance treaty) is slow and inconvenient, and that American firms and the US Justice Department are too often uncooperative or too respectful of local mores that might conflict with US free speech imperatives. As Hill (2014, 26) notes, "Data localization, for frustrated and impatient law enforcement agencies and their political allies, looks like a straightforward mechanism to free themselves from some of this bothersome dependence on Americans." Hence, it might be that governments using data localization are attempting to reduce America's Internet dominance or to ignore America's burdensome due process requirements.

Whatever other governments' reasons for adopting such strategies, US arguments against digital protectionism are at times inconsistent and unconvincing. For example, in its report on foreign trade barriers, the USTR (2013) argued that British Columbia's and Nova Scotia's privacy laws discriminate against US suppliers because they require that personal information be stored and accessed only in Canada (*Inside US Trade* 2012; USTR 2014a). In its 2012 report, the US government also cited Australia's approach to privacy, noting its unwillingness to use US companies for hosting, due to concerns about privacy violations (USTR 2012). Further, the United States complained about Japan's uneven, and Vietnam's unclear, approaches to privacy (ibid., 216). Ironically, the United States has argued that China's failure to enforce its privacy laws stifles e-commerce (ibid., 96). It seems the United States both criticizes other governments for failing to develop clear or adequate approaches to enforcing privacy *and* cites privacy as a barrier to trade. Moreover, since the Clinton administration, the United States has argued that privacy protections maintain trust in the Internet and that such protections are essential to creating an effective enabling environment for digital technologies. Hence, it is surprising to see the United States describe too much privacy and inadequate privacy regulations as "protectionist."

By 2014, the United States had a broader argument: that governments that failed to make an appropriate regulatory context for the free flow of information were effectively distorting trade. It chided China, South Africa,Thailand and the UAE for unclear Internet rules. It criticized South Africa for failing to effectively enforce its laws online; named Vietnam and Turkey for overreaching bans on Internet content; and condemned France for its proposals to tax Internet activity.[36] The USITC (2014, 1, 77–79) noted that digitally intensive firms identified Nigeria, Algeria and China as having high barriers to digital trade. But the United States also adopts protectionist strategies (relying on domestic rather than equally competent and affordable foreign producers) when they perceive that the Internet could be vulnerable to hacking or cyber theft (Nakashima 2014).

In 2015, the USTR found ever-expanding examples of digital protectionism. In its annual trade estimate report, it noted that Brazil provides tax reductions and exemptions on many domestically produced information and communications technology (ICT) and digital goods that qualify for status under its PPB (Processo Productivo Básico, or Basic Production Process). The PPB provides benefits to producers for creating goods that incorporate a certain minimum amount of local content. The United States named and shamed the Czech Republic for its failure to crack down on "cyber lockers" that feature pirated material for download and streaming, and criticized countries such as Estonia for having "too consumer-oriented IPR" and inadequate investment in online policing; it had similar complaints about Japan (USTR 2015c, 47, 137). The USTR also warned that procurement policies could be viewed as hidden forms of protectionism, noting that the Canadian government is consolidating information technology services across 63 Canadian federal government email systems under a single platform: "The request for proposals for this project invokes national security as a basis for prohibiting the contracted company from allowing data to go outside of Canada. This policy could preclude US 'cloud' computing providers from participating in the procurement process" (ibid., 69). The USTR, however, did not acknowledge that the United States also limits cloud-related procurement for national security reasons.

36 USTR (2014b): on China, see 77; on France, 128; on South Africa, 318; on Thailand, 330; on Turkey, 347; on the UAE, 358; and on Vietnam, 374.

While executives surveyed by the USITC described Algeria, China and Nigeria as the countries where they faced the highest barriers to digital trade, policy makers are most concerned about China (USITC 2014, 24). China has the world's largest Internet market, with 632 million users, and it will continue to grow rapidly (McKinsey Global Institute 2014). These officials state that China uses a wide variety of protectionist strategies, including discriminatory regulatory processes, informal bans on entry and expansion, overly burdensome licensing and operating requirements and other means to frustrate efforts of US suppliers of banking, insurance, telecommunications and Internet-related services such as electronic payment services. China's Internet regulatory regime is restrictive and non-transparent, affecting a broad range of commercial services activities conducted via the Internet (USTR 2015c, 70–72, 77–79). In April 2015, the Chinese government announced that it will suspend the implementation of new regulations requiring foreign companies that supply ICT to China's financial institutions to turn over sensitive commercial information about their equipment. China said it plans to revise those rules after getting feedback from interested parties (*Inside US Trade* 2015).

US policy makers are perhaps most concerned about online IPR protection as a trade barrier because it is so crucial to economic growth. Researchers have found that many governments use the Internet to steal trade secrets from key US firms, including defence suppliers and producers of dual-use technologies. Then Director of the NSA General Keith Alexander termed such theft "the greatest transfer of wealth in history" (IP Commission 2013). According to the US Defense Science Board (2013), other nations use the Internet to scour, penetrate and steal information on critical technologies, including drones, robotics and communications and surveillance technologies. They noted that China has reverse-engineered and reproduced some of the United States' most modern rifles, cannons and guns. US policy makers stress that US allies such as France, Israel and Korea also engage in such cyber theft. CNN reported that the Federal Bureau of Investigation found that half of 165 private companies surveyed claimed to be victims of economic espionage or theft of trade secrets, and that 95 percent of those attempts originated from individuals associated with the Chinese government. US policy makers are most concerned about cyber theft by China (Bruer 2015; Defense Science Board 2013; IP Commission 2013).

The United States is particularly vulnerable to this theft. Because defence is a public good, some governments have stakes in or partial ownership of firms making critical technologies. In the United States, however, private companies develop US-critical technologies and these private companies might not have adequate cyber defences. While the Defense Science Board (2013) recommended that the United States use deterrence to stop cyber theft, trade analysts have suggested that the government initiate a trade dispute or use naming and shaming against government perpetrators. In fact, the US government has long relied upon a coercion-based enforcement strategy in its trade agreements. However, this strategy has failed to secure strong IPR protection among US trade partners (Sell 2013).

US arguments about cyber theft ring hollow in the face of recent revelations about US signals intelligence practices. The US government has publicly defended its extensive global surveillance program and stressed that it does not use surveillance for commercial theft. Alas, US assertions are not completely credible. In the summer of 2015, WikiLeaks provided evidence that the United States spied on Japanese companies and policy makers related to trade negotiations; President Obama called Japanese Prime Minister Abe to apologize. In 2015 as well, Chancellor Angela Merkel's office said it found that the United States used Germany's top spy agency on European corporate targets.[37] The United States still insists it is not stealing corporate property and giving it to US companies.However, citizens and government officials in the United States and abroad may find it hard to distinguish between cyber monitoring to prevent crime and terrorism and cyber probing to steal technologies (Aaronson 2015). Nonetheless, the leaders of the 20 richest nations (the Group of Twenty) announced that they had agreed not to engage in cyber espionage against each other in November 2015 (Nakashima 2015). Clearly, the United States had convinced them that such language could be used to "catch" nations violating such commitments.

In 2015, US and foreign companies debated the appropriate role of the USITC in examining and addressing issues of digital protectionism. Some companies wanted to empower the agency to block cross-border flows of allegedly pirated or stolen information. Under section 337 of the Tariff Act of 1930 (19 U.S.C. § 1337), the USITC is required to conduct investigations into allegations of certain unfair practices in import trade, such as the infringement of certain statutory IPR and other forms of unfair competition. A company called Clear Correct in Pakistan transmitted digital models for braces in Pakistan and printed the braces in 3D printers in Texas. After another company challenged the digital models as a violation of its patents, the USITC decided that Clear Correct was violating US patents, an unfair

37 In November 2015, media whistleblower WikiLeaks published documents it says show the United States spied on 35 companies, government ministries and individuals in Japan. WikiLeaks said the intercepts related to topics such as US-Japan relations, trade negotiations and climate change strategy and that the surveillance dates back as far as 2006, the first term of Prime Minister Abe. For the leaked documents, see https://wikileaks.org/nsa-japan/. The targets included several Japanese companies: https://wikileaks.org/nsa-japan/selectors.html. On Germany, see Donahue (2015) and www.spiegel.de/politik/deutschland/ueberwachung-neue-spionageaffaere-erschuettert-bnd-a-1030191.html; on Brazil, see https://wikileaks.org/nsa-brazil/.

trade practice. Accordingly, the USITC could potentially forbid the company from transmitting data into the United States until the dispute was resolved (citing section 337). However, its ruling was quite narrow. The USITC weighed whether the digital data sets were "articles" within the meaning of section 337, but it did not weigh whether the digital transmission was an importation. Also, the USITC stressed that the circumstances under which it issued the cease-and-desist order in this investigation were unique.

But some US companies saw in the USITC's decision an opportunity to prod it to regulate "digital trade" as a means of protecting IPR. The Motion Picture Association considered asking the USITC to order Internet service providers to block traffic from foreign pirate websites, although its law firm, Jenner and Block, warned the association that a site-blocking order might not be technologically feasible. Meanwhile, companies and groups such as Google, the Internet Association, Public Knowledge and the EFF challenged the ruling in the US Federal Circuit Court and asked the USITC to reconsider its ruling that pure data transmissions are within the ambit of the commission's powers (Brandom 2015; Jenner and Block 2014; Fish and Richardson PC 2015; Duan 2014; Public Knowledge and EFF 2015).

On November 9, the Appeals Court found that the USITC had no authority under existing legislation to block the importation of electronic data. In a two-to-one decision the court ruled that electronically transmitted digital data does not fit Congress's definition of "article" (Trujillo 2015). While the decision is positive for an open Internet, it revealed that US officials must figure out how and where (what agency) to evaluate allegations of digital protectionism.

US firms and policy makers are not alone in finding digital protectionism. Canadian firms are also calling for global rules to regulate data protectionism (McKenna 2013). A 2011 study by the Conference Board of Canada found that Canada faced a multitude of barriers to digital trade, including its own investment barriers (Goldfarb 2011). The European Union is also increasingly concerned about trade barriers to its firms. In its most recent report on global trade barriers, it found Russia's local server requirements could be trade distorting. It also noted that "China continues to consider that only Chinese-developed information security technology is regarded as 'safe' and applies a concept of 'national security' far beyond normal international practice. This acts as a tremendous barrier for foreign companies competing for commercial applications in the IT sector. Furthermore, foreign companies continue to be blocked from participating in security-related standardization bodies" (European Commission 2015b, 6, 8).

While examples of digital protection might be easy to find, they are hard to measure. Because one must use models to estimate the size or effects of digital protectionism, the estimates are controversial. For example, a 2013 report by the European Centre for International Political Economy (ECIPE) found that EU GDP could be reduced by .08 percent to 1.3 percent and EU imports decreased by 11 percent if the European Union adopted overly rigorous data protection rules (ECIPE Project Group 2013). In September 2014, the USITC estimated that "removing foreign barriers to digital trade would increase US employment in digitally intensive industries which, in turn, would benefit the US economy as a whole.… The removal of barriers would trigger an estimated 0.1 to 0.3 percent increase (a $16.7–$41.4 billion increase at 2011 levels) in US GDP, a 0.7–1.4 percent increase in US real wages, and a 0.0 to 0.3 percent increase in US total employment" (USITC 2014, 22). Digitally intensive firms surveyed estimated that their sales abroad would be positively affected by the removal of foreign barriers. Moreover, the USITC noted that large firms in the wholesale trade and the digital communications sectors could see estimated increased sales of between five and 15 percent if these barriers were effectively removed or reduced (ibid.). However, these estimates rely on a wide range of assumptions about the digital economy and the economy in general.

FINDINGS: WHY SHOULD WE CARE ABOUT THE DIGITAL TRADE IMBALANCE?

For many years, the United States has sought to use trade agreements and policies to address cross-border Internet issues. Other countries are less willing to use trade policies and agreements to address information flows unless their concerns about privacy, surveillance and domestic regulation of the Internet are effectively addressed. Consequently, there is still an imbalance between US enthusiasm for digital trade rules and the responses of other countries. Nonetheless, the TPP has shown that a diverse set of nations can find common ground on rules to both govern digital trade and limit digital protectionism. The section below delineates this chapter's key findings related to digital trade and Internet governance.

The Internet has empowered more people to participate in trade. As a result, digital trade, which offers important benefits to society, is booming. More trade will likely promote more competition in the digital economy, which over time will likely provide producers and consumers with more and better services at lower prices. However, this competition cannot occur when governments use local laws and regulations to undermine foreign competitors. Most officials recognize that the best place to address trade-distorting policies is in trade agreements, which have a positive record in establishing trust and the rule of law among market actors.

Internet demographics will have important implications for trade policies and agreements. The largest and fastest-growing Internet markets are in highly populated developing and middle-income countries such as India, Brazil, China and Indonesia, where absolute numbers of users are high but the percentage of penetration is still relatively low. Internet firms from Canada, the United States and the European Union operating in these markets increasingly find contradictions between the norms that govern their business practices and the requirements of the jurisdictions where they now operate. Trade agreements could help clarify how governments regulate cross-border information flows and how firms sending, processing or using such flows should behave.

Nonetheless, trade agreements might not be the best venue for governing cross-border information flows. Trade agreements regulate the behaviour of states, not of individuals or firms; thus, companies and citizens have no direct way to influence trade agreement bodies. Moreover, trade agreements are negotiated in secret by governments; these negotiations move slowly and the public is not directly involved. In contrast, the Internet is governed in a more ad hoc, bottom-up and transparent manner. Stakeholders from civil society, business, government, academia and national and international organizations make Internet governance rules in a timely, open and collaborative manner without a central governing body. Many Internet activists would not take kindly to the WTO's being the key venue for the regulation of cross-border information flows, given its secretive, slow, top-down and closed processes. Moreover, many Internet issues that involve information flows, such as privacy or the security of data, are not market-access issues — although they are regulatory issues, and finding common ground on cross-border regulations has become an important rationale for twenty-first-century trade agreements. Finally, trade agreements are not explicitly designed to facilitate interoperability or universal standards, which is how Internet policies have traditionally been designed.

Trade agreements are sometimes perceived as favouring US interests and actors. During most of the twentieth century, the United States was the dominant market actor and the world's largest market. The WTO's GATS and its predecessor agreement, the GATT, as well as many other trade agreements, reflect US norms (such as transparency and due process), as well as US priorities (such as protecting IPR). However, other market actors, such as China or Russia, might view these priorities and language as skewed to meet US needs and not the needs of other countries. Government officials probably do not want to use trade policy to perpetuate or further US digital dominance. If the United States and other proponents of using trade agreements to regulate cross-border information flows want to change these perceptions, they must reframe the rationale for such language. Rather than focusing solely on the economic benefits of reducing barriers to digital trade, proponents should also explain how rules designed to foster cross-border information flows will build trust and yield benefits to human welfare and the Internet as a whole.

If policy makers want to use trade agreements to govern information flows, they must include language that ensures that governments also work to meet their human rights obligations. As information flows across borders, it can simultaneously enhance and undermine specific human rights. As an example, while an individual might benefit from access to information, that same information might also undermine privacy or reduce the individual's freedom of expression or right to organize. Further, while government officials want to protect the IPR of creators, in so doing they might, without intent, undermine access to information. The human rights effects of information flows are complex and constantly changing, and governments are just learning to protect and respect such rights online. Human rights are a key element of the rule of law online and thus must be included in international efforts to govern the Internet. However, the WTO agreements (and most trade agreements) do not contain language that links government obligations to protect, respect and remedy violations of human rights to government obligations for trade. Trade agreements such as the WTO have no authority to prod member states to provide an enabling regulatory context for the protection of these rights. Accordingly, should they choose to include binding rules governing cross-border information flows in trade agreements, policy makers should also include language clarifying the relationship of trade obligations to human rights obligations delineated in other international agreements and treaties. Moreover, policy makers should use these agreements to challenge the trade distortions of filtering and censorship.

Trade negotiations, however, could have positive implications for global Internet governance. Should negotiations under TiSA or other trade agreements succeed, they could provide an impetus to policy makers to develop globally coordinated policies on issues ranging from privacy to cyber security. A system of shared rules builds greater trust and could reduce costs for firms and individuals who must deal with different rules about how and where data can be collected and stored; when and under what conditions data can be transferred to other organizations; and what types of user authorizations are needed for collection, storage and transfer.

Progress on trade negotiations might reduce barriers to cross-border information flows and prod governments such as the United States to develop greater coherence between their trade objectives and other international policies and practices. As noted above, many countries have responded to US economic Internet dominance (or to revelations of NSA monitoring of the Internet) with policies that restrict the free flow of information and often

appear protectionist. However, protectionism might be in the eyes of the beholder. Until policy makers devise a set of rules governing information flows, and clear exceptions to those rules, countries will continue to argue as to the trade-distorting effects and legitimacy of such policies. In the end, both the Internet and netizens will suffer because, without clear and consistent rules, netizens could experience a more fragmented Internet. Hence, if policy makers choose to use trade agreements to regulate cross-border trade, they must find ways to balance trade and human rights obligations and, in so doing, make a broader case that such rules enhance human welfare.

POLICY RATIONALE AND RECOMMENDATIONS

The following three recommendations are designed to help policy makers encourage the free flow of information, preserve the open Internet and enhance human welfare. A policy rationale precedes each recommendation.

Policy Rationale One

Trade policy makers should encourage interoperability and the rule of law. Trade agreements encourage the rule of law through shared rules such as those on transparency, due process and public comment in trade policy making.

Recommendation One

Governments negotiating binding provisions to encourage cross-border information flows should also include language related to the regulatory context in which the Internet functions (for example, provisions to encourage interoperability, free expression, fair use, the rule of law and due process). By including such language, policy makers can argue that these rules enhance human welfare and Internet operability. They will also be better positioned to argue that trade agreements are appropriate venues for mediating tensions between national laws and cross-border information flows.

Policy Rationale Two

Trade policy makers need to better understand and measure digital trade and digital protectionism.

Recommendation Two

WTO member states should ask the WTO Secretariat to examine whether domestic policies that restrict information (short of exceptions for national security and public morals) constitute barriers to cross-border information flows that could be challenged in a trade dispute. Further, policy makers should develop strategies to quantify how such information restrictions might affect trade flows. Finally, they should test these provisions in a trade dispute.

Policy Rationale Three

Trade policy makers can do a better job linking digital trade and digital rights.

Recommendation Three

Although many countries have taken steps to advance digital rights globally, these governments have not figured out how to coordinate policies to promote cross-border information flows with policies safeguarding national security and digital rights. Nor have these governments developed a clear and compelling argument as to how these agreements will benefit netizens. They should connect these arguments to build public support among their public and to convince citizens and policy makers from other nations (including those that heavily censor the Internet) to see the benefits of digital trade agreements.

WORKS CITED

Aaronson, Susan A. 2015. "Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security." *World Trade Review*, April. http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid= 9644770&fileId=S1474745615000014.

Aaronson, Susan Ariel and M. Rodwan Abouharb. 2011. "Unexpected Bedfellows: The GATT, the WTO and Some Democratic Rights." *International Studies Quarterly* 55 (2): 379–408.

Aaronson, Susan Ariel and Michael Owen Moore. 2013. "A Trade Policy for the Millennials." *Baltimore Sun*, December 13. http://articles.baltimoresun.com/2013-12-17/news/bs-ed-trade-policy-20131217_1_trade-policy-trade-agreement-trade-liberalization.

Aaronson, Susan A. with M. Townes. 2012. "Can Trade Policy Set Information Free: Trade Agreements, Internet Governance and Internet Freedom (Policy Brief)." www.gwu.edu/~iiep/governance/taig/CanTradePolicySetInformationFreeFINAL.pdf.

Alden, Edward. 2015. "WikiLeaks and Trade: A Healthy Dose of Sunshine." *Renewing America* (blog), June 3. http://blogs.cfr.org/renewing-america/2015/06/03/wikileaks-and-trade-a-healthy-dose-of-sunshine/.

Alliance for Global Business. 1999. "Action Plan for Electronic Commerce." www.iccwbo.org/Data Policies/1999/A-Global-Action-Plan-for-Electronic-Commerce/.

Australian Government. 2014. "Trade in Services Agreement (TiSA)." Department of Foreign Affairs and Trade. Cached webpage, July 18. http://dfat.gov.au/trade/agreements/trade-in-services-agreement/Pages/trade-in-services-agreement.aspx.

———. 2015. "Trans-Pacific Partnership Agreement. Outcomes: Trade in the Digital Age." Fact sheet, October 12. https://dfat.gov.au/trade/agreements/tpp/Documents/outcomes-trade-digital-age.PDF.

Baker, Stewart. 2015. "Cybersecurity and the TPP." *The Volokh Conspiracy* (blog), November 6. www.washingtonpost.com/news/volokh-conspiracy/wp/2015/11/06/cybersecurity-and-the-tpp/.

BBC. 2014. "Trust in the Internet 'Now Missing.'" BBC News, May 14. www.bbc.com/news/technology-26512369.

Bendrath, Ralf. 2014. "Trading Away Privacy." *Eurozine*, December 14. www.eurozine.com/articles/2014-12-19-bendrath-en.html.

Brandom, Russell. 2015. "The MPAA Has a New Plan to Stop Copyright Violations at the Border." *The Verge*, January 2. www.theverge.com/2015/1/2/7481409/the-mpaa-has-a-new-plan-to-stop-copyright-violations-at-the-border.

Bridges. 2014. "Row Over Internet Domain Names Sparks Governance Trade Questions." *Bridges* 18 (23), June 26. www.ictsd.org/bridges-news/bridges/news/row-over-internet-domain-names-sparks-governance-trade-questions.

Bruer, Wesley. 2015. "FBI Sees Chinese Involvement Amid Sharp Rise in Economic Espionage Cases." CNN, July 24. www.cnn.com/2015/07/24/politics/fbi-economic-espionage/.

Bryson, Jay A. and Erik Nelson. 2015. "TPP Agreement: More Than Initially Meets the Eye." October 7. www08.wellsfargomedia.com/assets/pdf/commercial/insights/economics/international-reports/global-tpp-20151007.pdf.

BSA. 2015. "Powering the Digital Economy: A Trade Agenda to Drive Growth." Washington, DC. http://digitaltrade.bsa.org/pdfs/DTA_study_en.pdf.

Burri, M. 2013. "Should There be New Multilateral Rules for Digital Trade? Think Piece for the E15 Expert Group on Trade and Innovation." SSRN. September. http://ssrn.com/abstract=2344629.

———. Forthcoming. "Designing Future-Oriented Multilateral Rules for Digital Trade." In *Edward Elgar Research Handbook on Trade in Services*, edited by Pierre Sauvé and Martin Roy. Cheltenham, Gloucestershire, England: Edward Elgar.

Business Roundtable. 2012. "Promoting Economic Growth Through Smart Global Information Technology Policy: The Growing Threat of Local Data Server Requirements." Business Roundtable, June. http://businessroundtable.org/sites/default/files/legacy/uploads/studies-reports/downloads/Global_IT_Policy_Paper_final.pdf

Büthe, T. and H. V. Milner. 2008. "The Politics of Foreign Direct Investment into Developing Countries: Increasing FDI through International Trade Agreements?" *American Journal of Political Science* 52: 741–62.

Castro, Daniel and Robert Atkinson. 2014. "Beyond Internet Universalism: A Framework for Addressing Cross-border Internet Policy." Information Technology and Innovation Foundation, September. Washington, DC. www2.itif.org/2014-crossborder-internet-policy.pdf.

Castro, Daniel and Alan McQuinn. 2015. "Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness." Information Technology and Innovation Foundation, June 9. Washington, DC. https://itif.org/publications/2015/06/09/beyond-usa-freedom-act-how-us-surveillance-still-subverts-us-competitiveness.

