CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission on Internet Governance

ourinternet.org

PAPER SERIES: NO. 25 — FEBRUARY 2016

The Digital Trade Imbalance and Its Implications for Internet Governance

Susan Ariel Aaronson

THE DIGITAL TRADE IMBALANCE AND ITS IMPLICATIONS FOR INTERNET GOVERNANCE

Susan Ariel Aaronson

CHATHAM HOUSE
The Royal Institute of International Affairs

Copyright © 2016 by Susan Ariel Aaronson

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

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

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

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

This work is licensed under a Creative Commons Attribution — Non-commercial — No Derivatives License. To view this licence, visit (www.creativecommons.org/licenses/by-nc-nd/3.0/). For re-use or distribution, please include this copyright notice.

Centre for International Governance Innovation, CIGI and the CIGI globe are registered trademarks.

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

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

TABLE OF CONTENTS

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

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

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

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

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

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

www.ourinternet.org

ABOUT THE AUTHOR

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.

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
TLDs	top-level domains
TPP	Trans-Pacific Partnership
TTIP	Transatlantic Trade and Investment Partnership
TiSA	Trade in Services Agreement
UAE	United Arab Emirates
USITC	United States International Trade Commission
USTR	United States Trade Representative
WTO	World Trade Organization

EXECUTIVE SUMMARY

Today, information is currency; it facilitates productivity, exchange, technology and trade. Information is also the building block of the digital economy (an economy based on digital technologies — products and services that facilitate the creation, storage, analysis and sharing of data and information).[1] Although many countries are gaining expertise and market share, one country, the United States, dominates both the global digital economy and digital trade (commerce in products and services delivered via the Internet).[2] The United States is also the key force behind efforts to develop a system of trade rules to govern cross-border information flows.

The United States first proposed rules to govern cross-border information flows in the late 1980s. In recent years, the United States, Canada and the European Union have included *non-binding* language in trade agreements that is designed to ensure that information moves seamlessly across borders. In October 2015, after seven years of negotiation, the United States and its 11 negotiating partners found common ground on binding language in the Trans-Pacific Partnership (TPP). The United States is also trying to include similar language in the Transatlantic Trade and Investment Partnership (TTIP), and the Trade in Services Agreement (TiSA) under the World Trade Organization (WTO).

Proponents of using trade agreements to govern cross-border information flows rely mainly on economic arguments to justify these provisions. They suggest that by reducing barriers to trade and information, individuals, firms and governments will find it cheaper to send and store information. More people will have access to information, which, in turn, could boost Internet operability, economic growth and jobs. Although many policy makers acknowledge these potential benefits, they have not made digital trade rules a top priority. Instead, these officials have adopted a wide range of domestic policies to achieve local priorities such as bolstering local Internet industries, regulating the Internet within their borders or protecting the privacy of their citizens from surveillance or misuse of their private information. Many such officials are worried about their dependence upon US companies to provide Internet-related services and believe that they can best stimulate economic growth by nurturing local Internet firms. While many US officials understand that other states often have legitimate reasons to take these steps, the United States (and, to a lesser extent, the European Union) closely monitors such actions and policies and increasingly labels some of these policies "digital protectionism." The USITC (2013, 5-1-5-2) defines digital protectionism as