Chakravorti, B. Christopher Tunnard and Ravi Shankar Chaturvedi. 2015. "Where the Digital Economy Is Moving the Fastest." *Harvard Business Review*, February. https://hbr.org/2015/02/where-the-digital-economy-is-moving-the-fastest.

Chander, A. and U. P. Le. 2014. "Breaking the Web: Data Localization vs. the Global Internet." UC Davis Legal Studies Research Paper 378. http://dx.doi.org/10.2139/ssrn.2407858.

Charlemagne. 2013. "Reaching for the Clouds: Europe wants tougher data-privacy rules to deter American snooping." *The Economist*, July 20. www.economist.com/news/europe/21582015-europe-wants-tougher-data-privacy-rules-deter-american-snooping-reaching-clouds.

Cirlig, Carmen-Cristina for the European Parliament. 2014. "Overcoming Transatlantic Differences on Intellectual Property: IPR and the TTIP Negotiations." July. www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140760/LDM_BRI%282014%29140760_REV1_EN.pdf.

Council of Europe. 2014. "The Rule of Law on the Internet and in the Wider Digital World." Issue Paper 2014/1. December 8. https://wcd.coe.int/ViewDoc.jsp?id=2268589.

Council of the European Union. 2013. "Note: Report on the Findings by the EU Co-Chairs of the Ad Hoc EU-US Working Group on Data Protection." November 27. http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2016987%202013%20INIT.

Daigle, Lesley. 2015. *On the Nature of the Internet*. Global Commission on Internet Governance Paper Series No. 7. Waterloo, ON: CIGI. www.cigionline.org/publications/nature-of-internet.

Daily News. 2013. "US will push for Rules Governing Data Flows in Trans-Atlantic Deal." World Trade Online, July 13. http://insidetrade.com/search/site/US%20will%20push%20for%20Rules%20Governing%20Data%20Flows%20in%20Trans-Atlantic%20Deal.

———. 2014. "Publicly Funded German NGO Is Key Player In TTIP Opposition Movement." World Trade Online, July 18. http://insidetrade.com/daily-news/publicly-funded-german-ngo-key-player-ttip-opposition-movement.

Defense Science Board. 2013. "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat." United States Department of Defense, January. www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

De Filippi, Primavera. 2013. "Taxing the Cloud: Introducing a New Taxation System on Data Collection?" *Internet Policy Review* 2 (2): 1–7. http://policyreview.info/node/124/pdf.

Doctorow, Corey. 2015. "Leaked (final?) TPP Intellectual Property chapter spells doom for free speech online." Boing Boing, October 9. http://boingboing.net/2015/10/09/leaked-final-tpp-intellectu.html.

Donahue, Patrick. 2015. "German Spy Accusations Resurface as Merkel Cites 'Deficiencies.'" Bloomberg, April 23. www.bloomberg.com/news/articles/2015-04-23/german-spy-accusations-resurface-as-merkel-cites-deficiencies-.

Duan, Charles. 2014. In the United States Court of Appeals for the Federal Circuit Appeal from the United States International Trade Commission, Inv. No. 337-TA-833. Brief of Amici Curiae, Public Knowledge and the Electronic Frontier Foundation in Support of Appellants. 2014-1527, October 14. www.publicknowledge.org/assets/uploads/documents/brief-clearcorrect.pdf.

Easterly, William and Steven Pennings. 2013. "How Much Do Leaders Explain Growth? An Exercise in Growth Accounting." November. www.nyudri.org/wp-content/uploads/2013/10/Leaders-And-Growth.pdf.

eBay Inc. 2014. "Commerce 3.0 for Development: The Promise of the Global Empowerment Network." www.ebaymainstreet.com/sites/default/files/eBay_Commerce-3-for-Development.pdf.

ECIPE Project Group. 2013. "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, moving Commerce." ECIPE, March. www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.

Edgerton, Anna and Jordan Robertson. 2014. "Brazil-to-Portugal Cable Shapes Up as Anti-NSA Case Study." *Bloomberg*, October 30. www.bloomberg.com/news/2014-10-30/brazil-to-portugal-cable-shapes-up-as-anti-nsa-case-study.html.

EDRi. 2015. "TTIP and Digital Rights." The EDRi Papers Edition 11, May. https://edri.org/files/TTIP_and_DigitalRights_booklet_WEB.pdf.

EFF. 2015. "What is the Trans-Pacific Partnership Agreement?" www.eff.org/issues/tpp.

EOP. 1997. "Presidential Directive, Memorandum for the Heads of Executive Departments and Agencies: Electronic Commerce." EOP, July 1. http://clinton4.nara.gov/WH/New/Commerce/directive.html.

———. 2015. "US National Security Strategy." February. www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

Ermert, Monika. 2013. "Nations Begin to Take Action Against United States for NSA Spying." Intellectual Property Watch, July 9. www.ip-watch.org/2013/07/09/nations-begin-to-take-action-against-united-states-for-nsa-spying/.

———. 2014. "TISA Negotiations: Yes to E-Commerce, Data Flows, No to IPR, Data Protection?" Intellectual Property Watch, December 17. www.ip-watch.org/2014/12/17/TiSA-negotiations-yes-to-e-commerce-data-flows-no-to-ipr-data-protection/.

EUA. 2014. "Transatlantic Trade and Investment Partnership (TTIP) EUA Background Paper." December. www.eua.be/Libraries/Higher_Education/TTIP_background _paper_jan_2014.sflb.ashx.

———. 2015. "EUA Statement on TTIP and TiSA." EUA, January 30. www.eua.be/Libraries/Publication/EUA_Statement_TTIP.sflb.ashx.

EurActiv.com. 2010. "The Global Battle to Rule the Internet." October 3. www.euractiv.com/infosociety/internet-governance/article-142724.

———. 2013. "EU Challenges US Hegemony in Global Internet Governance." December 6. http://goo.gl/8VlICB.

European Commission. 2011. "European principles and guidelines for Internet resilience and stability." European Forum for Member States, March. http://ec.europa.eu/danmark/documents/alle_emner/videnskabelig/110401_rapport_cyberangreb_en.pdf.

———. 2013a. "How Much Does the TTIP Have in Common with ACTA?" European Commission, July. http://trade.ec.europa.eu/doclib/docs/2013/july/tradoc_151673.pdf.

———. 2013b. "European Commission Calls on the US to Restore Trust in EU-US Data Flows." European Commission press release, November 11. http://europa.eu/rapid/press-release_IP-13-1166_en.htm.

———. 2014a. "Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote." European Commission press release, March 12. http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.

———. 2014b. "Factsheet EU-US Negotiations on Data Protection." June. http://ec.europa.eu/deutschland/pdf/eu_-_us_negotiations_on_data_protection_-_june_2014.pdf.

———. 2015a. "Data Protection Day 2015: Concluding the EU Data Protection Reform Essential for the Digital Single Market." European Commission press release, January 28. http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm.

———. 2015b. "Report from the Commission to the European Council: Trade and Investment Barriers Report 2015." COM 2015 127. Final. http://europa.eu/rapid/press-release_IP-15-4618_en.htm.

European Commission — Justice. 2012. "How will the 'safe harbor' arrangement for personal data transfers to the US work?" http://ec.europa.eu/justice/policies/privacy/thridcountries/adequacy-faq1_en.htm#4.

———. 2015a. "Data protection Eurobarometer out today." June 24. http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm.

———. 2015b. "Protection of Personal Data." http://ec.europa.eu/justice/data-protection/index_en.htm.

———. 2015c. Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems), November 6. Com(2015) 566 final.

European Council. 2015. "Data Protection: Council Agrees on General Principles and the 'One Stop Shop' Mechanism." European Council press release, March 13. www.consilium.europa.eu/en/press/press-releases/2015/03/13-data-protection-council-agrees-general-principles-and-one-stop-shop-mechanism/.

European Union. 2011. "Legislation." *Official Journal of the European Union* 54 (May 14). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2011:127:FULL&from=EN.

———. 2014. "Digital Agenda for Europe." http://ec.europa.eu/digital-agenda/en/digital-agenda-europe.

Export.gov. 2013. "U.S.-EU Safe Harbor Overview." Export.gov, December 18. http://export.gov/safeharbor/eu/eg_main_018476.asp.

Expose the TPP. n.d. "The Trans-Pacific Partnership Would Undermine Internet Freedom." www.exposethetpp.org/TPPImpacts_InternetFreedom.html.

Fairless, Tom. 2014. "Europe Vs. US Tech Giants: Discontent on Continent Highlights Battle Over Economics, Culture, Internet Control." *Wall Street Journal*, December 9. www.wsj.com/articles/europe-vs-u-s-tech-giants-1418085890?mod=rss_Technology.

Federal Register: The Daily Journal of the United States Government. 2010. "Global Free Flow of Information on the Internet: Notice of Inquiry, 75 Fed. Reg 188, September 29." www.federalregister.gov/articles/2010/09/29/2010-24385/global-free-flow-of-information-on-the-internet#p-3.

Fish and Richardson PC. 2015. "ITC Says It Has the Power to Stop Infringing Transmissions of Digital Materials." March 13. www.lexology.com/library/detail.aspx?g=b96e269a-0b12-4fb5-85df-b13cb2e4f357.

Frizell, Sam. 2014. "Here's What Facebook Can Do With Your Personal Data in the Name of Science." *Time*, July 7. http://time.com/2949565/heres-what-facebook-can-do-with-your-personal-data-in-the-name-of-science/.

Gardner, Stephen. 2013. "EU Panel Data Protection Regulation Vote Delayed Until Fall by Amendments, PRISM." Bloomberg BNA, July 1. www.bna.com/eu-panel-data-n17179874844/.

Goldfarb, Danielle. 2011. "Canada's Trade in a Digital World." Conference Board of Canada. www.conferenceboard.ca/reports/briefings/tradingdigitally/pg2.aspx#ftn35-ref.

Goldsmith, J. L. and T. Wu. 2006. *Who Controls the Internet? Illusions of a Borderless World*. New York, NY: Oxford University Press.

Google. 2010. "Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information." Google, November 15. http://static.googleusercontent.com/media/www.google.com/en//googleblogs/pdfs/trade_free_flow_of_information.pdf.

———. 2011. Letter to Don Eiss, Trade Policy Staff Committee, re. Request for Public Comments to Compile the National Trade Estimate Report on Foreign Trade Barriers. USTR-2011-0008. November 15.

Greer, Evan. 2015. "The clock is ticking on a time bomb that could blow up a free internet: the TPP." *The Guardian*, November 6. www.theguardian.com/commentisfree/2015/nov/06/clock-ticking-time-bomb-blow-up-free-internet-tpp.

Hansen, Martin and Gabriel Slater. 2015. "TPP's Electronic Commerce Chapter." *National Law Review* (website), November 6. www.natlawreview.com/article/tpp-s-electronic-commerce-chapter.

Hill, Jonah Force. 2014. "The Growth of Data Localization Post Snowden: Analysis and Recommendations for US Policymakers and Industry Leaders." Lawfare Research Paper Series. 2 (3): 1–40, July 21.

Hindley, B. and H. L. Makiyama. 2009. "Protectionism Online: Internet Censorship and International Trade Law." ECIPE Working Paper. December. www.ecipe.org/media/publication_pdfs/protectionism-online-internet-censorship-and-international-trade-law.pdf.

Hirst, Nicholas. 2015. "US Tech Firms Targeted in Cybersecurity Talks." *Politico*, May 21. www.politico.eu/article/another-path-to-cybersecurity/.

Holleyman, Robert. 2015. "Remarks by Deputy U.S. Trade Representative Robert Holleyman to the New Democrat Network," May 1, Washington, DC. As prepared for delivery. USTR, May 1. https://ustr.gov/about-us/policy-offices/press-office/speechestranscripts/2015/may/remarks-deputy-us-trade.

Inside US Trade. 2011a. "US Tables Second Part of TPP Data Proposal, But Talks Still Preliminary." World Trade Online, November 11. http://insidetrade.com/inside-us-trade/us-tables-second-part-tpp-data-proposal-talks-still-preliminary.

———. 2011b. "US, EU Pursuing New e-commerce Principles for December Ministerial." World Trade Online, December 9. http://insidetrade.com/inside-us-trade/us-eu-pursuing-new-e-commerce-principles-december-ministerial.

———. 2012. "USTR Flags Procurement, Data Flow Issues as New Barriers in Canada." World Trade Online, April 27. http://insidetrade.com/inside-us-trade/ustr-flags-procurement-data-flow-issues-new-barriers-canada.

———. 2013. "Data Mining Revelations Could Impact US Business As EU Rewrites Rules." World Trade Online, June 14. http://insidetrade.com/inside-us-trade/data-mining-revelations-could-impact-us-business-eu-rewrites-rules.

———. 2014a. "US Tables New TiSA Proposal to Ensure Free Flow of Data." World Trade Online, May 16. http://insidetrade.com/inside-us-trade/us-tables-new-tisa-proposal-ensure-free-flow-data-network-access.

———. 2014b. "Leaked TISA Text Shows Clash on Data Transfer, Regulatory Transparency." World Trade Online, June 20. http://insidetrade.com/inside-us-trade/leaked-tisa-text-shows-clash-data-transfer-regulatory-transparency.

———. 2014c. "FTC Doubles Enforcement Actions Under Safe Harbor Amid EU Pressure." World Trade Online, July 3.

———. 2014d. "European Parliament Lays Out TISA Demands, Including China Participation." World Trade Online, January 16.

———. 2015. "China Publishes Notice Suspending Cyber Regs In Banking Sector." World Trade Online, April 24. http://insidetrade.com/inside-us-trade/china-publishes-notice-suspending-cyber-regs-banking-sector.

Internet and Jurisdiction Observatory. 2013. "Synthesis: Regular Update from the Synthesis & Jurisdiction Project." Volume 3. July 3. www.internetjurisdiction.net/wp-content/uploads/2013/08/Internet-Jurisdiction-SYNTHESIS-3-July-2013.pdf.

IP Commission. 2013. *The Report of the Commission on the Theft of American Intellectual Property*. The National Bureau of Asian Research, May. www.ipcommission.org/report/ip_commission_report_052213.pdf.

Israel, Tamir. n.d. "TISA Annex on Electronic Commerce: A preliminary Analysis by the Canadian Internet Policy and Public Interest Clinic." https://wikileaks.org/TiSA/ecommerce/.

James, Deborah. 2015. "Just Before Round of Negotiations on the Proposed TISA, WikiLeaks Releases Updated Secret Documents." Common Dreams, July 15. www.commondreams.org/views/2015/07/02/just-round-negotiations-proposed-TiSA-wikileaks-releases-updated-secret-documents.

Jenner and Block, LLP. 2014. "Memorandum to the Motion Picture Association: Use of the ITC to Block Foreign Pirate Websites." August 15.

Jerusalem Post. 2015. "Government Anti-Semitism Conference Endorses Net Censorship." *Jerusalem Post*, June 2. www.jpost.com/Israel-News/Government-anti-Semitism-conference-endorses-net-censorship-403123.

Jewish Telegraphic Agency. 2015. "News Brief: Cyberhate, Anti-Semitism Discussed at Jerusalem Forum." May 14. www.jta.org/2015/05/14/news-opinion/israel-middle-east/cyberhate-anti-semitism-discussed-at-jerusalem-global-forum.

Jourová, Vera. 2015."Speech by Commissioner Jourová: The future of U.S.-EU data transfer arrangements." Delivered at the Brookings Institution, Washington, DC. European Commission press release, November 16. http://europa.eu/rapid/press-release_SPEECH-15-6104_en.htm.

Kelsey, Jane and Burcu Kilic. 2014. "Briefing on US TISA Proposal on E-Commerce, Technology Transfer, Cross-border Data Flows and Net Neutrality." December 14. www.cil.cnrs.fr/CIL/IMG/pdf/analisis-cleaned.pdf.

Khan, Abdul Waheed. 2009. "Universal Access to Knowledge as a Global Public Good." Global Policy Forum Web Site. www.globalpolicy.org/social-and-economic-policy/global-public-goods-1-101/50437-universal-access-to-knowledge-as-a-global-public-good.html?itemid=id.

Kommerskollegium, National Board of Trade. 2014. "No Transfer, No Trade: The Importance of Cross-Border Data Transfers for Companies Based in Sweden." www.kommers.se/Documents/dokumentarkiv/publikationer/2014/No_Transfer_No_Trade_webb.pdf.

Kozner, Anthony. 2013. "All Major Tech Companies Say NSA Actions Put Public Trust In Internet At Risk." *Forbes*, December 9. www.forbes.com/sites/anthonykosner/2013/12/09/all-major-tech-companies-say-nsa-actions-puts-public-trust-in-internet-at-risk/.

Lagarde, Christine. 2015. "Reinvigorate Trade to Boost Global Economic Growth." International Monetary Fund, April.

La Rue, Frank. 2013. "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression." A/HRC/23/40. April. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

Lissitsa, Sabina and Svetlana Chachasvil-Bolotin. 2016. "Life satisfaction in the internet age — Changes in the past decade." *Computers in Human Behavior* 54 (January 6): 197–206. http://isiarticles.com/bundles/Article/pre/pdf/37816.pdf.

Litt, Robert S. 2013. "Privacy, Technology and National Security: An Overview of Intelligence Collection." July 19. www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy-technology-and-national-security-an-overview-of-intelligence-collection.

Makiyama, Hosuk Lee. 2011. "Future-proofing world trade in technology: Turning the WTO IT Agreement (ITA) into the International Digital Economy Agreement (IDEA)." Aussenwirtschaft, September 1. www.siaw.unisg.ch/journal/ausgaben/2011-iii.aspx.

Malcolm, Jeremy. 2015. "How Trade Agreements Harm Open Access and Open Source." *Open Access Week* (blog), October 21. www.eff.org/deeplinks/2015/10/how-trade-agreements-harm-open-access-and-open-source.

Mandel, M. 2013. "Data, Trade and Growth." TPRC 412: The 41st Research Conference on Communication, Information and Internet Policy. The Progressive Policy Institute, March. http://ssrn.com/abstract=2241302 or http://dx.doi.org/10.2139/ssrn.2241302.

Manyika, J., J. Bughin, S. Lund, O. Nottebohm, D. Poulter, S. Jauch and S. Ramaswamy. 2014. "Global Flows in a Digital Age: How Trade, Finance People, and Data Connect the World Economy." McKinsey Global Institute, April. www.mckinsey.com/insights/globalization/global_flows _in_a_digital_age.

Marchetti, Juan A. and Martin Roy. 2013. "The TISA Initiative: An Overview of Market Access Issues." Staff Working Paper ERSD-2013-11. WTO, November 27. www.wto.org/english/res_e/reser_e/ersd201311_e.pdf.

Martin, Eric. 2012. "WTO Members Seek Services Accord as Doha Stalls, US Says." Bloomberg.com, March 2. www.bloomberg.com/news/articles/2012-03-02/u-s-seeking-15-member-wto-services-deal-negotiator-says-1-.

Maskus, Keith E. and J. H. Reichman. 2004. "The Globalization of Private Knowledge Goods and the Privatization of Global Public Goods." *Journal of International Economic Law* 7 (2): 279–320.

Mattoo, A. and L. Schuknecht. 2000. "Trade Policies for Electronic Commerce." World Bank Policy Research Working Paper. http://elibrary.worldbank.org/doi/pdf/10.1596/1813-9450-2380.

Mattoo, A. and S. Wunsch-Vincent. 2004. "Pre-empting Protectionism in Services: The GATS and Outsourcing." *Journal of International Economic Law* 7(4): 765–800.

McKenna, Barrie. 2013. "Businesses Push for Freedom to Share Personal Data across Borders." *The Globe and Mail*, July 7. www.theglobeandmail.com/report-on-business/economy/businesses-push-for-freedom-to-share-personal-data-across-borders/article13054771/.

McKinsey Global Institute. 2011. "Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity." May. www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.

———. 2014. "China's Digital Transformation: The Internet's Impact on Productivity and Growth." July. www.mckinsey.com/insights/high_tech_telecoms_internet/chinas_digital_transformation.

Meeker, M. 2014. "Internet Trends 2014, Code Conference." May 28. http://kpcbweb2.s3.amazonaws.com/files/85/Internet_Trends_2014_vFINAL_-_05_28_14-_PDF.pdf?1401286773.

———. 2015. "Internet Trends 2015 — Code Conference." May 27. http://kpcbweb2.s3.amazonaws.com/files/90/Internet_Trends_2015.pdf?1432738078.

Meier, B. and R. F. Worth. 2010. "Emirates to Cut Data Services of Blackberry." *The New York Times*, August 2. www.nytimes.com/2010/08/02/business/global/02berry.html?pagewanted=all.

Murphy, Kevin. 2015. "Draconian Chinese Crackdown Puts Domain Industry at Risk." Domain Incite, May 27. http://domainincite.com/18586-draconian-chinese-crackdown-puts-domain-industry-at-risk.

Nakashima, Ellen. 2014. "Neustar, Telcordia battle over FCC contract to play traffic cop for phone calls, texts." *Washington Post*, August 9. www.washingtonpost.com/world/national-security/neustar-telcordia-battle-over-fcc-contract-to-play-traffic-cop-for-phone-calls-texts/2014/08/09/778edeaa-1e7b-11e4-ae54-0cfe1f974f8a_story.html.

———. 2015. "World's richest nations agree hacking for commercial benefit is off-limits." *Washington Post*, November 16. www.washingtonpost.com/world/national-security/worlds-richest-nations-agree-hacking-for-commercial-benefit-is-off-limits/2015/11/16/40bd0800-8ca9-11e5-acff-673ae92ddd2b_story.html.

National Board of Trade, Sweden. 2012. "E-commerce — New Opportunities, New Barriers: A survey of e-commerce barriers in countries outside the EU." www.kommers.se/In-English/Publications/2012/E-commerce--New-Opportunities-New-Barriers/.

Nepomuceno, Jigs. 2012. "Senate Ratifies Bicam Report on Data Privacy Act." *Zambo Times*, June 6. www.zambotimes.com/archives/48155-Senate-ratifies-bicam-report-on-Data- Privacy-Act.html.

New, William. 2014. "Leaked TPP Draft Reveals Extreme Rights Holder Position of US, Japan, Outraged Observers Say." www.ip-watch.org/2014/10/17/leaked-tpp-draft-reveals-extreme-rights-holder-position-of-us-japan-outraged-observers-say/.

———. 2015. "Confidential USTR Emails Show Close Industry Involvement in TPP Negotiations." *IP Watch*, June 5. www.ip-watch.org/2015/06/05/confidential-ustr-emails-show-close-industry-involvement-in-tpp-negotiations/?utm_source=IP-Watch+Subscribers&utm_campaign=9fdf634d39-WEEKLY_SUMMARY&utm_medium=email&utm_term=0_b78685696b-9fdf634d39-3521502576/05/2015.

NTIA. 2010a. "IPTF Global Free Flow of Information on the Internet Notice of Inquiry." September 29. www.ntia.doc.gov/federal-register-notices/2010/iptf-global-free-flow-information-internet-notice-inquiry.

———. 2010b. "Comments of the Computer and Communications Industry Association." December 6. www.ntia.doc.gov/files/ntia/comments/100921457-0457-01/attachments/CCIA%20Reply%20to%20DOC-NTIA%20NOI%20on%20Global%20Free%20Flow%20of%20Information.pdf.

———. 2010c. "Comments of the Center for Democracy and Technology." December 6. www.ntia.doc.gov/files/ntia/comments/100921457-0457-01/attachments/CDT-ARL-ALA%20Comments%20in%20the%20Free%20Flow%20NOI.pdf.

OECD. 1998. "OECD Action Plan." Directorate for Science, Technology and Industry Steering Committee for the Preparation of the Ottawa Ministerial Conference. SG/EC(98)9/Final. www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=SG/EC%2898%299/FINAL&docLanguage=En.

———. 2011a. "OECD Council Recommendation on Principles for Internet Policy Making." OECD, December.

———. 2011b. "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines." OECD, April.

———. 2013a. "The Internet Economy on the Rise: Progress Since the Seoul Declaration." www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/the-internet-economy-on-the-rise_9789264201545-en#page102.

———. 2013b. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." In *The OECD Privacy Framework*, 9–18. www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Palmer, Doug. 2012. "US steps up push for WTO services trade talks." Reuters, March 2. www.reuters.com/article/usa-trade-services-idUSL2E8E265D20120302#EPCHW0MJ5AwiAVDD.97.

Pearce, R. 2014. "Data Retention: Privacy Commissioner Issues Warning on Security." *Techworld*, September 4. www.techworld.com.au/article/551986/data_retention_privacy_commissioner_issues_warning_security/.

Penard, Thierry, Nicolas Poussing and Raphael Suire. 2013. "Does the Internet Make People Happier." *Journal of Socio-Economics* 46 (October): 105–16.

Powles, Julia. 2015. "Results May Vary: Border Disputes on the Frontline of the 'Right to Be Forgotten.'" *Slate*, February 25. www.slate.com/articles/technology/future_tense/2015/02/google_and_the_right_to_be_forgotten_should_delisting_be_global_or_local.html.

Price, Matthew. 2013. "Turn Back the Limousines: EU-US Trade Pact Faces Rocky Road." BBC News, July 1. www.bbc.co.uk/news/world-europe-23126238.

Public Knowledge and EFF. 2015. "Letter to Meredith M. Broadbent, Chairman, United States International Trade Commission." April 10. www.publicknowledge.org/assets/uploads/documents/letter-itc-public-interest.pdf.

Radio Free Asia. 2015. "China Seeks to Export Censorship to Overseas-Registered Domain Names: Report." November 6, www.rfa.org/english/news/china/china-censorship-11062015134614.html.

Rihter, Andreja. 2011. "The protection of privacy and personal data on the Internet and online media." Report, Committee on Culture, Science and Education Rapporteur: Ms. Andreja Rihter, Slovenia, Socialist Group, Doc. 12695. Council of Europe, July 29. http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=13151&Lang=EN.

Ronen, Gil. 2015. "Foreign Ministry to Fight Anti-Semitism on Google." Arutz Sheva, May 17. www.israelnationalnews.com/News/News.aspx/195514#.VW3ZBkY5W0q.

Samuel, Rebekah. 2011. "Controlling Copyright: Stifling Creativity, Innovation and Growth." *Media and Society* (blog), December 20. http://rebekahsamuel.com/blog/controlling-copyright-stifling-creativity-innovation-and-growth/.

Santoro, M. and W. Goldberg. 2009. "Fair Trade Suffers When China Censors the Internet. It's Not Just a Human Rights Issue." *Huffington Post*, January 8. www.huffingtonpost.com/michael-a-santoro-and-wendy-goldberg/chinese-internet-censorsh_b_156212.html.

Sayer, Peter. 2015. "Privacy watchdogs give EU, US three months to negotiate new Safe Harbor deal." PC World, October 19. www.pcworld.com/article/2994815/privacy-watchdogs-give-eu-us-three-months-to-negotiate-new-safe-harbor-deal.html.

Segal, Adam. 2015. "Cyber Week in Review: Net Politics." *Council on Foreign Relations* (blog), November 13. http://blogs.cfr.org/cyber/2015/11/13/cyber-week-in-review-november-13-2015/.

Sell, S. K. 2013. "Revenge of the 'Nerds': Collective Action against Intellectual Property Maximalism in the Global Information Age." *International Studies Review* 15: 67–85.

Seng, James. 2015. "What's Going On in China's Domain Name Industry." Circle ID, June 1. www.circleid.com/posts/20150601_whats_going_on_in_china_domain_name_industry/.

Shaffer, Gregory. 2000. "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of US Data Privacy Standards." *Yale Journal of International Law* 25 (Winter). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=531682.

Simmons, Beth A., Frank Dobbin and Geoffrey Garrett. 2007. "The Global Diffusion of Public Policies: Social Construction, Coercion, Competition or Learning?" *Annual Review of Sociology* 33: 449–72. http://ssrn.com/abstract=1517972.

Singh, Harsha V. 2013. "Welcome Remarks." CTS Workshop on E-commerce, June 16, WTO, Geneva, Switzerland. www.wto.org/english/tratop_e/serv_e/wkshop_june13_e/singh_e.pdf.

Spiegel Online International. 2013. "Growing Alarm: German Prosecutors to Review Allegations of US Spying." *Spiegel Online International*, June 30. www.spiegel.de/international/germany/german-prosecutors-to-review-nsa-spying-allegations-a-908636.html.

The Economist. 2014. "Start Up Nations: The Biggest Internet Economies." *The Economist*, July 12. www.economist.com/news/business/26850-biggest-Internet-companies.

Thielman, Sam. 2015. "WikiLeaks release of TPP deal text stokes 'freedom of expression' fears." *The Guardian*, October 9. www.theguardian.com/business/2015/oct/09/wikileaks-releases-tpp-intellectual-property-rights-chapter.

Third World Network. 2015. "Sharp 'asymmetries' in levels of ambition emerge in TiSA talks." SUNS #8003, April 16. www.twn.my/title2/wto.info/2015/ti150404.htm.

Tietje, Christian. 2011. "Global Information Law: Some Systemic Thoughts." Beiträge zum Transnationalen Wirtschaftsrecht, Heft 107. [Essays on Transnational Economic Law, No. 107]. Halle (Saale), Germany: Institute of Economic Law, Transnational Economic Law Research Center and School of Law, Martin Luther University Halle-Wittenberg. http://telc.jura.uni-halle.de/sites/default/files/BeitraegeTWR/Heft%20107.pdf.

Travis, Alan. 2013. "European Commission Backs Merkel's Call for Tougher Data Protection Laws." *The Guardian*, July 15. www.theguardian.com/world/2013/jul/15/european-commission-angela-merkel-data-protection.

Traynor, Ian. 2013. "NSA spying row: bugging friends is unacceptable, warn Germans." *The Guardian*, July 1. www.theguardian.com/world/2013/jul/01/nsa-spying-allegations-germany-us-france.

Trujillo, Mario. 2015. "Tech advocates triumph as court rejects Internet power for trade panel." *The Hill*, November 10. http://thehill.com/policy/technology/259668-tech-advocates-score-win-with-digital-imports-decision.

United Nations Conference on Trade and Development. 2015. "Information Economy Report 2015, Unlocking the Potential of E-commerce for Developing Countries." http://unctad.org/en/PublicationsLibrary/ier2015_en.pdf.

United States Department of Commerce. 2015. "Safe Harbor: Welcome to the US-EU and US-Swiss Safe Harbor Frameworks." October 9. www.export.gov/safeharbor/.

USITC. 2013. "Digital Trade in the U.S. and Global Economies, Part 1." Investigation No. 332-532, Publication 4415, July.

———. 2014. "Digital Trade in the U.S. and Global Economies, Part 2." Investigation No. 332-540, Publication 4485, September. www.usitc.gov/publications/332/pub4485.pdf.

USTR. 2012. "National Trade Estimate Report on Foreign Trade Barriers." March. https://ustr.gov/sites/default/files/NTE%20Final%20Printed_0.pdf.

———. 2013. "2013 National Trade Estimate Report on Foreign Trade Barriers." March, 60–61. www.ustr.gov/sites/default/files/2013%20NTE.pdf.

———. 2014a. "Section 1377 Review on Compliance with Telecommunications Trade Agreements." April. https://ustr.gov/sites/default/files/2013-14%20-1377Report-final.pdf.

———. 2014b. "National Trade Estimate Report on Foreign Trade Barriers." March. www.ustr.gov/sites/default/files/2014%20NTE%20Report%20on%20FTB.pdf.

———. 2015a. "U.S. Leads WTO Partners in Clinching Landmark Expansion of Information Technology Agreement." USTR press release, July. https://ustr.gov/about-us/policy-offices/press-office/press-releases/2015/july/us-leads-wto-partners-clinching.

———. 2015b. "TPP: Chapter 29 — Exceptions." November 5. https://medium.com/the-trans-pacific-partnership/exceptions-1299fbf34b76#.rbm5y87nc.

———. 2015c. "National Trade Estimate Report on Foreign Trade Barriers." March. https://ustr.gov/sites/default/files/2015%20NTE%20Combined.pdf.

WikiLeaks. 2014. "Leaked Financial Services Chapter of TISA." April 14. https://wikileaks.org/TiSA-financial/#start.

———. 2015. "The TiSA Annex on Domestic Regulation — Analysis of the 23 April 2015 Draft." https://wikileaks.org/tisa/domestic/04-2015/analysis/Analysis-TiSA-Domestic-Regulation-Annex.pdf.

Wilhelm, Ernst-Oliver. 2015. "A Brief History of Safe Harbor." IAPP. https://iapp.org/resources/article/a-brief-history-of-safe-harbor/.

World Bank. 2014. "World Development Report 2016: Internet for Development. Concept Note." Report No. 91877. World Bank, December 9. www.worldbank.org/content/dam/Worldbank/Publications/WDR/WDR%202016/WDR2016_Concept_Note.pdf.

WTO. 2011. "Communication from the United States, Work Program on Electronic Commerce: Ensuring that Trade Rules Support Innovative Advances in Computer Applications and Platforms such as Mobile applications and the Provision of Cloud Computing Services." S/C/W/339. Council for Trade in Services, September 20.

———. 2012a. "15 Years of the Information Technology Agreement: Trade, Innovation and Global Production Networks." www.wto.org/english/res_e/publications_e/ita15years_2012_e.pdf.

———. 2012b. "Information technology: progress reported on expanding product coverage." WTO News Item, November 1. www.wto.org/english/news_e/news12_e/ita_01nov12_e.htm.

———. 2013a. "WTO Public Forum 2013. The Internet as the World's Trading Platform: How and Why Is It So Successful?" WTO, October 3. www.wto.org/english/forums_e/public_forum13_e/pf13wks_e/wks15_e.htm.

———. 2013b. "Day 2 of Public Forum focuses on needs of consumers and small businesses." WTO, October 2. www.wto.org/english/news_e/news13_e/pfor_02oct13_e.htm.

———. 2015a. "Information Technology Agreement." www.wto.org/english/tratop_e/inftec_e/inftec_e.htm.

———. 2015b. "WTO Annual Report 2015." www.wto.org/english/res_e/publications_e/anrep15_e.htm.

———. n.d. "GATS: Fact and Fiction. Misunderstandings and Scare stories: The WTO and Internet Privacy." www.wto.org/english/tratop_e/serv_e/gats_factfiction10_e.htm.

Wunsch-Vincent, S. 2006. "The Internet, Cross-Border Trade in Services and the GATS: Lessons from US Gambling." *World Trade Review* 5 (3): 319–55.

ABOUT THE AUTHOR

Susan Ariel Aaronson is Research Professor of International Affairs at George Washington University's Elliott School of International Affairs and a George Washington University Cross Disciplinary Fellow. Susan teaches courses in trade, digital trade and digital rights, and corruption and good governance. She is currently directing projects on digital trade and digital rights, the World Trade Organization and human rights, repression and civil conflict, and whistle-blowers in international organizations. Her work has been funded by major international foundations including MacArthur, Ford and Rockefeller; by governments such as the Netherlands, the United States and Canada; by the United Nations, the International Labour Organization and the World Bank; and by US corporations including Ford Motor Company and eBay. Susan is the author of six books and numerous articles on trade, human rights, digital trade, corruption and globalization. She is a member of Working Group 2 of the Freedom Online Coalition and the academic board of Business and Human Rights.org. She is also the director of the eBay Policy Scholars at George Washington University.

CHAPTER SIX:
SOLVING THE INTERNATIONAL INTERNET POLICY COORDINATION PROBLEM

Nick Ashton-Hart

ACRONYMS

CC	Coordination Committee
CSTD	Commission on Science and Technology for Development
DACS	Digital Affairs Coordination Service
DEPOt	Digital Environment Policy Observatory
GPT	general purpose technology
IASC	Inter-Agency Standing Committee
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	information and communications technology
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IGO	intergovernmental organization
INTERPOL	International Criminal Police Organization
IP	Internet Protocol
ITU	International Telecommunication Union
LDC	least developed country
NGO	non-governmental organization
OCHA	Office for Coordination of Humanitarian Affairs
OECD	Organisation for Economic Co-operation and Development
ToR	terms of reference
UNCTAD	UN Conference on Trade and Development
WSIS	World Summit on the Information Society
WTO	World Trade Organization

INTRODUCTION

The digital ecosystem and its beating heart, the "network of networks" that is the public Internet, are inherently borderless and consequently impact, and are impacted by, an increasing spectrum of international public policy just as they do daily life. This is due to two factors:

- the Internet is a general purpose technology (GPT),[1] one of only a relative handful in all of recorded history; therefore, it drastically alters society worldwide through its impact on pre-existing economic and social structures; and
- the Internet's already enormous impact is accelerated and amplified further due to the principle of network effects.[2]

Given that less than 50 percent of humanity is currently online, these two realities ensure the impact that the Internet will have on policy making, and vice versa, is only just beginning to be felt — and will escalate and accelerate.

This chapter argues that continuing to address Internet-related public policy in subject-area silos, independently developing and implementing policy with ad hoc efforts to coordinate related activities, would be a serious mistake and a major missed opportunity. It does not argue for creation of a new international policy-making process but that existing fora, both intergovernmental and non-governmental, should coordinate with each other at the institutional level to deliver better policy results within existing processes and mandates. A straw man proposal for accomplishing these objectives is included in the Annex.

SETTING THE STAGE

Many stakeholders find it difficult to determine where to get help with key security and operational Internet concerns, especially across national boundaries. The "Internet dimension" to traditional public policy issues arose long after virtually all existing multilateral institutions were created to handle the "analog world." Globalization has created interdependencies between traditional policy silos, even without factoring in the further complexity added by the digital environment.[3] Multiple agencies must address elements of a single issue to create a sustainable outcome and this naturally creates tension: if negotiating parties cannot find a path to an outcome that meets their needs, conflicts are more difficult to resolve and stakeholders are incentivized to engage in "forum shopping" the same issue in multiple venues.

The constellation of public/private and non-governmental organization (NGO)-based processes that fill key roles in the Internet's technical management[4] can be confusing for governments (as well as others), given the many divergent mechanisms for decision making. Conversely, multilateral agencies can prove difficult and frustrating for non-

1 For context, other GPTs include electricity and the printing press. For further reading, see Rosenberg and Trajtenberg (2004). For perhaps the definitive treatment of the subject, especially from an economic perspective, see Lipsey, Carlaw and Bekar (2005).

2 For the most user-friendly, short explanation of what the network effect is and its context, see http://en.wikipedia.org/wiki/Network_effect.

3 For an excellent and prescient analysis specific to the Internet, see Keohane and Nye (1998). For a *tour d'horizon* of this dynamic across various policy fields see Drezner (2001).

4 A graphical illustration of the various technical functions can be found at www.icann.org/resources/unthemed-pages/functional-2014-02-20-en?routing_type=path. Another graphic that puts those functions into the broader socio-economic contexts of policies impacted by the Internet is available at www.icann.org/resources/unthemed-pages/layered-model-org-2014-02-20-en?routing_type=path. See also footnotes 3 and 8.

governmental stakeholders. At their most inclusive, these fora generally limit NGO participation to observation and occasional short comments when governments are finished talking. At their least inclusive, NGOs are unable to attend meetings at all or provide input in any way that can impact outcomes.

Finally, high-profile issues such as cyber security are tackled in a multitude of institutions and processes, ranging from purely intergovernmental and formalized (such as the Organisation for Economic Co-operation and Development [OECD] or the North Atlantic Treaty Organization, among others) to informal (such as conferences and multi-stakeholder collaborative environments), and the landscape is rapidly evolving.[5]

INTERNATIONAL POLICY MAKING DIRECTLY RELATED TO INFORMATION AND COMMUNICATIONS TECHNOLOGIES

The multilateral information and communications technology (ICT) policy framework was negotiated at the World Summit on the Information Society (WSIS) in 2003 and 2005.[6] While the WSIS negotiation process did include elements that involved non-governmental stakeholders, such as the Working Group on Internet Governance, the decisions it adopted were fundamentally intergovernmental in nature and the follow-up process to its implementation arrogates decision making largely to governments. UN agencies have a coordination mechanism for their activities — UNGIS (the United Nations Group on the Information Society)[7] — as do the UN member states themselves.[8] For all other stakeholders, there are opportunities to meet — notably at the annual meetings of the Internet Governance Forum (IGF) and the WSIS Forum — however, these are not policy-making fora.[9] This asymmetry has created continuous friction among stakeholders.[10]

By contrast, the key global technical functions that make possible all communications on Internet Protocol (IP)-based networks, including the Domain Name System and various IP-related addressing systems, predate the WSIS and are managed by several non-treaty-based organizations created by non-state actors. At these organizations, all stakeholders (including governments) collaborate on policy and standards-development activities that are by design interdependent, and where a high degree of coordination between among is necessary.

There are persistent debates about the governance of these organizations and disagreements about the relative positions of stakeholders vis-à-vis each other in decision-making processes. The practical results of the interrelationships between organizations demonstrate that coordination across interrelated policy activities creates results that are far more than the sum of their parts.[11]

At the time the WSIS conferences concluded, discussion of the Internet dimension of "offline" public policy issues was limited and largely related to technical subjects. Since then, digital issues have rapidly been mainstreamed into the work of policy making at the international level, but the natural silos of different subject areas has resulted in many (and probably most) stakeholders no longer being aware of where aspects of "their" issues are being addressed.

Against this background, periodic calls are made for an "Internet agency" of one sort or another to centralize

5 See pages 17–20 of www.unog.ch/80256EE600580270/(httpHomepages)/451CD0DD8D177D6780256F040066CF64?OpenDocument. A listing of the institutions and processes discussed in this report may be found in the database that accompanies it (see UN Conference on Trade and Development [UNCTAD] 2014, 9–11).

6 See www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2316|0.

7 Further information on its activities may be found at www.ungis.org.

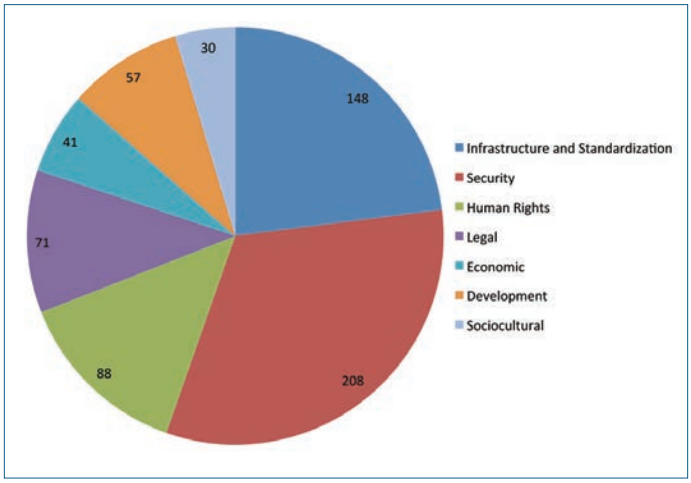
8 The most important in decision-making terms is the Commission on Science and Technology for Development (CSTD). See http://unctad.org/en/Pages/CSTD.aspx.

9 Within the WSIS framework the key discussion forum is the IGF and the regional and national IGFs; these latter continue to proliferate worldwide. The majority of policy making and standards development related to core Internet addressing and related areas take place outside of multilateral institutions.

10 While an in-depth analysis is beyond the scope of this chapter, in brief, the friction manifests itself as calls for increasing multi-stakeholder-driven policy development on the one hand and assertion of the need for state actors to remain the decisive decision makers in international public policy on the other.

11 For the non-technical reader, two examples are salutary: the development and deployment of the Domain Name System Security Extensions — an improvement to the global Internet addressing system's security architecture — and the development and deployment of domain name addresses in scripts such as Hindi, Arabic and Chinese, known as Internationalized Domain Names. For the former, see Rickard (2009), and for the latter see EURid and UN Educational, Scientific and Cultural Organization (2011).

Figure 1: Mechanisms Addressing Public Policy Issues Pertaining to the Internet



Data source: UNCTAD (2014).

Internet policy.[12] Some stakeholders (notably, but not entirely, developed countries) reject this idea as intended to allow governments to "take control" of key Internet functions and content online, while others see it as the only way that stretched policy makers, especially in developing countries, can hope to holistically influence international public policies that affect them.

That stalemate and the underlying political and societal differences that give rise to it have made multilateral discussions related to the digital environment extremely contentious, whether at the UN General Assembly, the Economic and Social Council and its many subsidiary bodies,[13] or the work of the more than two dozen UN-specialized agencies. The most well-known examples of these disputes relate to the activities of the International Telecommunication Union (ITU).[14]

12 Some of these calls are seen as a smokescreen for governments to control Internet content; others are seen as a positive need for better coordination across the multiplicity of actors and processes involved in Internet policy. All make similar points at the level of basic narrative. Two examples illustrating the opposite ends of the spectrum are:

- an Indian proposal for a "United Nations Committee for Internet Related Policies" (see http://cis-india.org/internet-governance/blog/india-statement-un-cirp for more information); and
- the Panel on Global Internet Cooperation and Governance Mechanisms, convened by the Internet Corporation for Assigned Names and Numbers (ICANN), proposed a distributed fully multi-stakeholder-driven, ecosystem-based approach to Internet governance issues. Its approach underpins the NETmundial Initiative (see www.netmundial.org), launched by ICANN, the World Economic Forum and cgi.br in November 2014. See ICANN (2014).

13 For an excellent *tour d'horizon* of this dynamic, viewed through the lens of information security policy, see Gjelten (2010). The Snowden revelations have made the issues Gjelten describes far more acute.

14 A current European view of the ITU and its role in Internet policy may be found in Schaller and Thimm (2014).

The difficulties can seem unique to each community, but really they are not: stakeholders understand and participate in the activities of the silo with which they are most concerned, but related activities outside of that silo are a different story altogether. This suggests a mechanism is needed to facilitate engagement between silos on interrelated subjects without complicating policy-making activities or creating another policy-making forum.

How Serious Is the Problem of Digital Policy Development Dispersion?

Despite mainstreaming digital issues throughout international policy-making environments, the first study of the scope of that dispersion was published in November 2014 (UNCTAD 2014, 17–20).[15]

The survey grouped governmental and non-governmental "mechanisms" addressing "identified international public policy issues pertaining to the Internet" into seven broad clusters (ibid.). Despite an acknowledgement that the list is not exhaustive, it nevertheless contains 643 mechanisms across 40 issues in those seven clusters.

As an illustration of the extreme level of policy fragmentation, the "Security" cluster alone involves more than a dozen international organizations, a similar number of regional intergovernmental bodies and numerous non-governmental fora.

It is important to recognize that facilitating participation and coordination across related or interconnected issues in different fora is entirely separate from value judgments about how those processes should operate. The need for different objective outcomes has resulted in very different models of decision making. For example, development of technical standards, such as at the Internet Engineering Task Force (IETF), ensures that barriers to entry for new participants are very low, as the objective outcomes are technical: success is much more likely if anyone with sufficient technical knowledge, good English language skills and a good idea is easily able to participate with like-minded experts. By contrast, where different socio-economic interests have to resolve issues that do not lend themselves to a technical solution, the processes used are different: resolving values-related disputes, such as the practical application of international law related to social issues, tends to be much more formalized and rules-based and results in very different choices about which stakeholders should have what level of standing.

This differentiation is particularly important with respect to digital issues because in each thematic cluster — for

15 The UNCTAD (2014) report began as an effort on the sidelines of the CSTD's Working Group on Enhanced Cooperation (see http://unctad.org/en/Pages/CSTD/WGEC.aspx). The story of that exercise may be found in Dickinson (2014).

example, security — there are fora that must address values-based issues and more empirical, technical issues, and the successful result of both can be strongly interdependent. As an example, negotiations about encryption have a very technical element: facilitating development of encryption standards to ensure products and services that rely upon them are in fact secure. They also have elements that are values-based: balancing the use of encryption to facilitate objectives as varied as freedom of expression, protection of intellectual property and protection of national security through access to encrypted information. No single method of working on policy suits all of these diverse objectives, but a successful result that is technically valid and socially acceptable is greatly assisted if each process or fora can interact and coordinate constructively with the work in the others.

Geneva's Role in International Internet-related Policy Development

Two-thirds of the UN system's work takes place in Geneva,[16] and the Diplo Foundation has estimated that more than 50 percent of all international policy meetings related to the digital environment take place there as well. (See Figure 2). In the last decade of his engagement with international policy related to the digital environment, the author has observed a clear trend emerging: discussions related to the Internet have spread with respect to both the number of processes and the number of agencies involved in them.

There are numerous reasons why this is occurring:

- This is the natural result of the spread of the economic and social impacts of the Internet itself: the principle of network effects, combined with an increasing proportion of humanity online, means that the Internet dimension to pre-Internet (or "offline") issues has increased.[17]
- Governments are experiencing the same spread of Internet dimensions to the work of ministries at the national level, and the inherently global nature of the Internet naturally ensures that governments will seek international responses to emerging issues. This spread has rapidly accelerated and become far more political and divisive since the Edward Snowden revelations.
- Multilateral institutions perceive tackling Internet-related issues as important for demonstrating their relevance to core stakeholders and also across the UN system. This incentivizes the proliferation of activity even when duplicative or tangential to the mandate of the organization.[18] Of course, the same dynamic can and does play out at the national level among ministries.
- Governments seeking a policy result internationally have an incentive to "forum shop," raising the same core issue in multiple fora to see where it gets the most traction.

All of this is complicated by the structural division between UN member states' missions in Geneva: the general UN mission handles most of the UN processes, while the World Trade Organization (WTO), UNCTAD, the International Trade Centre, the World Intellectual Property Organization and a few others are usually handled by the trade mission. Often, each of the two has a separate ambassador and there are sometimes competitive dynamics between them; this increases opportunities for forum shopping and for contradictory policy proposals.[19] Trade policy increasingly implicates ICT issues and especially the Internet, increasing the number of discussions and their relative economic significance.[20]

This spread of Internet-related discussions and their complexity, intensity and variety, alongside their increasing politicization, has attracted the attention of the UN secretariat at a senior level,[21] as well as the host country Switzerland,[22] and has resulted in increased allocation of resources to Internet issues by Geneva-based missions.[23] In particular, human rights legal advice is needed in more

16 According to the UN Office in Geneva; see www.unog.ch/80256EE600580270/(httpHomepages)/451CD0DD8D177D6780256F040066CF64?OpenDocument.

17 Approximately 580,000 people go online for the first time every day, an increase from 550,000 in 2012. This number is derived from ITU (2014).

18 The ITU is a particular "hot spot" for this dynamic.

19 A good example of this was discovered in 2012, when the general missions of some countries were making proposals for a treaty-making conference under the aegis of the ITU that were not congruent with their trade commitments at the WTO — and the two missions were not only unaware of the problem, they had not even asked their colleagues in the other mission for advice. See Lee-Makiyama and Samarajiva (2012).

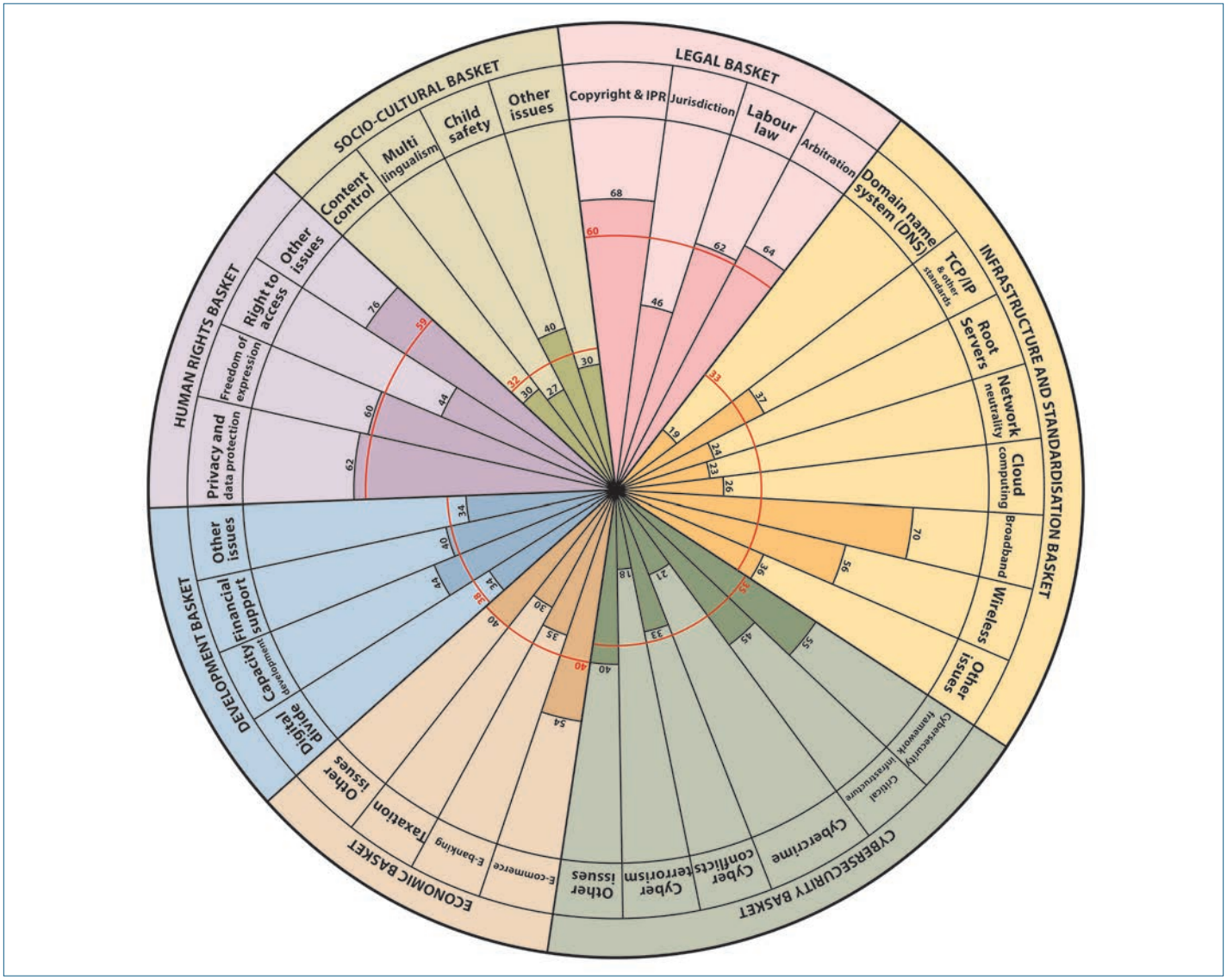
20 There are many examples of this, but the most significant are the ongoing Trade in Services Agreement negotiations (see https://en.wikipedia.org/wiki/Trade_in_Services_Agreement). These negotiations are outside the WTO per se, although all the participating countries are WTO members, and the informal discussions on how to address Internet-related trade more formally at the WTO itself started with a US proposal to the WTO Services Council. See WTO (2014).

21 This is based upon the author's bilateral conversations with relevant officials.

22 The host country funds the Geneva Internet Platform to help the Geneva international community deal with the increasingly complicated and busy Internet-related policy situation. See www.giplatform.org/.

23 The experience of the United Kingdom is salutary, yet far from unique: in correspondence with the author, in late 2013 there was one person who reported officially dedicating 25 percent of their time to Internet issues. As of this writing, there is a first secretary dedicating about 30 percent to the subject and another dedicated full time. It is also the author's observation that while two years ago the "Internet portfolio" was often allocated to a third or second secretary, it is now normally handled by a first secretary.

Figure 2: Geneva's Role in Global Internet Governance (in %)



Source: Kurbalija (2014).

and more fora as a direct consequence of the Snowden revelations.

Despite increased resourcing, those diplomats responsible for Internet issues are stretched. National governments, especially in OECD countries, are establishing Internet policy coordination teams to respond to the increase in both national and international policy discussions with an Internet dimension.

On the non-governmental side, even civil society groups from the developed world routinely say that they are unable to attend all the meetings that concern them relating to digital issues because of Geneva's relative cost. There are other barriers to entry: the complexities of NGO accreditation at different agencies create burdens for participation, with requirements for multiple applications for standing and long approval timelines.[24]

For stakeholders from developing and least developed countries (LDCs), the situation is much worse. It is very common to see diplomatic missions in Geneva, especially for LDCs, that have only two or three diplomats to cover the work of 95 UN agencies and related international organizations and the more than 250 international NGOs in Geneva.[25] Even countries that have made ICTs and the

24 For further details on the barriers NGOs face and some ideas for how to remediate these issues see Zettler (2009).

25 A WTO publication found that the average number of staff in Geneva diplomatic missions was 6.3 at the end of 2012, although the statistical coverage of the report is on 136 of the 173 UN member states (vanGrasstek 2013, 88, Table 3.1). For a high level statistical view of international Geneva more broadly, see WhyGeneva.ch (2015).

Internet a key part of their national development plans cannot allocate sufficient staff time in Geneva to cover Internet issues when they have so few staff to start with. It is the author's personal experience that following the work of even one of several agencies in Geneva with substantial activities related to the digital environment can take up all of one person's time throughout most of the year.

In addition to Geneva, many non-governmental mechanisms and processes that have pivotal responsibilities for various aspects of international Internet-related policy are widely distributed. There are also key intergovernmental organizations (IGOs) — such as the OECD, the International Criminal Police Organization (INTERPOL) and the United Nations Office on Drugs and Crime — with long-standing work programs in Internet-related policy based elsewhere. It is also true that fundamentally important processes in every major policy cluster are devolved to non-intergovernmental organizations. Nevertheless, it is clear that Geneva will be a major locus of an increasing amount of Internet-related multilateral policy work. It is also clear that this work would benefit enormously by better coordination, especially given that non-governmental processes have fundamentally important roles that the more formalized IGO-based processes must leverage.

WHY HAVE WE NOT SEEN A HOLISTIC RESPONSE TO THE PROBLEM?

The proposition that better coordination of Internet-related policy making is necessary is not new; it has been discussed since before the conclusion of the WSIS agreements in 2003 and 2005 (Drake and Price 2014). There are several reasons why the problem has not been solved, which are worth noting (Drake and Kaspar 2014).

First, the "pain threshold" of a critical mass of stakeholders in dealing with the burdens imposed by lack of coordination has not been sufficiently high to force action. The level of pain is growing alongside a significant increase in negative, political and polarized discussion of Internet issues over the last 18 months.

Second, the proposals for coordination have either failed to adequately address the political fault lines and/or meet the practical need for a holistic solution,[26] and thereby sufficiently motivate both non-governmental and governmental institutions to collaborate in two key ways:

- they are entirely voluntary, fully multi-stakeholder initiatives (which some countries won't accept), or are entirely intergovernmental, such as new UN agencies intended to make policy (which others reject);[27] and
- they are not comprehensive enough, either:
  - failing to inspire sufficient confidence in their likely practical effectiveness and scope; or
  - unable to achieve a critical mass of participation from governmental, intergovernmental and non-governmental stakeholders.[28]

It is likely that the scales have finally reached a tipping point: a spate of high-profile terrorist and quasi-terrorist incidents in various countries, combined with high-profile hacking incidents, has dramatically increased calls for action on various cyber security fronts. Given that these incidents have often had multinational dimensions, this has led to dramatically increased interest in action to increase international cooperation on Internet issues more widely.[29]

LOOKING FOR SOLUTIONS: BUILDING ON PAST EXPERIENCE

To find solutions, it is helpful to look at how the international community has sought to solve policy coordination problems crossing multilateral, governmental and non-governmental silos at the international level. A particularly relevant example may be found in the genesis and development of the Office for Coordination of Humanitarian Affairs (OCHA), a specialized agency of the UN.

---

26 For example, the use of encryption to facilitate human rights online is active at the Human Rights Council (in standard-setting bodies such as the IETF) and a long-standing feature of law enforcement-related discussions at a host of such venues, just as it will undoubtedly come up in a trade context during ecommerce discussions at the WTO and UNCTAD. It has been active at the OECD for several years and implicates existing treaty arrangements such as the Wassenaar Arrangement (for the most comprehensive overview, see http://en.wikipedia.org/wiki/Wassenaar_Arrangement). Without effective coordination — and cross-silo participation by stakeholders — sustainable and equitable results will be difficult at best, and further complexity and conflicts of laws problems are the more likely result. The existing legal landscape of this subject is a well-known and long-standing global headache for commerce. A good practical example of this can be found at www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html.

27 The Indian CIRP proposal is the most well-known example. See footnote 13.

28 The NETmundial Initiative is the latest of many examples. See footnote 13.

29 The author has attended a number of private meetings in recent months with capital-based senior government figures who have come to Geneva specifically to see how the international system can better address security and broader Internet policy issues, and whether a new international agency is needed to do so.

OCHA was created by the UN General Assembly in 1991[30] to ensure better coordination in humanitarian emergencies across the UN system as well as between the UN and the non-governmental humanitarian community (UN General Assembly 1991).

Just as in the Internet policy space, the humanitarian community is composed of many UN agencies with different operational mandates and priorities, but also thousands of independent non-governmental actors, some of which have budgets that are larger than all but the largest multilateral humanitarian institutions. Ensuring that all can respond within their mandates and expertise quickly and in a way that minimizes duplication and gaps in coverage is literally a life-and-death matter, often for large populations.

The OCHA has grown since its inception[31] to cover policy coordination between agencies and an extensive shared logistics function. It also provides a venue for shared fundraising and trust funds to ensure systemic capacity for very rapid response.

While some of these functions are not transferable to the Internet policy situation, the following are.

The Inter-Agency Standing Committee (IASC):[32] created by the UN General Assembly (1991), the IASC is a forum for UN and non-UN organizations to work together to facilitate coordination, minimize gaps in delivery and agree on shared activities and programs. It has various sub-bodies it establishes as needed, some permanent, others for specific time-bound purposes. While the "full members" of the IASC are all part of the UN system, there are "standing invitees" from the non-UN world that collectively represent several hundred entities from the largest and wealthiest NGOs to groups of volunteers.[33]

Providing shared information sources and databases:[34]

- ReliefWeb is the most comprehensive humanitarian information source in the world for practitioners, aggregating information from 3,500 sources from across the humanitarian community. A one-stop portal that's highly user configurable and which includes "push" updates, in 2013 alone it had five million unique visitors;[35]
- IrinNews[36] is a news and analysis portal providing information for the wider world on humanitarian issues. Just over half its audience is not from the humanitarian community; it helps to ensure journalists and researchers have a trusted place to turn for comprehensive information on humanitarian activities, including image and video libraries as well as documentary films, all of which have been used by mainstream press outlets worldwide; and
- humanitarian response:[37] a suite of digital tools for those working on emergencies, particularly those in the field, ranging from comprehensive contact information to meeting schedules to detailed maps and common datasets.

Also relevant is that the OCHA doesn't decide what should be done or by whom. It is administratively responsible to the UN, but the stakeholders participating in the IASC are key to defining what services it provides.[38] Its decisions are generally made by consensus.[39]

Characteristics of a Successful Mechanism

To create a solution to the coordination problem that is both politically viable and practically useful is difficult but not impossible. The following would need to be avoided:

- creating a new agency or intergovernmental body of UN member states with a general Internet-wide remit — this will not attract a sufficient level of intergovernmental support;
- substantially widening the mandate of an existing UN agency or intergovernmental body or process. For the various agencies to cooperate, a mechanism that engenders trust is needed and making one the "first amongst equals" would do the opposite and exacerbate competitive dynamics that already exist;
- disconnecting the new process from the multilateral system. The intergovernmental institutions have established mandates and collectively will be unwilling to fully participate in any process that is

30 The original proposer was the United States, at the instigation of former President George H. W. Bush.

31 A one-page graphical history may be found at www.unocha.org/sites/default/files/OCHA_Category/About%20Us/History/AshortHistory_OCHA_1200.jpg.

32 See www.humanitarianinfo.org/iasc/.

33 According to the IASC, "In practice, no distinction is made between 'Members' and 'Standing Invitees' and the number of participating agencies has expanded since inception of the IASC in 1992." See http://humanitarianinfo.org/iasc/pageloader.aspx?page=content-about-default (and confirmed in interviews with OCHA staff by the author).

34 Only the relevant services are discussed — the complete picture is available at www.unocha.org/what-we-do/information-management/im-services.

35 See http://reliefweb.int/report/world/reliefweb-highlights-2013.

36 See http://irinnews.org.

37 See www.humanitarianresponse.info/.

38 While the UN humanitarian agencies are obliged to collaborate by the member states that fund them (and to which they answer), the non-multilateral humanitarian actors are not so obliged and presumably remain participants in the OCHA because they see it as worthwhile.

39 For a discussion of decision making, objectives and mandates, the revised IASC Terms of Reference (ToR) (2014) are available at http://humanitarianinfo.org/iasc/downloadDoc.aspx?docID=6700&type=pdf.

entirely outside the international system. For the same reason, the new process cannot be disconnected from or disenfranchise the non-IGO sector. Many aspects of international policy making with a digital dimension are decided and managed outside the UN system, ranging from the management of the Internet's addressing systems to collaboration on prevention of crime online at EUROPOL (the European Police Organization) and INTERPOL to the London Process on spam mitigation, to name just a few examples; and

- duplicating existing processes or reducing their value.[40] Any features that have this effect will create suspicion in all of the organizations whose participation is sought, as they will likely suspect that the new entity's underlying purpose is in taking power from participating organizations over time.

With this in mind, the following are essential to success:

- The process should create a venue where collaboration by the multiplicity of actors and organizations that make or implement international Internet policy is facilitated and incentivized to ensure maximum synergies are possible. It must do so in ways that incentivize participation and collaboration by as many processes and institutions as possible — and not itself be a policy-making forum.
- The solution is administrative in nature and must be seen as neutral — and therefore must not be part of any existing agency or process with a policy-making or policy-implementation mandate. This suggests that its leadership should report administratively and financially to a neutral party, but the organizations and entities it serves must have a mechanism to evaluate its performance in a manner that creates effective accountability to its participants.
- It should provide services that facilitate understanding — both for all stakeholders and the interested public — of the multitude of activities related to Internet policy at the international level, decisions taken, processes under way and what facilities exist for participation in these fora. This requires services that contextualize information for different audiences in order to relate activities to their interests.
- It should not be large or expensive. A small team with specific, quantifiable objectives should suffice, especially early on.
- It should be located where the bulk of working international meetings that relate to the Internet are held — Geneva, Switzerland.
- It should recognize that different stakeholder communities work differently and often use different processes and languages. It must be able to speak to and work with all stakeholders constructively.

Constituting a mechanism along these lines meets three main political and practical needs. First, it would provide a political compromise between those who want a new, classic intergovernmental organization and those who would prefer nothing new. Second, it would meet the needs of both governments and the non-governmental sector in navigating the thicket of different institutions and processes with policy roles by helping them to find and understand the value in their context of the various processes that exist. And third, it would create a forum where collaboration across entities could proceed in a structured, demand-driven way that would not disrupt, negatively impact or duplicate existing structures.

FINAL THOUGHTS

The pain threshold of actors in dealing with the increasingly complex digital environment and the policy challenges it has complicated has reached the point where investing the energy in solving the problem is less demanding than continuing to live with the status quo, as long as political and practical fault lines are avoided.

There is one additional element in favour of action: 2015 is the decennial review of the WSIS. Proposals for a new intergovernmental Internet agency are already in the process of reintroduction. Providing a viable path that effectively addresses the coordination issues and facilitates greater engagement by developing countries and LDCs and their stakeholders would have substantial value. Such a counterproposal would meet the practical needs that proponents of a new "Internet agency" are looking for (although it would not meet, it must be acknowledged, some underlying political objectives for some proponents), without the negative baggage that a new policy-making agency is likely to be burdened with.

While it affects all stakeholders, developing countries and particularly LDCs have a legitimate complaint about the difficulty of participating in Internet policy across so many institutions and processes. At a practical level, there is a genuine and pressing need to address stakeholders' calls for clarity on where to turn for best practices and technical assistance in solving practical issues.

ACKNOWLEDGEMENTS

I would like to thank the many policy makers from the governmental, intergovernmental and non-governmental spheres who reviewed drafts of this document, in some cases more than once, and who without exception provided very detailed and thoughtful comments. While all were promised anonymity, I know who you are and you have my gratitude. This chapter is much better for your contributions, even if I am solely responsible for the end result.

40 In the latter case, creating links with the existing fora where Internet policy is discussed, including but not limited to the annual IGF, will be important to many stakeholders.

ANNEX: A STRAW MAN FOR A DIGITAL AFFAIRS COORDINATION SERVICE

Digital Affairs Coordination Service

Mission: To provide a venue where all organizations and processes engaged in activities impacting the digital environment at the global level may collaborate and exchange information to ensure their efforts maximize the potential for cooperation, each within their mandates.

To provide information services that facilitate all stakeholders' understanding of the many activities, processes and negotiations taking place worldwide in both intergovernmental and non-governmental fora that relate to the digital environment and how they may participate in these activities.

Location: Geneva, Switzerland

Structure

Coordination Committee

The Coordination Committee (CC) is composed of principals designated by each of the member organizations — organizations or processes with a mandate that has an international impact on policy development or implementation related to the digital environment, including:

- multilateral, treaty-based organizations such as UN agencies and non-UN family members, for example, the OECD and the WTO;
- NGOs such as the IETF and ICANN; and
- less formal bodies such as the London Action Plan and the Messaging, Mobile and Malware Anti-Abuse Working Group,[41] both of which deal with unsolicited electronic messaging (often referred to as "spam") mitigation, and the International Consumer Protection and Enforcement Network, a global network of national consumer protection organizations that addresses the transboundary dimension of consumer protection online.

Primary Objectives

The overall objective of the CC is to improve coordination of activities among the agencies and processes that impact or are impacted by the digital environment, including the public Internet. This objective is facilitated through a program of work:

- to identify and address areas where:
  - gaps in mandates or lack of operational capacity exist;
  - there is overlap in activities that could be rationalized; and
  - collaboration is necessary or desirable for an outcome that is more than the sum of its parts;
- to share information on the issues their organizations are confronting in execution of their mandates as relevant;
- to advocate common principles to parties outside the CC where useful or necessary and as agreed by the CC;
- to resolve disputes or disagreements about and among participants on coordination issues;
- to propose services that the Digital Affairs Coordination Service (DACS) can offer to stakeholders participating in policy activities related to the DACS' mandate across its member organizations and the wider public interested in digital environment policy;
- to provide an annual evaluation of the activities of the DACS to the director-general of the UN Office in Geneva for publication, including a facility that allows for comments on the report to be taken from interested stakeholders; and
- participation and accreditation in members' processes: one of the CC's priorities should be to look at the various mechanisms for participation of stakeholders through the exchange of best practices and by identifying opportunities for facilitating participation, especially for stakeholders from developing countries and LDCs. Ideally, the CC should have a standing committee dedicated to these questions. Given the cost of physical participation in meetings, considering how to facilitate meaningful participation by stakeholders at a distance using electronic tools should be a priority.[42]

Key Principles

- Non-policy making: the CC is not a policy-making body; decisions reached by the CC can only be implemented by the members acting within their own organizations;
- respect for mandates: decisions of the CC may not compromise organizations with respect to their own mandates;
- ownership: that all organizations have an equal ownership of the CC and its subsidiary bodies and the decisions they reach;

41 See http://londonactionplan.org/ and www.m3aawg.org/.

42 It is understood that each institution is responsible for stakeholder participation directly in its activities; this process would address participation in related activities across institutions.

- overall objective: to support effective policy making and implementation activities through mutually agreed coordination involving member organizations;
- subsidiarity: that decisions will be taken at the most appropriate level as agreed by CC principals;
- impartiality of the secretariat: the secretariat does not represent the interests of any one organization or group of organizations; and
- transparency: the activities of the CC should be public by default with any redactions from minutes of meetings kept to the minimum necessary for legal requirements or best practices with respect to the privacy of individuals.

Membership

As mentioned above, the CC should be composed of organizations or processes with a mandate for international policy making or policy implementation that impacts upon the digital environment at the international level.

The CC's overall objective is inclusive coordination, while maintaining a relatively limited number of "members" to ensure functionality and focus.

Membership is subject to continuous review and new members are accepted on a case-by-case basis. Organizations aspiring to become members would be encouraged to contact the CC secretariat. The CC may set any criteria for membership that it may deem useful from time to time, provided it publishes the same and seeks comment on the criteria it decides upon when changes are proposed.

The CC should operate under terms of reference (ToR) that may be amended as required from time to time; it should seek comment in advance from stakeholders, where appropriate, when revisions are proposed.[43]

Secretariat

The CC secretariat is responsible for providing technical support and servicing the meetings of the CC and its subsidiary bodies as well as monitoring the implementation of its decisions.

In general, the CC secretariat is tasked with:[44]

- proactively maintaining communication channels among organizations;
- collating and suggesting possible future agenda items on an ongoing basis;
- preparing an annual work plan for the CC based on decisions taken at its annual meetings;
- facilitating preparations for each meeting of the CC principals and subsidiary bodies;
- facilitating regular and ad hoc meetings of the same;
- disseminating minutes and records of meetings and decisions taken;
- monitoring the implementation of CC and subsidiary body decisions; and
- supporting the chairs of the CC bodies in highlighting and fostering connectivity and collaboration between the members and their designated representatives in the CC's work overall.

The secretariat of the CC should require only a handful of people. By way of comparison, the equivalent body of the OCHA consists of eight persons.[45]

Relationships and Cooperation

To the extent useful and agreed by the CC, the activities of the DACS should (within its remit) assist other environments and processes where very broad discussions of international Internet-related public policy take place. The best way to understand what is meant is to use examples; below are two. It is true that the depth of cooperation in the examples provided would likely allow only a limited number of such engagements each year for resourcing reasons.

Working with the IGF

As the IGF is the main global discussion forum that brings together all Internet stakeholders across all issues, links between the IGF's and the DACS' activities are important. The following are suggested as ideas for engagement by DACS in the IGF's annual meetings:[46]

- A meeting of the CC at the principals level could be held at the IGF, open to all IGF attendees.

43 The OCHA's ToR would seem a useful basis for drafting of an initial ToR for the CC. See www.humanitarianinfo.org/iasc/downloadDoc.aspx?docID=6700&type=pdf. The phrase "seek comment" could mean that the existing members would consult their own members and stakeholders, or comment could be taken by the DACS itself more broadly, or both.

44 It is understood that the secretariat's objectives and ToR may be modified by the CC.

45 See "The Team" at the bottom right of www.humanitarianinfo.org/iasc/pageloader.aspx?page=content-contact-default.

46 It is worth highlighting that a number of these proposals are taken from UNCTAD (2012). It is certainly the case that these functions could be addressed by the IGF; to date, the funding of the IGF has been insufficient to implement these measures. Allowing a DACS to work as proposed would help the IGF considerably without cost to the IGF itself.

- Focus sessions could be held by the DACS to allow all IGF attendees to understand the DACS' main activities and to take input from IGF attendees on them. For example, creating opportunities at the IGF for attendees to comment on CC proposals to facilitate participation of stakeholders in work streams across thematic subject areas and institutions (see "participation and accreditation in members' processes" point in the Primary Objectives section above) would be a value-add for both attendees and the DACS, especially where it has a focus on facilitating such engagement by developing country and LDC stakeholders.
- Wherever possible, and subject to CC members' internal priorities and resources, it could prove useful to have focus sessions on thematic subject areas that are shared by the relevant CC member institutions (for example, social development, human rights online, cyber security and others).
- Wherever possible the DACS should provide materials on a thematic basis drawn from the Digital Environment Policy Observatory (DEPOt) (see below), which could be of use to IGF attendees.
- Any outcomes of the IGF could be provided to the CC for use as appropriate within CC member organizations. Likewise, the DACS secretariat should ensure that where CC members' activities correspond to subjects raised in the previous year's IGF outputs that this is provided back to the IGF secretariat for onward communication to IGF participants.

Working with the London Process

Of all the thematic subject areas related to Internet policy, cyber security is perhaps the most important priority area across stakeholder communities.[47] Each year a major international conference is held covering all aspects of cyber security as part of what is known as the "London Process."

Here are a few ideas for how DACS could engage with the process:

- At least one meeting of the CC at the principal level could be held during the meeting, open to all attendees as observers.
- Sessions could be organized by the DACS to familiarize interested attendees about current priorities of the DACS and of the CC as they relate to various cyber security issues and to take input from attendees on each. The secretariat can then collate and publish input received for consideration by the CC. For example, creating opportunities at the conference for attendees to comment on CC proposals to facilitate participation of stakeholders in work streams related to cyber security (see "participation and accreditation in members' processes" point above) would be a value-add for both conference attendees and the DACS.
- Wherever possible, the DACS should provide materials on a thematic basis drawn from the DEPOt for conference attendees. These should make it easy to understand the main activities under way in various aspects of cyber security across CC member organizations.

Additional DACS Services

DEPOt

The DEPOt is the digital environment equivalent of ReliefWeb[48] for the humanitarian community: a single place where all the policy processes, reports, meeting information, and information on how to participate in relevant policy activities is aggregated in one place. It should provide open access to information on activities happening across entities that relate to the same policy area or to interrelated policy areas presented in a common accessible language and format that's tailored to the following audiences, in no particular order:

- government;
- private sector;
- civil society;
- technical and standards community; and
- academia.

An essential element of DEPOt will be ensuring "push" technologies are available so that stakeholders receive information relevant to them as it becomes available. At a later stage, creating a portal that is to digital environment issues as IrinNews is to the humanitarian community may be needed.

In the initial stages, only a handful of staff should be required to create and manage DEPOt. The DACS should seek in-kind contributions or partnerships relevant to the needs of DEPOt to facilitate its deployment at the lowest cost for the highest feature set in the interests of the community who will use it. This should include partnerships with compatible initiatives, perhaps to the extent of largely outsourcing DEPOt where that would best realize the intended outcome.[49]

47 See footnote 5.

48 See footnotes 12 (second bullet) and 46 for examples.

49 The Global Internet Policy Observatory proposed by the European Union being an example. See European Commission (2014). For a similar project see NETMundial's "Solutions Map" at www.netmundial.org/solutions-map.

Reporting

- Administrative and financial supervision: the director-general of the UN Office in Geneva
- Evaluation of operational effectiveness: the CC, through an annual review by the principals
- Input from stakeholders directly participating in digital policy issues: as decided by the CC from time to time

Additional reporting lines could be accommodated.

Funding

It is the usual practice for UN functions to be paid for by UN member states. While the DACS is administratively and financially within the UN system, it is inherently a public-private hybrid and not purely multilateral. Non-governmental funding should be facilitated and welcomed; ideally at least 50 percent of total funding should come from such sources. It is also essential that funding of any kind should avoid the appearance (or the reality) of undue influence on the DACS or its activities.

WORKS CITED

Dickinson, Samantha. 2014. "A Journey Can be More Important than the Destination: Reflecting on the CSTD Working Group on Enhanced Cooperation." In *Beyond NetMundial: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem*, edited by William J. Drake and Monroe Price, 66–70. www.global.asc.upenn.edu/app/uploads/2014/08/BeyondNETmundial_FINAL.pdf.

Drake, William J. and Lea Kaspar. 2014. "Institutionalizing the Clearing House Function." In *Beyond NetMundial: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem*, edited by William J. Drake and Monroe Price, 47–54. www.global.asc.upenn.edu/app/uploads/2014/08/BeyondNETmundial_FINAL.pdf.

Drake, William J. and Monroe Price, eds. 2014. *Beyond NetMundial: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem.* August. www.global.asc.upenn.edu/app/uploads/2014/08/BeyondNETmundial_FINAL.pdf.

Drezner, Daniel. 2001. "Globalization and Policy Convergence." *International Studies Review* 3 (1). www.danieldrezner.com/research/policyconvergence.pdf.

EURid and UN Educational, Scientific and Cultural Organization. 2011. "Internationalized Domain Names: State of Play" *.eu Insights*, May. www.eurid.eu/files/publ/insights_IDNs.pdf.

European Commission. 2014. "Feasibility Study on Using Automated Technologies to Support Policy-making." Digital Agenda for Europe: A Europe 2020 Initiative. http://ec.europa.eu/digital-agenda/en/news/feasibility-study-using-automated-technologies-support-policy-making.

Gjelten, Tom. 2010. "Shadow Wars: Debating Cyber 'Disarmament.'" *World Affairs Journal* (November/December). www.worldaffairsjournal.org/article/shadow-wars-debati.ng-cyber-disarmament.

ICANN. 2014. "Towards a Collaborative, Decentralized Internet Governance Ecosystem: Report by the Panel on Global Internet Cooperation and Governance Mechanisms." May. www.icann.org/en/system/files/files/collaborative-decentralized-ig-ecosystem-21may14-en.pdf.

ITU. 2014. "Key ICT Indicators for Developed and Developing Countries and the World (Totals and Penetration Rates)." ITU. www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/ITU_Key_2005-2014_ICT_data.xls.

Keohane, Robert O. and Joseph S. Nye, Jr. 1998. "Power and Interdependence in the Information Age." *Foreign Affairs* (September/October). www.foreignaffairs.com/articles/54395/robert-o-keohane-and-joseph-s-nye-jr/power-and-interdependence-in-the-information-age.

Kurbalija, Jovan. 2014. "Switzerland and Internet Governance: Issues, Actors, and Challenges." *Politorbis* 57: 51-52. www.eda.admin.ch/eda/en/fdfa/services-and-publications/publications.html/content/publikationen/en/eda/schweizer-aussenpolitik/reihe-politorbis/politorbis-57.

Lee-Makiyama, H. and R. Samarajiva. 2012. "Whither Global Rules for the Internet?" ECIPE Policy Briefs No. 12/2012. www.ecipe.org/media/publication_pdfs/PB201212b.pdf.

Lipsey, Richard, Kenneth Carlaw and Clifford Bekar. 2005. *Economic Transformations: General Purpose Technologies and Long-Term Economic Growth*. Cambridge, UK: Oxford University Press.

Rickard, W. 2009. "The Long Road to DNSSEC Depoyment." *IETF Journal* 5 (2): 12–15. September. www.internetsociety.org/sites/default/files/IETFJournal0502.pdf.

Rosenberg, Nathan and Manuel Trajtenberg. 2004. "A General-Purpose Technology at Work: The Corliss Steam Engine in the Late-Nineteenth-Century United States." *The Journal of Economic History* 64 (1): 61–99. doi:10.1017.S0022050704002608.

Schaller, Christian and Johannes Thimm. 2014. "Internet Governance and the ITU: Maintaining the Multistakeholder Approach." CFR.org, October 22. www.cfr.org/internet-policy/internet-governance-itu-maintaining-multistakeholder-approach/p33654.

UNCTAD. 2012. *Report of the Working Group on Improvements to the Internet Governance Forum.* A/67/65 (for UN General Assembly) and E/2012/48 (for UN Economic and Social Council). http://unctad.org/meetings/en/SessionalDocuments/a67d65_en.pdf.

———. 2014. "The Mapping of International Internet Public Policy Issues Database." UNCTAD: Intercessional Panel of the Commission on Science and Technology for Development. Prepared for the CTSD. http://unctad.org/meetings/en/SessionalDocuments/CSTD_2014_Mapping_InternetDatabase_en.pdf.

UN General Assembly. 1991. "Strengthening of the Coordination of Humanitarian Emergency Assistance of the United Nations." A/RES/46/182. December 19. www.un.org/Docs/journal/asp/ws.asp?m=A/RES/46/182.

vanGrasstek, Craig. 2013. "The History and Future of the World Trade Organisation." WTO. www.wto.org/english/res_e/booksp_e/historywto_e.pdf.

WhyGeneva.ch. 2015. "Geneva at a Glance." www.whygeneva.ch/media/ecowhygeneva/files/chapitre_1_ci_2014_2015.pdf.

WTO. 2014. "Communication by the United States: Work Programme on Electronic Commerce." JOB/SERV/196. November 27. WTO: Council on Trade in Services. https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=129292,128589,127204,126879,126078,124972,124185,119666,77941,92922&CurrentCatalogueIdIndex=0&FullTextSearch=.

Zettler, Angela. 2009. "NGO Participation at the United Nations: Barriers and Solutions." United Nations Internship Programme. http://csonet.org/content/documents/BarriersSolutions.pdf.

ABOUT THE AUTHOR

Nick Ashton-Hart is the senior permanent representative of the technology sector to the United Nations, its member states and the international organizations in Geneva. He has participated in multilateral policy development since 1992, been an active part of the Geneva community for 14 years and a resident for the past eight.

He came to international policy from private sector careers in both the entertainment and information and communications technology sectors. In the music industry, he managed some of the world's most successful and influential artists, including the "Godfather of Soul," James Brown. In the tech sector, he started as a systems administrator in the 1990s and finished up as a temporary chief information officer/chief technology officer five short years later, giving him broad hands-on technology experience.

He is currently executive director of the Internet & Digital Ecosystem Alliance (IDEA), a Swiss NGO with the mission to ensure that for-profit and not-for-profit Internet stakeholders have a voice in the multilateral policy community in Geneva. Geneva is home to 26 UN agencies and more than 50 percent of the international Internet policy meetings and processes that take place each year. Nick is the only person who participates across them in a representational capacity.

Prior to founding IDEA, he was Geneva Representative of the Computer & Communications Industry Association (CCIA), director for At-Large and senior director for participation and engagement, both with the Internet Corporation for Assigned Names and Numbers, and executive director of the International Music Managers Forum.

Nick's pro bono and advisory roles include: associate fellow of the Geneva Centre for Security Policy; senior fellow of the Diplo Foundation; member of e15Initiative Trade and Innovation Expert Group and Expert Group on the Digital Economy; member of the Evian Group@IMD Trade Task Force (www.imd.org/eviangroup/); and member of the board of directors for MetaBrainz Foundation, the corporate home of MusicBrainz (http://metabrainz.org/). He is also a featured blogger on CircleID (www.circleid.com/members/7172/) and can be found @nashtonhart on Twitter.

CHAPTER SEVEN:
GOVERNANCE OF INTERNATIONAL TRADE AND THE INTERNET: EXISTING AND EVOLVING REGULATORY SYSTEMS

Harsha Vardhana Singh, Ahmed Abdel-Latif and L. Lee Tuthill

ACRONYMS

ASCM	Agreement on Subsidies and Countervailing Measures
CTG	Council on Trade in Goods
FTAs	free trade agreements
GATS	General Agreement on Trade in Services
ICTs	information and communication technologies
IP	intellectual property
IPRs	intellectual property rights
ISPs	Internet service providers
ITU	International Telecommunication Union
KORUS	Korea–US (FTA)
MFN	most-favoured nation
OTT	over-the-top
PTAs	preferential trading agreements
SMEs	small and medium-sized enterprises
TBT	Technical Barriers to Trade
TISA	Trade in Services Agreement
TPP	Trans-Pacific Partnership
TRIPS	Trade-Related Aspects of Intellectual Property Rights
WIPO	World Intellectual Property Organization
WTO	World Trade Organization

INTRODUCTION

Until recently, policy makers and businesses did not adequately focus on the significant overlap between Internet and trade governance, but with a large and increasing presence of the Internet in global trade and investment, there is a growing interest in examining the synergy or conflict arising between these issues. There is a need to identify trade rules and practices that are sufficient to deal with emerging issues, and the new trade rules, modes of common understanding and cooperative mechanisms that would be required as the Internet becomes a larger part of the trade and investment domain.

An important part of this exercise is to examine the relevance and sufficiency of the regulatory provisions in the World Trade Organization (WTO) agreements as well as the emerging major free trade agreements such as the Trans-Pacific Partnership (TPP). This chapter discusses these aspects as well as the new trade-related concerns that need to be addressed, including the difficulty of determining jurisdiction and rules of origin, the classification of products and relevant disciplines applicable to them, complications arising for competition policy and regulatory practices due to bundling of products enabled by Internet and new communications technologies, some intellectual property rights (IPRs) issues, special assistance to small and medium-sized enterprises (SMEs), and a need for effective participation by the private sector in developing appropriate regulatory regimes.

The TPP provides an indication of certain trade-related measures and cooperative initiatives, but there is a need to go beyond that framework and develop a more comprehensive and participative regime that adequately addresses the issues arising due to the overlap between trade and Internet governance. Thus, the multilateral forum of the WTO needs to pay closer attention to these issues. The chapter suggests options ranging from soft to hard law that could be considered by the WTO in this context.

INTERSECTION OF TRADE AND INTERNET GOVERNANCE: KEY CHALLENGES

An intense and often controversial debate about Internet governance has taken place at the international level for more than a decade. During this time, however, the intersection between trade and Internet governance was not given significant attention.

This can be explained by several factors, but two are worth highlighting: On the one hand, the Internet governance community has long been arguing about the basic rules, principles and arrangements that should regulate the Internet; the interface with trade norms has received relatively little attention in this context. On the other hand, when the WTO was established in 1995, the Internet was still in its infancy. Subsequent to the launching of the WTO Work Programme on Electronic Commerce in 1998, the trade community then became absorbed with the Doha Round negotiations and, later, with efforts to overcome the stalemate in these negotiations, whose agenda is still dominated by the twentieth-century-era trade concerns prevalent when it was launched in 2001. These concerns largely focused on agricultural subsidies and tariffs on industrial goods.

Nevertheless, this situation is evolving rapidly with the changing nature of global trade flows. The large-scale diffusion of information and communication technologies (ICTs), the phenomenal development of the Internet and the extraordinary expansion of the digital economy are revolutionizing trade. According to a report by the McKinsey Global Institute (Manyika et al. 2014), "digital technologies are transforming global flows in three ways: through the creation of purely digital goods and services, 'digital wrappers' that enhance the value of physical flows, and digital platforms that facilitate cross-border production and exchange." The report points out that

"cross-border Internet traffic grew 18-fold between 2005 and 2012" and could further "increase eightfold by 2025" (ibid., 1 and 113). Cross-border e-commerce retailing has grown to account for more than 10 percent of trade in goods in less than a decade. At the same time, businesses are increasingly moving data across borders as an intrinsic part of their daily operations. Disruptive technologies — such as 3-D printing — are likely to have an even more significant impact on these production modes and trade flows, although the nature and extent of the impact is not yet entirely clear.

In this context, the trade community is taking a growing interest in the digital economy, beyond the narrower notions of e-commerce, and grappling with whether existing global trade rules are sufficient to support the expansion of global e-business and digital trade. The trade community is increasingly looking into whether new trade rules are needed and, if so, which ones. It is also becoming aware of the linkages with the broader Internet governance discussions. For its part, the Internet governance community is realizing that trade negotiations are not only about goods and services, but are also moving toward governing deeper regulatory issues extending beyond national borders, which include intellectual property, data protection, privacy and cross-border data flows. The Internet governance community is also interested in better understanding the WTO and trade governance more broadly, and in examining whether lessons could be drawn from trade rules for the ongoing discussions about Internet governance. These discussions focus on "the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet" (Working Group on Internet Governance 2005).

Thus, there is a pressing need to bridge the policy and knowledge gaps between the trade and Internet governance communities, and to foster a better understanding between them. Doing so could lead to identifying possible linkages and synergies, as well as to ensuring that normative developments in these two communities are mutually supportive and contribute to the overall goal of ensuring the open and participatory nature of the Internet, which underpins the digital economy. This chapter seeks to contribute to this objective by mapping issues at the intersection of trade and Internet governance.

Issues at the Nexus of International Trade and the Internet

The Internet is a vehicle or platform for sharing information and, increasingly, for promoting or concluding commercial transactions. Trade is the exchange of goods and services that the Internet platform facilitates in multiple ways.

The Internet being a general purpose technology, and an evolving one in terms of its use and technological complexities, its linkages across sectors and the scope of its use are increasing. Normally, trade involves the crossing of national borders by the product, producer or consumer. Today, goods trade is increasingly viewed in terms of value chains, with products crossing borders more than once, and with services and data flows playing a growing role in the operation of these value chains. Services trade is analyzed in terms of four modes of supply: border crossings by goods, consumers, commercial entities and persons supplying services. The Internet extends trade by allowing transfer of information, which then converts into intra-company operations, or sales to other producers or final consumers, including repair and maintenance services or facilitating supply chain operations. Although Internet-based trade is dealt within the General Agreement on Trade in Services (GATS), primarily in terms of mode 1 (i.e., cross-border supply of service), it can also concern establishment-related issues (such as commercial presence). It therefore raises a wide variety of issues linked with regulation of trade.

Another important point is that the Internet is not a chain, but rather a web. Thus, production and consumption of any particular service on the Internet could take place at any point or points within this web, and involve multiple participants and locations (countries) through activities that are either a direct part of the transactor or flanking support. This creates issues of jurisdiction, and a need for collecting relevant information, expanding the scope of existing regulations, developing new forms of trade regulation and addressing cross-jurisdictional issues through international cooperation. As mentioned by the World Economic Forum (2009, 6) in a publication on ICT: "The behaviors of networked economies are non-linear. They are marked by increased velocity, systemic interdependencies and hyper-personalization. In such a dynamic sector environment, it is essential to fully embrace the concept of innovation…such topics as open trade, effective competition, privacy, security and quality of service will all require innovative approaches and policy."

Tensions can often emerge between the objectives and policies underpinning trade regulation; for example, the goal of maintaining open trade versus the objectives of promoting privacy or security. The latter types of objectives are covered by WTO carve-outs under articles allowing for "general exceptions" and "security exceptions." However, many other regulatory policies not necessarily permitted under the WTO exceptions are in flux insofar as global and national governance of the Internet is concerned (see the following section on "Principles for Trade Regulation"). In the context of Internet policy, therefore, governments are faced with the need to address new situations arising from changes in technologies and business models, in some cases leading to a need to manage smooth transitions to a

new, more stable set of regulatory measures (for example, competition and pricing used by over-the-top [OTT] services).

When potentially WTO-inconsistent policies are adopted, trade governance takes into consideration whether the measures concerned are:

- specifically allowed or not under the WTO system for justifiable objectives;
- disguised forms of trade restrictions or deliberately creating anticompetitive situations in favour of domestic industry (for example, through certain localization requirements), and whether there are disciplines within the WTO to address them;
- unduly restrictive policies in terms of their effects (such as standards or taxation); and
- addressing some form of market failure or externality.

Such assessments can require consideration of how policies may or may not contribute to a level playing field, how best to address market failures and whether certain disciplines should be imposed on regulators or regulatory regimes to achieve the objectives of open trade under pro-competitive conditions.

Important questions in this context also include:

- Is it *feasible* to regulate the trade under consideration?
- Is it *necessary* to regulate?
- If it is necessary to regulate, is there a relatively less trade-restrictive manner to regulate it, and whether the regulation be mandatory or voluntary?
- In a transboundary environment, how can interoperability between national approaches in this area be achieved?
- Since some governments and industry players suggest industry self-regulation, when should rules be developed by the government or by industry itself?

Regarding the final point, additional issues would arise if industry were to self-regulate. For example, which industry body/bodies should be considered relevant for providing the appropriate regulatory framework, and even international standards, for operations? Also, to the extent that industry bodies establish international standards or codes of conduct, how might their work relate to that of relevant international institutions, such as the WTO, the International Telecommunication Union (ITU) or the World Intellectual Property Organization (WIPO)?

Principles for Trade Regulation

Trade regulation, as reflected in the WTO, has some established principles and disciplines. Due to the evolving nature of technology and products traded on the Net, some new issues are under consideration or are still a work in progress. Some others are yet to be considered in any meaningful way.

The structure of trade regulation in WTO includes:

- Most-favoured nation (MFN) treatment, national treatment, agreement to limit use of trade restrictions and possibility of deviating from the aforesaid binding principles, provided there are legitimate and justifiable reasons to do so (for example, environment, food security, natural resource depletion, unfair trade).
- Transparency and inquiry points, possible review of actions and changes in law/regulations, forums to address concerns regarding policies of other WTO members, and accountability of members through the committee processes and dispute settlement.
- Agreed-upon disciplines for addressing unfair trade, imports causing injury to domestic industry, and applying standards for reasons of health, safety, environment, national security, prevention of fraud and deceptive practices.

One of the most important issues that the Internet has raised in terms of trade governance relates to classification of Internet-enabled trade in goods and services. If a product is not unambiguously classified, then it is not clear which legal rules apply to that product. All governance, in terms of trade regulation, thus depends on classification. This is a major issue in the WTO for services, including for Internet-based services, because many of the most fundamental principles of trade are linked to whether a product is covered under the goods or the services agreements. Further, classification often determines whether or not a GATS commitment or General Agreement on Tariffs and Trade tariff concession has been taken on a particular product, and, if a dispute arises, which products would be the directly competing products affected. This aspect — i.e., the determination of "like products" — is of great significance in dispute settlement deliberations. This determination of "like product" is also required to assess whether or not WTO's non-discriminatory treatment provision is being violated and thus is crucial for the enforcement of MFN or national treatment obligations under the WTO.

Definition or classification of goods/services involves two distinct strains of analysis:

- One is to determine whether or not a product is a good or a service, because that will affect the disciplines applying to its trade, since trade rules in WTO differ

for goods and services. This complication arises because products whose trade previously required physical transportation (such as books, recorded music or films) can now also be traded digitally over the Internet via electronic access or downloads by the consumer. At present, there is no unanimity in the WTO as to whether such digital products are goods or services.

- The second classification issue is whether some of the services available over the Internet today are *new* services or an *existing* classified service being delivered through the Internet — i.e., is it simply a different way of delivering the same service. While existing services are already classified and may be subject to disciplines incorporated in the schedules of the GATS, a new service would need to be classified. In the WTO, how to determine whether a service is new or how to assign a classification is an issue under discussion and for which there is not yet a common view or conceptual solution.

With technological advances, the same technology can deliver more than one service — for example, radio, telephony, mobility, storage of information, education, films and medical services — which is described as a process of convergence of multiple services on the same technology platform. Convergence makes regulation difficult because the regulatory issues may not be the same across these different products. Convergence also implies that there would be multiple types of users, possibly creating additional regulatory issues to be addressed for a general purpose technology or platform. An important feature of the Internet as a general purpose technology is that it allows for a continuing enhanced possibility of convergence and multiple linkages. Thus, the scope and impact of existing policy considerations will keep expanding as new issues for regulation arise. These issues could include:

- Considering how to determine location of the exported product and thus the rules of origin. This issue could become quite complicated due to many different free trade agreements (FTAs) with dissimilar regulatory regimes that may differ across nations or even across product categories.

- Evolving business and pricing models are very different from traditional models for goods and services. Several products can be bundled together and it may be difficult to have a specific, predetermined, single price for any particular product in the bundle. Further, many Internet business models today gain revenue wholly or largely via advertising revenue rather than by charging the end consumer. For regulators, regulatory issues covering pricing and anticompetitive activities may become more difficult to determine in such situations where hitherto unconventional pricing mechanisms are used to cover costs and increase market presence. New business models make it easy to cross-subsidize, and make it difficult for the regulator to determine whether competitive conditions are being adversely affected. Further, with cross-subsidization or even "dumping" of a product, the combination of new pricing models and products with the possibility of significant bundling makes it difficult to determine the extent of the breach and to specify a remedy that will not go beyond the extent of the breach.

- Since the Internet and Internet-using technological developments allow for a growing convergence of activities, it is difficult to determine which regulations and/or trade commitments are relevant for the converged activities, and also whether new approaches are needed to address the issue. As mentioned above, with growing convergence, the Internet can be used to provide a variety of products and services. The key issue is how to regulate in cases where different types of products can be produced from the same source, and where one does not know the scope and limit of such sets of products or activities.

- Judging where to draw the line with regulatory intervention. Since it is sometimes technologically possible to bypass the regulatory safeguards, when is it necessary or cost-effective to continue to impose the same regulatory requirements on traditional business and trade, and how?

- Issues relating to personal data, privacy, security or managing social concerns assume a much larger dimension in view of the ubiquitousness of the Internet. Means to address these concerns may have positive or negative implications for the supply of services in general, as well as development options based on taking advantage of new technologies, and on foreign direct investment and technology transfer.

- Determining which IPR issues need to be addressed and the best way of doing so.

- Deciding how to manage issues that may arise with the possible changes in existing legal standards for work, as tasks such as home-based work become a larger component of the work force. This is especially important because Group of Seven countries are now emphasizing sustainable development and striving to implement social standards throughout the supply chain.

- Considering what are the ways that governments can achieve greater coherence with respect to regulatory principles or conditions that apply across different countries or different product categories as Internet technologies enable trade and value chains to become truly global.

- How to build trade-related information technology capacity in countries that have yet to catch up?

The European Union and the United States have emphasized a set of principles for ICT trade through a joint submission in the WTO (2011). The proposed principles include: transparency; open networks, network access and use; governments not preventing cross-border information flow; no restriction for infrastructure to be established locally or that local infrastructure should be used, nor preferential treatment to national suppliers of ICT; allowance of full foreign ownership; maximizing the availability and use of spectrum, in line with ITU recommendations where possible; legally distinct and functionally independent regulatory authorities; authorizing provision of competitive telecommunications services; ensuring interconnection on commercial terms; and international cooperation to increase the level of digital literacy globally.

Industry in large markets has also emphasized similar principles, as well as promotion of international standards, dialogues and best practices, and the need to address emerging legal and policy issues on the open nature of the Internet, security and privacy, and jurisdiction. Industry seeks to ensure that trade agreements cover all relevant aspects of digital trade in the future and also notes that developments on disciplines or common understanding could take place through various mechanisms, including bilateral, regional and multilateral trade agreements, or through development of a completely new treaty on digital goods, services and information flows.

THE WTO'S ROLE IN ADDRESSING THESE CHALLENGES

In large part, WTO discussions relating to e-commerce and Internet concerns have taken place under the auspices of the WTO Work Programme on Electronic Commerce, established in 1998 by trade ministers. The WTO Decision establishing the program adopted a wide-ranging definition to encompass all potentially relevant goods and services and any other issues that might arise in the WTO context: "Exclusively for the purposes of the work programme, and without prejudice to its outcome, the term 'electronic commerce' is understood to mean the production, distribution, marketing, sale or delivery of goods and services by electronic means" (WTO 1998, paragraph 1.3).

Thus the WTO's definition of "e-trade" covers anything from online sales of merchandise later delivered by post, to online hotel or plane reservations, to online sales of insurance policies, e-banking, and electronic reports by architects, engineers or consultants. It would also include promotional websites, Internet advertising, downloading of music or videos, long-distance medical diagnoses, online university courses or connection with foreign call centres for customer service inquiries. However, diverse views on many issues covered by the Work Programme on Electronic Commerce are yet to be resolved.

A number of WTO agreements become relevant in case of trade in goods resulting in commerce through the Internet. WTO e-commerce discussions on Internet-related trade have taken place under the General Council, the Council for Trade in Services, the Council for Trade in Goods (CTG), Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the Committee on Trade and Development. Further, WTO trade policy reviews cover some aspects of Internet trade under services. Other major efforts that have an impact on Internet-related trade and the use of the Internet are the two Information Technology Agreements, which open up trade for a large part of global trade in the ICT products identified in the agreed-upon lists.[1]

The TRIPS Agreement provides minimum intellectual property (IP) standards that all WTO members have agreed to apply and enforce. These standards may differ for groups of countries; for example, least developed countries most notably do not have the same applicable obligations under the agreement. Certain issues examined by the CTG include: market access conditions for products relating to e-commerce; customs valuation; import licensing; customs duties and other duties and charges; standards in relation to e-commerce; rules of origin; and tariff classification. The most relevant agreement is the GATS because a great many services are information-intensive and, hence, digitizable. For this reason, most of the in-depth discussions on Internet-related issues have taken place in the Council for Trade in Services.

GATS

A significant feature of the GATS disciplines is that all provisions of this agreement are relevant for the Internet — for example, MFNs, national treatment and market access provided under the four modes in the schedules of individual members; transparency provisions; dispute settlement, and possibility of discussing concerns within committees and the council.

In this context, it is also worth noting that most of the above-mentioned principles emphasized by the United States and the European Union for ICT are already covered by the framework of GATS disciplines.

A very useful document to guide the understanding on this issue is a progress report by the Council for Trade in Services on the Work Programme on Electronic Commerce, adopted by the WTO's General Council in 1999 (WTO 1999). This clarifies the scope of the GATS

1 For a summary discussion, see www.wto.org/english/thewto_e/minist_e/mc10_e/briefing_notes_e/brief_ita_e.htm.

provisions that are significant for the electronic delivery of services. These include MFN (Article II), transparency (Article III), increasing participation of developing countries (Article IV), domestic regulation, standards and recognitions (Articles VI and VII), competition (Articles VIII and IX), protection of privacy and public morals and the prevention of fraud (Article XIV), market access commitments on electronic supply of services (Article XVI), national treatment (Article XVII), and access to and use of public telecommunications transport networks and services (Annex on Telecommunications).

Importantly, issues relating to anticompetitive activities or discriminatory access could be addressed through the GATS Annex on Telecommunications, and the principles in the WTO Reference Paper on telecommunications (WTO 1996). This paper is the basis of disciplines committed in the schedules notified by many WTO members on addressing good regulatory practice and anticompetitive practices. The first paragraph of GATS Article VI on domestic regulation is also pertinent: "In sectors where specific commitments are undertaken, each Member shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner."

Additional insight into Internet-related services is also provided by the WTO's dispute settlement panel and Appellate Body reports of the WTO. In 2000, the United States brought a dispute pertaining to the telecom-related regulatory practices of Mexico, which *inter alia* also affected Internet services (WTO 2004a has the Panel Report). In fact, most GATS-related dispute settlement cases have involved online or networked services. For example, the case brought by Antigua and Barbuda against the United States concerned gambling services provided over the Internet (WTO 2004b, 2005). Two important disputes relating to China litigated, respectively, an element related to online music downloads (WTO 2009a; 2009b), and electronic payment services (WTO 2012). Panel findings have confirmed that GATS disciplines and commitments apply to services supplied electronically. The panel report in WTO (2004b), for example, found that supply of a service through mode 1 includes all means of delivery (including the Internet). In one excerpt, the panel summed up this view, saying,

> we conclude that mode 1 includes all means of delivery. We are of the view that when a Member inscribes the word "None" in the market access column of its schedule for mode 1, it commits itself not to maintain measures which prohibit the use of one, several or all means of delivery under mode 1 in a committed sector or sub-sector. This is especially so in sectors and sub-sectors where cross-border supply is affected essentially if not exclusively through the Internet. (Ibid., paragraph 6.287)

In WTO (2009a, paragraph 7.1209), the panel found that the scope of China's commitment in its GATS schedule on "sound recording distribution services" extends to sound recordings distributed in non-physical form, through technologies such as the Internet.

A closer look at the WTO framework of disciplines in the area of services does, however, suggest three gaps:

- First, although the framework of disciplines exists, substantive content of disciplines or interpretative tools need to be developed through further negotiations to enable that framework to specifically address many of the concerns.
- Second, the framework itself is lacking in terms of having not yet developed disciplines in areas such as subsidies, safeguards and government procurement.
- Third, the complex and constantly evolving nature of Internet-based transactions, together with new business models, creates conditions where enduring trade disciplines may become difficult both to devise and to implement. In this situation, either new forms of trade disciplines may need to be developed, or some enhanced forms of international cooperation would be needed to address overlapping new issues.

TRIPS

The WTO Council for TRIPS has discussed IPRs and the Internet, but its discussions did not yield concrete results. When the WTO Work Programme on Electronic Commerce was adopted in 1998 (WTO Document WT/L/274), the TRIPS Council was requested to "examine and report on the intellectual property issues arising in connection with electronic commerce," including "protection and enforcement of copyright and related rights; protection and enforcement of trademarks," and "new technologies and access to technology" (WTO 1998, paragraph 4.1). E-commerce was addressed by the council as a standing item on its agenda from 1998 to 2003; however, the council's discussions were largely inconclusive and no specific follow-up actions emerged. The need for further study to understand the issues involved was highlighted in some of the reports of the TRIPS Council to the WTO General Council.

In addition to the lack of consensus in discussions at the TRIPS Council, large copyright-based industries and many industrialized countries considered TRIPS' provisions to be inadequate and insufficient to address violations of IPRs in the digital environment. The elaboration of more effective norms for this purpose was pursued in a number of other forums and venues.

In 1996, WIPO adopted the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty, known together as the Internet Treaties. The Copyright Treaty updates the Berne Convention and provides further extensions to distribution and rental rights, as well as including rights for interactive downloading and for the distribution of copies and protection against the circumvention of technology measures. The Performances and Phonograms Treaty refines the Rome Convention and provides an updated set of international rights for performers and record producers. The treaty effectively updates the Rome Convention to accommodate certain forms of interactive downloading and distribution, as well as protection against the circumvention of technical protection measures.

These treaties were implemented in the United States by the Digital Millennium Copyright Act (1998) and in the European Union by the Copyright Directive (2001). Both the United States and the European Union have proposed to incorporate the key provisions of the WIPO Internet Treaties into the TRIPS Agreement, but this proposal did not garner broad support when it was tabled at the TRIPS Council.

Apart from WIPO, "TRIPS Plus" provisions — which go beyond the minimum standards of the WTO TRIPS Agreement — have been incorporated in many bilateral, regional and plurilateral trade agreements for the purpose of achieving more effective IPR enforcement in the digital environment. This was also one of the key objectives of the Anti-Counterfeiting Trade Agreement, which was ultimately rejected by the European Parliament in 2012.

Ultimately, the TRIPS Council can again take up the discussion on IPRs and the Internet if it wishes. According to Article 71 (1) of the WTO TRIPS Agreement, the Council "may also undertake reviews in the light of any relevant new developments which might warrant modification or amendment of this Agreement." Given that more than a decade has elapsed since the TRIPS Council discussed these issues, it might be time to revisit them in light of the drastic changes in the digital economy described above and the new studies and empirical evidence available since then. This could be one of the items to discuss at WTO; the WTO's 2015 Ministerial Declaration at Nairobi, stated that new issues may be raised for discussion.[2]

Finally, one aspect of the TRIPS-related WTO regime that can impact IP protection on the Internet, and which is often overlooked, is the exercise of cross-retaliation involving TRIPS. The WTO Dispute Settlement Understanding contemplates the possibility for WTO members to suspend concessions in the field of TRIPS to redress an injury suffered with respect to trade in goods or services. WTO arbitrators have thus far approved TRIPS cross-retaliation on three occasions: in favour of Ecuador against the European Communities, of Antigua against the United States, and of Brazil against the United States. In 2013, the WTO awarded Antigua the right to impose annual sanctions worth US$21 million against US patents, copyrights, trademarks and other IPRs. News reports indicated that Antigua was considering setting up a website to sell US copyrighted movies and songs, but the move ultimately did not materialize.

The WTO's Future Role in Governance of Internet

The WTO concept of standards, as captured in the WTO's Technical Barriers to Trade Agreement (TBT), was established in a pre-globalization and pre-digital era and does not adequately take into account the open standards that have been developed by globally open communities. There is a possibility of bringing in these standards bodies within the WTO system through observership in meetings, informal meetings or other appropriate means. This is important because the development and evolution of technologies on which the Internet is based exemplifies the success of this bottom-up, globally open, market-driven system of standardization.

It thus needs to be examined whether there is a need for the WTO to update its concepts and definitions of standards, and the underlying processes, to the twenty-first-century reality so as to encompass more inclusiveness and openness in an era of global challenges that require increased innovation. This can be realized through an explicit acknowledgement by the WTO of the value of the standards-setting and developing bodies that follow a globally open, market-driven paradigm (Karachalios and McCabe 2013). Analysis of the TBT Agreement might show that it is congruent with the relevant principles of, for example, the Internet Engineering Task Force. Clarity on this aspect, however, including application to the area of services, would help limit potential uncertainty relating to the Internet.

Lessons from WTO Governance for Internet Governance

The WTO regime encompasses a number of useful rules, mechanisms and arrangements that could be worthwhile to consider in the context of Internet governance and are relevant in the context of Internet- and trade-related developments. These include:

- **Binding principles:** An established set of principles and disciplines for "good governance," such as non-discrimination and technological neutrality.

2 The Ministerial Declaration states: "While we concur that officials should prioritize work where results have not yet been achieved, some wish to identify and discuss other issues for negotiation; others do not. Any decision to launch negotiations multilaterally on such issues would need to be agreed by all Members" (WTO 2015, paragraph 34).

- **Transparency:** It is imperative that trade regulations and policies are transparent so individuals and companies involved in trade can know as much as possible about the conditions of trade. To achieve this, governments have to inform the WTO and other members of specific measures, policies or laws through regular "notifications." The WTO conducts regular reviews of individual countries' trade policies — the trade policy review — with the objectives of increasing transparency and understanding of countries' trade policies and practices through regular monitoring, and improving the quality of public and intergovernmental understanding of these policies and practices. Finally, deliberations at different WTO bodies and the availability of the minutes of such deliberations contribute to this objective of transparency.

- **Policy flexibility:** The ability to meet legitimate policy objectives even if the policy required for this purpose is contrary to the primary rules. Thus, flexibility is provided in WTO, subject to specific disciplines, including the criteria of necessity and meeting the relevant conditions (Articles XIV and XIV bis of GATS). The types of conditions under which flexibilities are allowed reduce the scope for discrimination or disguised form of protectionism. Further, they provide a predictable and agreed basis to address two different types of issues: those relating to governance *on* the Internet — limiting and controlling what goes on online — and governance *of* the Internet — regulating the operation of the physical infrastructure of the system.

- **Mechanisms for exchange of information:** Enquiry points and committees for discussing trade-related concerns.

- **Cooperation and mutual support:** Governments identify issues that cannot be addressed adequately by any single government or jurisdiction, but rather need several governments that cooperate or collaborate to establish mutually supportive systems. Similar systems are also used to provide capacity improvement possibilities for those who require them to come up to a more informed and efficient level of performance.

- **Coherence:** Regulatory policies are not always the same across countries, and differences in them could cause difficulties in connecting markets, for example, difference in encryption laws or addressing competition or certain public policy-related issues. The WTO provisions give a basis for greater coherence among such differences in the content of relevant policies.

- **Dispute settlement:** An established body of judicial decisions that provides greater certainty to trade policy governance.

However, as mentioned above, there are three types of gaps to be addressed in making WTO governance more effective. The architecture of GATS is flexible and anything could be negotiated within the framework by limited groups or by all WTO members. Nonetheless, such discussions are currently not yielding results within the WTO, with the stalemate in Doha Round negotiations creating a trust deficit among members. Thus, negotiations on the Trade in Services Agreement (TISA) are being held using the GATS framework, but as a plurilateral outside the WTO.

There may be a possibility, however, to consider certain categories of steps ranging from "soft" to "hard" agreements among WTO members. Based on the discussion above, these could include the following options:

- Form a platform to exchange views on digital trade and governance for discussions between government and business, with track-two initiatives among major stakeholders included in the process.

- Examine the implication of Internet-based trade requiring coherent policies in multiple sectors. This could be part of the continuing program on e-commerce under the GATS, with a wider mandate to discuss important service sectors.

- Examine how some industries, such as finance, have dealt with local hosting requirements.

- Examine how the principles of WTO's TBT Code of Good Practices can be applied to reduce regulatory uncertainty for Internet-based trade. A number of private standards bodies have accepted these principles and notified the WTO as well. This could be done by all the relevant standards bodies pertaining to the Internet.

- Examine how "good offices" by the chairperson of a committee or the director general could be used to address concerns of all parties.

- Add information to the existing WTO trade databases on measures affecting digital trade so that the factual basis could become clearer for policy makers.

- Develop voluntary guidelines or codes of conduct on important digital trade issues, for example, focusing on best practice or means of addressing concerns such as privacy, security, jurisdictional issues, etc.

- The growth of supply chains has led to a trade facilitation agreement to deal with a number of customs matters within the WTO. The interlinked and complex nature of the Internet would suggest a need to go beyond that and consider whether some agreement could be made on facilitation of Internet-based trade.

Five currently promising areas that cut across different WTO committees or councils are:

- Discussion on SMEs, a topic which has been emphasized in more than one WTO committee. In such discussions, members could share experience on e-commerce success cases, particularly with respect to SMEs. To some degree, such exchanges have been featured in e-commerce seminars held by the Committee on Trade and Development and the Services Council. The latter has recently approved information exchange as an e-commerce agenda item for its meetings that will focus on SMEs, among other issues of members' choosing. Such discussion could be generalized across the WTO within its bodies more widely. Enhanced discussions could also address some of the regulatory issues affecting SMEs, which often have crosscutting relevance for all enterprises.

- Sharing information on the experience of individual WTO members about their efforts at policy coherence and regulatory initiatives designed to address digital trade. Sharing of experience is an established practice in WTO bodies. For instance, Chinese Taipei tabled a paper in the WTO's Council for Trade in Services where it presented its data protection legislation and opened the discussion among members on this issue.

- The increasing overlap between goods and services and the impact of new technologies on conventional concepts of trade regulation — such as rules of origin, unfair trade, application of the four modes of supply (currently only in GATS) to trade in goods — and a possible need to examine the sufficiency of safeguards mechanisms for goods with Internet-based trade allowing easy shift in location.

- Identifying the specific requirements for least developed countries and other economies in terms of upgrading their capacities for digital trade and the possibility of prioritizing the relevant policy response.

- Improved data collection, both within the WTO and interagency groups, so as to clarify specific issues and create a better basis for policy consideration. This exercise is ongoing, and closer attention could be given to issues arising with respect to digital trade.

In general, these suggestions largely do not focus on negotiations of new disciplines because the conditions for doing so in the WTO are not presently encouraging. However, negotiations in FTAs are ongoing on and many Internet-related concerns are part of the issues being addressed there. Some of these are mentioned below.

It is quite possible that some of the softer topics, including initiation of more substantive discussions unlinked to negotiations, may not easily yield tangible results in the WTO. Therefore, WTO efforts need to be supplemented by more coordinated outside work — for example, by academic or research institutes in both developed and developing countries — that can be widely shared with trade and Internet governance communities. One avenue of useful research might be to focus on the kinds of regulatory guidelines and codes of conduct needed to facilitate the smooth functioning of the Internet as a trade highway, as well as possible means of securing barrier-free Internet-enabled trade.

Other examples of issues that have yet to be dealt with include: addressing concerns on jurisdiction and liability; clarifying the classification of new services that arise, for example, in social media or various OTT services and mobile apps; and considering whether investment or competition policy-related provisions or agreements could provide a basis for a wider set of relevant disciplines on digital trade. It also remains to be seen whether it will be possible for some of the e-commerce provisions in plurilaterals to be brought into the WTO through scheduling or other means.

DEVELOPING PROVISIONS FOR INTERNET TRADE GOVERNANCE: TISA AND TPP

Increasingly, regional and plurilateral trade agreements are addressing e-commerce and digital matters, such as cross-border data flows and IPR enforcement in the digital environment. For instance, the 2011 Korea–US FTA (KORUS) was the first international treaty to include rules on cross-border data flows. However, to the chagrin of the private sector, the provision only requires that parties should "*endeavor* to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders" (emphasis added) and is not more strongly worded in terms of its mandatory nature.

Among the mega-regionals, negotiations of the TPP have concluded and TISA is the most advanced. The TISA negotiations are being held under secrecy, but indications about the content of its chapter on e-commerce are available online. Considering the issues being addressed in TISA, we can see the areas where higher disciplines will be developed. These include movement of information or cross-border information flows, online consumer protection, personal information protection, unsolicited commercial electronic communications, transfer of access to secure code, interoperability, open networks, network access and use, local infrastructure/local presence, electronic authentication and electronic signatures, customs duties on electronic deliveries, international cooperation and security exceptions. Given the major importance of the United States in both TPP and TISA, and the fact that the concerns of another large economy in TISA, i.e., the European Union, are similar to those of the United States, the results of the TPP on electronic commerce give a good

indication of the likely evolution of disciplines in this area within TISA.

TPP and E-commerce

Conditions affecting digital trade can be found in several parts of the TPP, such as the services-related chapters on cross-border trade in services, financial services, temporary entry for business persons, telecommunications and e-commerce.[3] Of course, the provisions relating to goods also impact Internet-based commerce since international supply chains comprise both goods and services, including the use of Internet-based services.

Provisions relating to telecommunications are very significan for Internet because they affect the conditions for access and use of the network for providing Internet services. The most evident impact, however, is through the provisions relating to e-commerce (see below). In addition, as discussed earlier in this chapter, the IPR-related provisions are also important (see the following section on "TPP and IPRs").

Chapter 14 of the TPP[4] contains provisions specifically relating to e-commerce. They cover several issues, such as:

- no customs duties, fees or other charges on digital products;[5]
- establishing certainty of market conditions in terms of the principle of non-discrimination generally applying to e-commerce;
- avoiding any unnecessary regulatory burden on electronic transmissions;
- facilitating electronic authentication and electronic signatures;
- facilitating use of cloud-computing services;
- protection of personal information;
- online consumer protection, including means for consumer redress and building consumer confidence, and allowing cross-border transfer of information by electronic means, including personal information, when the activity is for the conduct of business (this is not binding if the government needs to use a policy for legitimate public policy objectives, subject to the policy meeting certain conditions[6]);
- members do not require location of computing facilities in another member's territory as a condition for conducting business in that territory;
- interconnection charge sharing;
- addressing unsolicited commercial electronic messages;
- cooperation among the members of the TPP Agreement on sharing experiences,[7] exchanging information, assisting SMEs to overcome obstacles, encouraging self-regulation by the private sector and building capabilities to address cyber-security matters;
- prohibition, with limited justifiable exceptions, on requiring the transfer of, or access to, software source code as a condition for the import, distribution, sale or use of such software or products containing such software in the TPP member's territory;
- when a TPP country requires assurance that information technology equipment complies with a technical regulation or standard for electromagnetic compatibility, the requirement is that the TPP member accept a supplier's declaration of conformity with the specified standard or technical regulation for unintentional electromagnetic disturbances with respect to any other device or system in that environment;[8] and
- e-commerce provisions being subject to dispute settlement.

It is noteworthy that several of the principles emphasized by the European Union and the United States in their above-mentioned submission to the WTO have been addressed by the TPP, an agreement whose members account for about 40 percent of global GDP and about one-quarter of world trade.

3 For the text of the TPP's chapter 14 on electronic commerce, see www.mfat.govt.nz/en/about-us/who-we-are/treaty-making-process/trans-pacific-partnership-tpp/text-of-the-trans-pacific-partnership/.

4 As in other parts of the TPP Agreement, this chapter also has some exceptions to the disciplines agreed in general.

5 In the WTO, the decision on imposing no duty on e-commerce is validated by the ministers at each WTO Ministerial Meeting, and remains in force only until the subsequent meeting.

6 The policy should not be applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade, and should not impose restrictions on transfers of information greater than are required to achieve the objective.

7 The list of topics for exchanging information and sharing experiences is open ended, but the TPP text specifically mentions: personal information protection; online consumer protection, including means for consumer redress and building consumer confidence; unsolicited commercial electronic messages; security in electronic communications; authentication; e-government; and consumer access to products and services offered online among the members of TPP.

8 This provision is in Section B of the TPP's chapter on TBT.

TPP and IPRs

Following the model of previous FTAs concluded by the United States, particularly KORUS, the TPP has strong IP and enforcement provisions in the digital environment.

Chapter 18 of the TPP includes several provisions that pertain to Internet-related transactions. Transparency provisions specifically mention the Internet as a means of providing information to the public. Article 18.28 provides disciplines relating to country code top-level domain names. Section J in the chapter specifically addresses Internet service providers (ISPs) and includes a number of provisions on legal remedies and safe harbours, including several connected with copyright infringement. The digital environment is mentioned in several places, and the Internet is covered through the use of terms such as "transmission to the public by any medium" (New Zealand Foreign Affairs & Trade 2016, article 18.57) or "by wire or wireless means" (ibid., articles 18.59; 18.62). This enhances the scope of the IPR provisions to include services provided through the Internet. In this context, two aspects of the TPP are especially noteworthy:

- Strengthened technological protection measures: Article 18.68 of the TPP provides for a strengthened set of provisions compared to earlier preferential trading agreements (PTAs), but along the lines of KORUS, to avoid the circumvention of technological protection measures that authors, performers and producers of phonograms may use in connection with the exercise of their rights in order to protect the unauthorized use of their works.

- Detailed provisions on liability for ISPs: Such provisions entail incentives for ISPs to cooperate with copyright owners in deterring any unauthorized storage and transmission of copyrighted materials (ibid., article 18.82.1[a]). They also limit the scope of remedies that may be available against online service providers for copyright infringements that they do not control and take place through systems or networks controlled or operated by services providers (articles 18.82.1[b], 18.82.2).

Regarding strengthened technological protection, WTO TRIPS Plus provisions have long attracted criticism from civil society groups for their potentially negative effects on access to knowledge and the broad dissemination of information in the digital environment. Emphasized by the United States, article 18.66 of the TPP — a new provision that does not feature in previous US PTAs — relates to limitations and exceptions to copyright:

> Each Party shall endeavor to achieve an appropriate balance in its copyright and related rights system, among other things by means of limitations or exceptions that are consistent with Article 18.65 (Limitations and Exceptions), including those for the digital environment, giving due consideration to legitimate purposes such as, but not limited to: criticism; comment; news reporting; teaching, scholarship, research, and other similar purposes; and facilitating access to published works for persons who are blind, visually impaired or otherwise print disabled.

The US press release on this matter in 2012 elaborated on how US consumers and businesses rely on a range of exceptions and limitations, such as fair use, in their businesses and daily lives and mentions specifically that under its Digital Millennium Copyright Act, the United States provides "safe harbors limiting copyright liability, which help to ensure that legitimate providers of cloud computing, user-generated content sites, and a host of other Internet-related services who act responsibly can thrive online."[9] The objective is to achieve an appropriate balance between IP protection measures and dissemination of knowledge and information, but such IPR provisions will likely remain a source of tension in trade and IP governance arrangements in the digital economy.[10]

ENHANCING SME TRADE AND INVESTMENT: SPECIFIC RULES AND REGULATIONS

Provisions relevant to SMEs would need to address the specific shortcomings or difficulties faced by SMEs. These could include technical assistance for SMEs, or introducing certain flexibilities in the form of exceptions to certain disciplines that are perceived as creating obstacles to their participation in trade. Examples include the kind of SME support policies that are in the TPP, that are envisaged in the Transatlantic Trade and Investment Partnership and the provision in footnote 2 of the WTO Agreement on Subsidies and Countervailing Measures (ASCM).[11] Two major constraints faced by SMEs are finance and market

9 This was the first time that the United States sought to include such provision in an FTA. See https://ustr.gov/about-us/policy-offices/press-office/blog/2012/july/ustr-introduces-new-copyright-exceptions-limitations-provision.

10 Internet intermediaries such as ISPs and Internet platforms are particularly keen not to see the "safe harbor" and limited liability provisions they have enjoyed under the Copyright Act be undermined by overly broad IP rules in trade agreements that increase transaction costs and risks for their operations.

11 Under this footnote, subsidy support provided *inter alia* to SMEs would be outside the scope of the disciplines specified by the ASCM because such subsidies would not be considered "specific" subsidies. The subsidy disciplines of the ASCM exempt subsidies that are not specific. It is noteworthy that the GATS does not have any disciplines on subsidies.

information. While financial support would require specific initiatives, market information could be made available together with developing policy coherence in different jurisdictions.

In today's global markets with supply chains and lead firms, it is very important to develop capabilities for meeting international standards. There are two types of standards to consider in this context, namely product standards and process standards. The latter also increase efficiency. There may be a need to emulate and learn from certain existing programs aimed at enhancing the capacities of SMEs. One example is a modular approach to improve capacities of SMEs, focused on incremental and step-wise improvement in a standards-related capacity of the firm. This training, after completing the fourth or fifth module of incremental training, would enable the enterprise to meet international standards.[12] Another example is a recent program in Rwanda, where the existing links with local supply chains are being strengthened by training enterprises to meet standards that are required by the importers in their key export markets. This program includes developing better links and commercial connections with regional value chains to export the "regionally produced products" to major global markets.

Many SMEs operating in new technology areas are relatively efficient and provide niche products for the market. Others, however, need to identify segments of the value chain where their entry is most feasible and efficient. Links to supply chains depend on market information, timely policy facilitation and the creation of hubs for small-scale industry to link up or operate with others that are connected in the value chain through forward and backward linkages.

Another aspect of assisting SMEs is to enable them to climb up the value chain and produce higher value-added products. This requires specific training and skill generation, and collaborative dialogue between industry and government. An important supplementary process could include training programs conducted by private industry to better link up with markets and meet the relevant standards. In this regard, it is also useful to consider the provisions on supporting SMEs, which are now part of the TPP, primarily in chapter 24, as well as some other chapters, such as that on e-commerce.

It is also important to supplement the above-mentioned efforts by collecting and disseminating information on examples of success cases of SMEs using Internet-based business opportunities. This could be done at the national level or even at the regional level, including by establishing a permanent platform for this purpose.

CONCLUSION

The futures of the multilateral trading system and Internet governance are at critical crossroads. Governance arrangements in both areas aim to maintain openness and avoid a drift toward national measures that might unduly restrict global trade and digital flows, leading to fragmentation and balkanization of the markets of these global public goods. There is thus much at stake, and it is extremely important to develop a more coordinated dialogue and interaction between trade governance and Internet governance as they seek to achieve their common objectives. There is also much that each community can learn from one another regarding the way norms, procedures and decision making have developed in their respective areas.

This said, trade governance is more established and more institutionally mature than Internet governance, as reflected in the WTO regime and the FTAs with their set of treaties, soft norms and dispute settlement mechanisms. The growing importance of digital trade for global trade makes it imperative for the WTO to consider how to best address it, and a number of suggestions have been made in the chapter for this purpose. In the meantime, the scope for norm setting and institutional innovation on these issues seems greater in FTAs, especially in the plurilaterals such as the TPP and TISA. Nonetheless, it is still possible to consider several initiatives within the WTO, including some which are part of recently concluded mega-regional FTAs.

In this context, it is also important for the trade community not to lose sight of the broader trends and developments occurring in the context of the Internet governance arrangements and of the possible implications of trade-related negotiations and measures on such frameworks. It will also be incumbent on the Internet governance community to improve its understanding of key trade principles and disciplines, to ensure that their efforts are consistent with, and mutually supportive of, trade governance affecting the Internet.

ACKNOWLEDGEMENTS

The views expressed in this chapter should not be ascribed to any other person or to any organization. The authors are grateful to an anonymous referee for comments to improve the discussion in the chapter.

12 An example is the ZED training module of the Quality Council of India, aimed specifically at SMEs.

WORKS CITED

Karachalios, Konstantinos and Karen McCabe. 2013. "Standards, Innovation and their Role in the Context of the World Trade Organization." E15 Think Piece. Geneva: International Centre for Trade and Sustainable Development and World Economic Forum.

Manyika, James, Jacques Bughin, Susan Lund, Olivia Nottebohm, David Poulter, Sebastian Jouch and Sree Ramaswamy. 2014. *Global flows in a digital age: How trade, finance, people, and data connect the world economy.* McKinsey Global Institute, April.

New Zealand Foreign Affairs & Trade. 2016. *Trans-Pacific Partnership Agreement*. www.mfat.govt.nz/assets/_securedfiles/Trans-Pacific-Partnership/Text/18.-Intellectual-Property.pdf.

Working Group on Internet Governance. 2005. *Report of the Working Group on Internet Governance*, June. www.wgig.org/docs/WGIGREPORT.pdf.

World Economic Forum. 2009. *ICT for Economic Growth: A Dynamic Ecosystem Driving The Global Recovery.* Geneva: World Economic Forum. www3.weforum.org/docs/WEF_IT_DynamicEcosystem_Report_2009.pdf.

WTO. 1996. "Negotiating group on basic telecommunications." Telecommunications Services Reference Paper, April 24. www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm.

———. 1998. "Work Programme on Electronic Commerce." Document WT/L/274, September 30.

———. 1999. "Work Programme on Electronic Commerce. Progress Report to the General Council." Document S/L/74, July 27.

———. 2004a. "Mexico — Measures Affecting Telecommunications Services." Document WT/DS204/R, April 2.

———. 2004b. "United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services." Report of the Panel Document WT/DS285/R, November 10.

———. 2005. "United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services." Report of the Appellate Body Document WT/DS285/AB/R, April 7.

———. 2009a. "China — Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products." Document WT/DS363/R, August 12.

———. 2009b. "China — Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products." Report of the Appellate Body Document WT/DS363/AB/R, December 21.

———. 2011. "Contribution to the Work Programme on Electronic Commerce." Document S/C/W/338, July 13.

———. 2012. "China — Certain Measures Affecting Electronic Payment Services." Document WT/DS413/R, July 16.

———. 2015. *Nairobi Ministerial Declaration*. Adopted on December 19. Document WT/MIN(15)/DEC, December 21.

ABOUT THE AUTHORS

Harsha Vardhana Singh is a senior associate of the International Centre for Trade and Sustainable Development, and a senior fellow of the International Institute for Sustainable Development.

Ahmed Abdel-Latif is a special assistant for policy and programme in the Office of the Director General for the International Renewable Energy Agency.

L. Lee Tuthill is a counsellor in the Trade in Services Division of the World Trade Organization.

CHAPTER EIGHT:
CYBER SECURITY AND CYBER RESILIENCE IN EAST AFRICA

Iginio Gagliardone and Nanjira Sambuli

INTRODUCTION

Over the last few years, cyber security has gone from a concern that loomed large in the future for East Africa to an issue of pressing importance. In Kenya — one of Africa's largest economies and East Africa's central tech hub — it is estimated that cybercrimes cost the country more than 2 billion Kenyan shillings (US$22.56 million) in 2013 (Otieno 2014).

The increasing awareness of the need to address cyber-security threats in Africa, however, has also reproduced old clichés about gaps between the continent and more advanced areas of the globe. The few reports available on cyber security in Africa have been characterized by alarmist tones, asking, for example, whether Africa has become "a new safe harbor for cybercriminals" (Kharouni 2013). They have, however, offered very thin empirical evidence that Africa is any more dangerous than other continents and, in many cases, have been sponsored by cyber security firms with vested interests (Jackson 2015). From a different angle, the increasing presence of Chinese telecom companies in Africa has led to allegations that these companies may be hiding "backdoors" in their equipment to allow the Chinese government to spy on users, including African citizens, or to shield its own spying efforts elsewhere (Protalinski 2012). Recent leaks from the former US National Security Agency (NSA) contractor Edward Snowden, which revealed that the NSA itself tried to install backdoors in equipment produced by Huawei, China's largest IT company, have given such accusations an ironic twist. As Thomas Rid (2014) succinctly put it, "there is now more publicly available evidence that the [US] NSA exploited Huawei than there is public evidence that shows the PLA [People's Liberation Army] or other Chinese agencies did so."

This chapter, while recognizing the threats posed by cyber security in East Africa and highlighting some fragilities and contradictions of the measures developed to date, focuses on the specific challenges that have followed the contours of East Africa's distinctive digital cultures. Mobile phone banking innovations have facilitated greater flows of currency and increased chances for skimming these transactions (Harris, Goodman and Traynor 2013; Herbling 2014). Remittance-based economies have presented opportunities for cyber attacks on the banking institutions that facilitate these transfers (Mukinda 2014; Quarshie 2012). Terrorist threats, in particular from the Islamist group al-Shabaab, have stressed the need to respond to militants employing digital media to further their cause (Kagwanja and Karanja 2014), but also to reflect on the possibility that the increasing securitization of domestic and international politics may require costly trade-offs with individual and collective freedoms, and offer excessive powers to executive bodies in the absence of adequate checks and balances (Makulilo 2012).

Through three case studies focusing on Kenya, Ethiopia and Somalia, national responses are connected to continental and global efforts to reinforce cyber security. These case studies offer the opportunity to understand how three neighbouring countries that have developed very different notions of their national information societies have elaborated distinctive responses to a similar challenge.

Kenya, given its ambition to emerge as East Africa's leading information and communications technology (ICT) innovator, has made the most effort to respond to cyber security threats. *Emulating* countries that have similarly emerged at the forefront of the information revolution, Kenya has made strides to adopt internationally recognized standards, seeking to offer a sense of readiness to withstand cyber attacks. By doing so, however, Kenya has also created high expectations about its ability to adequately respond to growing risks, and will have to invest significant resources to live up to them.

Ethiopia, while similarly showing adherence to international standards, as displayed by its draft cyber security law, which incorporates many of the provisions in the Council of Europe Convention on Cybercrime, appears more exposed to the risk that the cyber security agenda could be exploited politically to further domestic goals. As the precedent of the Anti-Terrorism Proclamation analyzed below illustrates, the Ethiopian government has often relied on *extraversion* to achieve its goals, turning its unequal relations with the international environment in its own favour, and furthering its own agenda while giving the impression of responding to international calls.

Finally, the case of Somalia, or the Somali territories,[1] offers an example of how solutions may emerge through *enculturation*, relying on local knowledge to address global threats. As explained later, in the absence of a functioning state, customary law has been employed to ensure that people get compensated in cases of fraud perpetrated through mobile phones or has offered a response when sensitive data are released by mistake in the public domain.

These three mechanisms — emulation, extraversion and enculturation — are not mutually exclusive. On the contrary, while each of the countries surveyed displays one of them to a greater extent, these mechanisms can be found in all three countries to varying degrees. Approaching the analysis of cyber resilience through these lenses is meant to offer greater space to appreciate the nuances of how

1 The term Somali territories is used to reflect the realities of governance within what is formally represented by the state of Somalia. In the north, the self-declared independent country of Somaliland has its own government, constitution and media legislation. Independent governance is similar in Puntland, the region south of Somaliland, although Puntland seeks a role in a greater Somalia. There are other smaller regions of the country that claim self-governance in the absence of a functioning central government.

global and local agendas interact and to highlight the risks of international agendas that too flatly emphasize the need for countries in Africa to catch up with more resilient countries, without adequately considering the context in which legislations and technical measures develop.

The chapter begins by clarifying the contours of cyber security and cyber resilience in Africa and then concentrates on the three case studies of Kenya, Ethiopia and Somalia, focusing on governments' role in shaping the cyber security agenda and drawing comparisons that can offer new lessons for, and beyond, East Africa.

CYBER SECURITY AND CYBER RESILIENCE IN EAST AFRICA

Debates on cybercrime and cyber security tend to concentrate around dramatic events such as the defacement of popular online spaces, sensitive information leaks or diffusion of particularly infectious malware. Less attention has been paid to broader issues of cyber resilience, that is, an organization or government's capability "to withstand negative impacts due to known, predictable, unknown, unpredictable, uncertain, and unexpected threats from activities in cyberspace" (ISACA 2014). Resilience refers to the idea that failures will inevitably occur, but promotes the adoption of holistic, cooperative measures that ensure a system does not wholly collapse. The objective is therefore maintaining as much normalcy as possible or returning to that level as quickly as possible following a cyber attack.

The concept of cyber resilience underlines the need for broad, concerted and comprehensive approaches to cyber security, but in reality, the implementation of measures to curb cyber attacks has been selective and driven by narrower agendas. Western powers with interest in East Africa have largely emphasized the need to combat extremism (Cassim 2011). The United States' efforts in East Africa, for example, have contributed to supporting greater preparedness for cyber attacks as a component of its larger anti-terrorist strategy, rather than as part of a coherent and concerted cyber security initiative for the region (Ploch 2010). China, for its part, through its increasing investment in telecommunication in Africa — more than US$3 billion went to Ethiopia alone to overhaul its telecommunication infrastructure — has largely favoured state-led initiatives, leading to fears that the state actors may be gaining too much power compared to other players involved in the shaping of national information societies (Gagliardone 2014).

It is in this light that the African Union Convention on Cyber Security and Personal Data Protection, which offers continental reference to improve cyber preparedness in Africa, has also raised concerns that in the charged political climate characterizing many countries on the continent, the heightened emphasis on security and state-led responses may impact free speech and privacy as governments that have been criticized for their abuses gain enhanced abilities to police the cyber world (Macharia 2014). The possibility that personal data could be processed without subjects giving free and informed consent when this is "in the public interest" (Art. 14.2.i), in particular, delineate scenarios where users may be stripped of their ability to be in control of their data and, on the contrary, be controlled in the name of agendas they had little voice in shaping (Access 2014). Concerns related to political tensions characterizing specific countries in Africa, as well as the fragility of institutions that should safeguard individual and collective freedoms, need to be taken into serious account. They should, however, avoid giving the impression that this is just an African problem, reproducing the cliché that unaccountable governments on the continent are simply implementing good provisions poorly. As the now abundant literature on the securitization of foreign and domestic policy (see, for example, Howell and Lind 2009), as well as on the abuses of individual rights perpetrated by the most advanced regimes (see Greenwald 2014) illustrate, the security agenda has created ample spaces for abuse by governments and private companies globally. The quest for more coordinated approaches to withstand cyber attacks should thus not be simply treated as a technical problem that requires technical solutions, but as a political one that requires transparent and open debates.

COUNTRY CASE STUDIES

Kenya: Putting Policies, Laws and Frameworks into Practice

Holding a dominant ICT position in East Africa, Kenya has made great strides in incorporating ICTs into various industry sectors. As of 2013, it was noted that ICTs contributed to 12.1 percent of the country's GDP (Mwenesi 2014a). International organizations appear to have bet on Kenya's ICT visions and ambitions. The World Bank Group alone invested around US$4.1 billion between 2003 and 2010 (Mwenesi 2014b). Such confidence presents massive opportunities, but can also be easily eroded if Kenya is not able to face emerging challenges in ways that match its ambition to be recognized as East Africa's ICT hub.

Kenya's first major international cybercrime case exposed some of the cyber vulnerabilities and gaps the country faces. In December 2014, 77 foreigners — one Thai national and 76 Chinese — were arrested in Nairobi; they were found in possession of equipment capable of a massive cyber attack, such as infiltrating Safaricom's[2] M-PESA (mobile money transfer) system, cash machines and bank accounts (Agence France-Presse 2014). Chinese officials claimed that this was another fraud den aimed outwardly

2 Safaricom is Kenya's leading mobile network operator.

at China, however, and not at Kenya (Otuki 2014). Even if this was the case, the cybercrime ring was only discovered by chance, when a fire broke out in a house some members were living in, and it had been operating completely hidden from authorities. According to the Kenyan police, the suspects were charged with operating an unlicensed telecommunication facility, and could face up to 15 years in jail or have to pay a 5 million Kenyan shilling fine (US$54,000), with more charges pending (Nzwili 2015). It is not clear yet under which specific law these suspects would be tried. The Chinese government assumes the criminal acts were targeted at them and has officially requested that its Kenyan counterpart extradite the suspects to face trial in China, where sound judicial procedures are in place, rather than potentially releasing the group in Kenya. The latter part of the Chinese government's reasoning was interpreted as indicating that Kenya may not have strong enough laws under which to prosecute the cybercrime suspects, eliciting reactions that Kenya must prove it has the "capacity, and will, to investigate and prosecute crimes of such magnitude and complexity" (*Daily Nation* 2015).

Kenya's strategy to strengthen the country's cyber resilience is caught between recognition of the still fragile status of the country in the digital realm and the ambition to make Kenya one of East Africa's leading players, emulating and seeking partnerships with actors that are better prepared to respond to emerging threats.

In 2012, with support from the International Telecommunications Unit as part of its Global Cybersecurity Agenda, the government created the Kenya National Computer Incident Response Team Coordination Centre (KE-CIRT/CC) to offer technical services in the management of cyber security.[3] More specifically, KE-CIRT/CC's role is to offer advice on national cyber-security matters and to coordinate responses to cyber incidents in collaboration with local, regional and international stakeholders. The centre falls under the Communication Authority of Kenya's docket, and offers what it dubs as "reactive and proactive services." The former service entails incident response, coordination and resolution, including the collection of national statistics about cyber incidents, while the latter entail technical advisory and capacity building, including technical research and development.[4] However, there is hardly any publicly available information, in the form of reports or news items on the centre's work or outputs, indicating if and how it has worked in conjunction with other government institutions addressing cyber-security matters. It has also been noted that due to capacity and requisite skills constraints, as well as engagement with other stakeholders, the centre's effects and impacts are hardly felt, and it could risk losing its relevance in the industry (Kigen et al. 2014, 41).

The contradictions between the tendency to emulate solutions adopted elsewhere and the need to concretely implement them into a national context have also been felt in more recent and apparently more coordinated efforts. Kenya's National Cybersecurity Strategy, developed in 2014, for example, aims to define the country's cyber-security vision, goals and objectives to secure the nation's cyberspace while continuing to promote the use of ICT to enable economic growth (Government of Kenya 2014, 5). In this strategy, the national government, through the ICT ministry, purports to enhance the nation's cyber-security posture by securing critical infrastructure, applications and services, with mention of (cyber) resilience through business impact analysis, continuity of operations and disaster recovery. These elements, however, are not articulated further, beyond being listed in a diagrammatic format (ibid., 7). The strategy document also talks of the government's awareness raising and training of the public and workforce on securing the national cyberspace by working in conjunction with academia to develop higher education curriculums on cyber security and specialized training programs. The third goal touches on developing required laws, regulations and policies to secure the nation's cyberspace as well as collaboration and information sharing; a comprehensive framework is envisioned to minimize duplication of effort as well as government-led approaches to designing and maintaining information-sharing capabilities to facilitate knowledge exchange and lessons learned among various stakeholders.

Given cases of fraud and of incitement to violence through ICTs that have occurred in Kenya, and given the aforementioned efforts from the government to tackle cyber security, the big question is how all the various institutions mandated with addressing the issue can work effectively and coordinate. The Kenyan case shows that theoretical attempts, while impressive, are not sufficient to address ever-growing cyber-security threats in the East African hub, and the region in general. There is a need to move from paper to practice, to strengthen existing institutions and processes, especially within the government, as well as recruit and build capacity well equipped to tackle emerging issues. That will form a critical stepping stone in moving from reacting to cyber threats or attacks, to setting in place strategies and measures to ensure cyber resilience in the country.

Ethiopia's Cyber Resilience: Turning International Priorities into National Agendas

Ethiopia has emerged as a paradox in East Africa with regard to ICTs and cyber security. Despite lagging behind in access, with only two percent of its population connected to

3 See www.ke-cirt.go.ke/index.php/itu-to-support-kenya-cybersecurity-efforts/.

4 See www.ke-cirt.go.ke/index.php/services/national-cirt-services/.

the Internet in 2014 (ITU 2015), the Ethiopian government has developed increasingly advanced legal and technical means to ensure greater control over the information transiting over communication networks and to defend the country from cyber attacks. These measures have been publicly justified by the need to align with international standards and respond to mounting cyber threats, but have also significantly boosted the ability of centralized power to persecute individuals and organizations, often without adequate oversight and checks and balances.

The Information Network Security Agency (INSA), first created in 2006 and then "re-established" in 2011, has been at the forefront of attempts to improve Ethiopia's cyber resilience. Shaped in the guise of the US NSA, the INSA has taken on the responsibility of "protecting" the national information space, taking counter measures against information attacks, which the law frames as any attack against the national interest, constitutional order and nation's psychology by using cyber and electromagnetic technologies and systems. It is answerable to the prime minister's office and every other governmental body has the duty to cooperate with the INSA. Its wide powers have caused concern, however. It empowers the director of the agency to designate the profiles, financial documents, equipment, methods and work outputs of certain personnel, as "top secret" and render them inaccessible to individuals, including the auditor general, if it is believed that national security would be at stake if otherwise disclosed. The law also allows the agency's investigators to conduct "virtual" forensic enquiries without judicial warrant on computers or infrastructures that are purported to be attacked or to be the source of attacks, eroding the constitutional right to privacy of users by leaving interpretation of their rights at the mercy of intelligence officers (Yilma 2014).

One of INSA's first acts has been the drafting of what later became the Telecom Fraud Offences Proclamation, passed by the Council of Ministers in 2012, which reaffirmed the state monopoly over telecommunications, imposed severe sanctions for any operator trying to compete with or bypass Ethio-telecom, and with Article 6 it extended the provisions of the Anti-Terrorism Proclamation to the online sphere. The proclamation can be considered the first "Internet law" in Ethiopia and contained measures aimed at combatting cyber attacks, including "unlawful interference," "unlawful interception" and "illegal access to a telecom network." In 2014, INSA proceeded to draft Ethiopia's first dedicated cyber security law, which incorporates many of the provisions included in the Council of Europe Convention on Cybercrime as well as the African Union Convention on Confidence and Security in Cyberspace. This could be seen as a welcome move, but should be considered also in the context of how similar laws have been previously used to stifle dissent. French political scientist Jean Francois Bayart (2000) has suggested analyzing the interaction of numerous governments in Africa with the international system through the lens of extraversion, to understand how they have turned their weaknesses in their favour. The Anti-Terrorism Proclamation in Ethiopia, passed in 2009 — five years before the cyber-security law began to be drafted — is a clear example of this mechanism. Framed as an effort to comply with the UN Security Council requests that "terrorist acts are established as serious criminal offences in domestic laws" (UN Security Council 2001), it also created the legal preconditions to actually prosecute critical voices within Ethiopia (or Ethiopians in the diaspora). Out of the 33 individuals convicted under the Anti-Terrorism Proclamation between 2009 and 2014, 13 have been journalists, leading organizations such as Human Rights Watch to denounce the law and its application as "deeply flawed" (Human Rights Watch 2013). The proposed cyber-security law may risk following a similar path.

In an ironic twist, the Ethiopian government has been accused of being behind cyber attacks targeting some of its political opponents. According to the Citizen Lab, software developed in the United Kingdom and in Italy has been employed to breach the computers of political opponents living abroad and spy on their communications (Citizen Lab 2013; 2015). This led an Ethiopian citizen residing in the United States to sue the Ethiopian government for infecting his computer. The Electronic Frontier Foundation is representing the plaintiff in this case.

Somalia and Somaliland: Resilience from the Ground Up

The Somali territories have become synonymous with stereotypes of chaos and lawlessness. This common perception, however, obscures examples of trust, security and regulation that have emerged in several areas, including trade and telecommunications. Despite decades of conflict, an externally oriented, open and relatively unrestricted economy has flourished (Little 2003). Enterprising companies, not shattered institutions, have provided ways for Somalis to send and receive money. These companies are primarily owned and initiated from the Somali diaspora, and have responded to the needs of Somalis and found opportunities in a remittance-based economy. Radio stations and telecommunications companies have also been able to function, and sometimes thrive. Hormuud Telecom is the largest of these companies and has been turning a profit since 2002. Hormuud also runs a mobile money transfer system, and plans to launch 3G network capacity soon, despite recent orders from al-Shabaab to close in some regions (Nyambura-Mwaura 2013). Another telecommunications firm, Telesom, has led the way in Somaliland, and also has a mobile money transfer system, Zaad. This model has been praised by Bill Gates, and was modelled after Kenya's M-PESA system, and has flourished in a region where 26 percent of the population pay bills over mobile, the highest rate

in the world (Stremlau and Osman 2015; Penicaud and McGrath 2014).

The particular growth of mobile banking has been connected to the lack of regulation and formal institutions that have slowed its growth elsewhere. As Stremlau (2012) and Carrier and Lochery (2013) have noted in their studies of trade and mobile banking in Somaliland and Eastleigh,[5] trust networks and traditional *xeer*[6] law contribute to the functioning of these informal systems. Trust is essential. In an environment of real physical insecurity, services such as EVCPlus, Hormuud's money transfer system, make much more sense than cash. EVCPlus has a US$300 limit, which does not reduce the risk of skimming or fraud, but is still safer and more convenient than using cash (Mohamed 2013). Furthermore, mobile money has emerged to fill a major gap in the banking sector whereby consumers can hold their money in "e-wallets." While some technical solutions have been advanced to reduce or avoid the likelihood of fraud, it is in the solving of disputes related to the increasing reliance of transfer on ICTs that the most interesting phenomena have emerged.

In the absence of formal regulatory and banking systems, complex relations among courts, clan-based governance and companies have been able to regulate and resolve conflicts (fraud, mistaken transfers or disputes over the amount of the transfer) over mobile money. This "hybrid judicial process" (Stremlau and Osman 2015) that has emerged to resolve disputes is an example of what we refer to as enculturation, a process by which local knowledge and resources are adopted to address issues that have found different solutions elsewhere. Companies in Somalia are increasingly regarded as the first authority to effectively resolve the conflict. In an area of instability and fierce competition among telecommunications and mobile money providers, their reputation for fairness and effectiveness is critical for their success. Government courts are generally regarded as corrupt and easily manipulated by the wealthier party, but are nevertheless part of a more formal complaints procedure if the conflict involves two individuals or families. *Sharia* courts are regarded as more trustworthy and, in some disputes, they may have a role if one party advocates for their intervention. But, in many cases, the most effective way of resolving a conflict between two people is the intervention of elders. This approach draws on traditional mechanisms for resolving property disputes, including those that would also be applied to more traditional businesses such as the livestock trade. It has also been refined and tested through the dynamic remittance industry, upon which the mobile banking and other ICT projects have been built (ibid.).

This combination of different mechanisms of conflict resolution, however, has been more difficult to implement in the areas controlled by al-Shabaab, which has highly restricted the use of ICTs and banned Internet use, declaring it to be un-Islamic. The group, however, uses social media to advance its agenda, presenting potential threats to its neighbours. Al-Shabaab has posed a different set of challenges and issues. Certainly its use of new technologies and the potential threat of cyber attack have been taken seriously in anti-terror efforts.

CONCLUSION

The analysis of how Kenya, Ethiopia and Somalia have offered distinctive responses to increasing cyber threats offers an important comparative angle to understand the continuities and discontinuities of collective efforts toward enhanced cyber security at the global, regional and national levels. International and national legislations, from the Council of Europe Convention on Cybercrime, to the African Union Convention on Cyber Security and Personal Data Protection, to the national laws seeking to implement the norms included in those conventions, may offer the impression of a growing consensus on how to strengthen cyber resilience. The analysis of the three countries indicates significant variance in approaches and responses to cyber security and cyber resilience.

This state of affairs is open to competing interpretations. From a more positive angle, this diversity can be perceived as the result of a successful interaction between international norms, which establish broad frameworks and set shared standards, and national legislations and practices, which adapt and localize these norms to ensure their local relevance. From a more critical point of view, some of the laws that are being discussed or the practical responses that are being publicly articulated can be seen instead as a tactic to please donors and international organizations, while implementation takes a different route.

As this short chapter seeks to explain, a third interpretation is possible, which calls for a more participatory agenda in deciding norms and procedures to reinforce cyber resilience at the national and regional level. Rather than reproducing the cliché that good provisions are poorly implemented in Africa, either because of a lack of means or because political actors on the continent may use them to pursue particular agendas, this interpretation more broadly cautions toward the ample discretionary power entrusted to governments and private companies by the (global or national) securitization agenda, and suggests avoiding treating cyber security as simply a technical problem requiring technical solutions. The three concepts

5 Eastleigh is a suburb of Nairobi that is populated mainly by Somali immigrants. The Somali diaspora has led a thriving economy and communications sector, but has also garnered attention from both the Kenyan police and al-Shabaab.

6 *Xeer* is analogous to a customary law regime but more extensive, in that it serves as an overall social contract governing relations between clans as well as defining the role of the individual within the community (Stremlau 2012, 160).

of emulation, extraversion and enculturation adopted here are meant to establish clearer links between the technical, social and political. The debate about cyber resilience in Africa is in the early stages and these categories should be interpreted simply as an encouragement to break down the prevalent narrative that Africa needs to catch up with other countries, and highlight some of its contradictions. There are multiple paths that can lead to reinforcing a country's ability to withstand or respond to an attack and some of them may need spaces for discussion among a broader variety of stakeholders than the small niche that has driven the agenda to date.

WORKS CITED

Access. 2014. "African Union Adopts Framework on Cyber Security and Data Protection." www.accessnow.org/blog/2014/08/22/african-union-adopts-framework-on-cyber-security-and-data-protection.

Agence France-Presse. 2014. "Kenya Arrests 77 Chinese Nationals in Cybercrime Raids." *The Guardian*, December 5. www.theguardian.com/world/2014/dec/05/kenya-chinese-nationals-cybercrime-nairobi.

Bayart, J.-F. 2000. "Africa in the World: A History of Extraversion." *African Affairs* 99 (395): 217–67.

Carrier, N. and Lochery, E. 2013. "Missing States? Somali Trade Networks and the Eastleigh Transformation." *Journal of Eastern African Studies* 7 (2).

Cassim, F. 2011. "Addressing the Growing Spectre of Cybercrime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players." *Comparative and International Law and Justice South Africa* 44: 123–38.

Citizen Lab. 2013. "You Only Click Twice: FinFisher's Global Proliferation." https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

———. 2015. "Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware." https://citizenlab.org/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/.

Daily Nation. 2015. "Try Crime Suspects Here." *Daily Nation*, January 15. www.nation.co.ke/oped/Editorial/China-Kenya-Hacking-Trial/-/440804/2590722/-/fcv6r1z/-/index.html.

Gagliardone, I. 2014. "Media Development with Chinese Characteristics." *Global Media Journal* 4 (2): 1–16.

Government of Kenya. 2014. Cybersecurity Strategy. Ministry of Information Communications and Technology.

Greenwald, G. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York, NY: Metropolitan Books/Henry Holt.

Harris, A., S. Goodman and P. Traynor. 2013. "Privacy and Security Concerns Associated with Mobile Money Applications in Africa." *Washington Journal of Law, Technology and Arts* 8 (3): 245–64.

Herbling, D. 2014. "Kenyans Move Sh 1.1trn on Mobile Phones in 6 Months." *Business Daily*, August 10. www.businessdailyafrica.com/Kenyans-move-Sh1-1trn-on-mobile-phones-in-6-months/-/539552/2414794/-/y22x2tz/-/index.html.

Howell, J. and J. Lind. 2009. *Counter-Terrorism, Aid and Civil Society: Before and After the War on Terror*. Basingstoke, UK: Palgrave Macmillan.

Human Rights Watch. 2013. "Ethiopia: Terrorism Law Decimates Media." www.hrw.org/news/2013/05/03/ethiopia-terrorism-law-decimates-media.

ISACA. 2014. "European Cybersecurity Implementation: Resilience." www.isaca.org/Knowledge-Center/Research/Documents/European-Cybersecurity-Implementation-Resilience_res_Eng_0814.pdf?regnum=256607.

ITU. 2015. ICT Statistics. www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

Jackson, T. 2015. "Can Africa Fight Cybercrime and Preserve Human Rights?" BBC News. www.bbc.com/news/business-32079748.

Kagwanja, P. and M. Karanja. 2014. "How Cybercrime Complicates War on Terror." *The East African*, August 18. www.theeastafrican.co.ke/news/How-cybercrime-complicates-war-on-terror/-/2558/2422854/-/item/0/-/3ur4taz/-/index.html.

Kharouni, L. 2013. "Africa: A New Safe Harbor for Cybercriminals?" Trend Micro Incorporated Research Paper. www.trendmicro.co.uk/media/misc/africa-new-safe-harbor-for-cybercriminals-en.pdf.

Kigen, P., C. Kisutsa, C. Muchai, K. Kimani, M. Mwangi and B. Shiyayo. 2014. "Kenya Cybersecurity Report 2014." www.serianu.com/downloads/KenyaCyberSecurityReport2014.pdf.

Little, P. 2003. *Somalia: Economy without State*. Bloomington, IN: Indiana University Press.

Macharia, J. 2014. "Africa Needs a Cybersecurity Law But AU's Proposal Is Flawed, Advocates Say." http://techpresident.com/news/wegov/24712/africa-union-cybersecurity-law-flawed.

Makulilo, A. B. 2012. "Privacy and Data Protection in Africa: A State of the Art." *International Data Privacy Law* 2 (3): 163–78.

Mohamed, H. 2013. "Electronic Transfers Improve Somalia Economy." Aljazeera. www.aljazeera.com/indepth/features/2013/08/201383114161492568 2.html.

Mukinda, F. 2014. "Fraudsters Find Easy Cash in Mobile Banking, Report Says." *Daily Nation*, September 7. http://mobile.nation.co.ke/news/-/1950946/2444632/-/format/xhtml/-/10da2sbz/-/index.html.

Mwenesi, S. 2014a. "ICT Contribution to Kenya's GDP now at 12.1%." Human IPO, July 22. www.humanipo.com/news/46203/ict-contribution-to-kenyas-gdp-now-at-12-1/.

———. 2014b. "World Bank Allocates $12m for Kenya County for ICT projects." Human IPO, April 17. www.humanipo.com/news/42926/world-bank-allocates-12m-for-kenya-county-ict-projects/.

Nyambura-Mwaura, H. 2013. "Somalia's Hormuud Rings up Telecom Profits Despite Anarchy." Reuters, November 13. http://uk.reuters.com/article/2013/11/13/uk-somalia-hormuud-idUKBRE9AC0WQ20131113.

Nzwili, F. 2015. "China and Kenya at Odds over Suspected Chinese Cyber Criminals." *The Christian Science Monitor*, January 26. www.csmonitor.com/World/Africa/2015/0126/China-and-Kenya-at-odds-over-suspected-Chinese-cyber-criminals.

Otieno, J. 2014. "Worries over New Avenues of Cybercrime." *The East African*, September 22. www.theeastafrican.co.ke/news/Worries-over-new-avenues-of-cyber-crime/-/2558/2461630/-/vsn7k0z/-/index.html.

Otuki, N. 2014. "Beijing Says Runda Fraud Ring Likely Targeted China." *Business Daily*, December 5. www.businessdailyafrica.com/Beijing-says-Runda-fraud-ring-targeted-China/-/539546/2546306/-/item/0/-/v9hr5bz/-/index.html.

Penicaud, C. and F. McGrath. 2014. "Innovative Inclusion: How Telesom ZAAD Brought Mobile Money to Somaliland. GSMA Mobile Money for the Unbanked Programme.

Ploch, L. 2010. "Countering Terrorism in East Africa: The U.S. Response." CRS Report for Congress, Congressional Research Service.

Protalinski, E. 2012. "Former Pentagon Analyst: China has Backdoors at 80% of Telecoms." ZDNet, July 14. www.zdnet.com/article/former-pentagon-analyst-china-has-backdoors-to-80-of-telecoms/.

Quarshie, H. O. and A. Martin-Odoom. 2012. "Fighting Cybercrime in Africa." *Computer Science and Engineering* 2 (6): 98–100.

Rid, T. 2014. "Snowden, 多谢 多谢." Kings of War, March 23. http://kingsofwar.org.uk/2014/03/snowden-thanks-very-much/.

Stremlau, N. 2012. "Somalia: Media Law in the Absence of a State." *International Journal of Media and Cultural Politics* 8 (2,3): 159–74.

Stremlau, N. and R. Osman. 2015. "Courts, Clans and Companies: Mobile Money and Dispute Resolution." *Stability: International Journal of Security and Development* 4 (1).

UN Security Council. 2001. Resolution 1373, New York, September 28.

Yilma, K. 2014. "Developments in Cybercrime Law and Practice in Ethiopia." *Computer Law & Security Review* 30 (6): 720–35.

ABOUT THE AUTHORS

Iginio Gagliardone is research fellow in new media and human rights at the University of Oxford. He is a member of the Programme in Comparative Media Law and Policy, a research associate of the Oxford Internet Institute as well as an associate of the Centre of Governance and Human Rights at the University of Cambridge. His research focuses on the relationship between new media, political change and human rights, and on the emergence of distinctive models of the information society. His most recent research projects explore the nature and significance of hate speech online, with a particular emphasis on the trade-offs between freedom of expression and human dignity, and on how social networking platforms are responding (or failing to respond) to the challenges hate speech presents.

Nanjira Sambuli is a research manager at iHub, Nairobi, where she leads the Governance & Technology research pillar. Nanjira is trained as a mathematician with experience as a new media strategist for organizations such as the United Nations Environment Programme, United Nations Human Settlements Programme, Africans Act 4 Africa, and Global Power Shift, on their pan-African and international campaigns. She is also the editor of *Innovative Africa: The New Face of Africa*, a series of essays on the emerging African tech landscape. Nanjira is interested in understanding the unfolding impacts of information and communication technology adoption and how those impact governance, innovation, entrepreneurship and societal culture in her native Kenya, and also across the African continent.

ABOUT CIGI

We are the Centre for International Governance Innovation: an independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis.

Our research programs focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners and support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

Au Centre pour l'innovation dans la gouvernance internationale (CIGI), nous formons un groupe de réflexion indépendant et non partisan qui formule des points de vue objectifs dont la portée est notamment mondiale. Nos recherches, nos avis et l'opinion publique ont des effets réels sur le monde d'aujourd'hui en apportant autant de la clarté qu'une réflexion novatrice dans l'élaboration des politiques à l'échelle internationale. En raison des travaux accomplis en collaboration et en partenariat avec des pairs et des spécialistes interdisciplinaires des plus compétents, nous sommes devenus une référence grâce à l'influence de nos recherches et à la fiabilité de nos analyses.

Nos programmes de recherche ont trait à la gouvernance dans les domaines suivants : l'économie mondiale, la sécurité et les politiques mondiales, et le droit international, et nous les exécutons avec la collaboration de nombreux partenaires stratégiques et le soutien des gouvernements du Canada et de l'Ontario ainsi que du fondateur du CIGI, Jim Balsillie.

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

ABOUT CHATHAM HOUSE

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

CIGI MASTHEAD

Executive

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

Publications

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

For publications enquiries, please contact publications@cigionline.org.

Communications

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

CIGI

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

CHATHAM HOUSE
The Royal Institute of International Affairs

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

RECYCLED
Paper made from recycled material
FSC® C023070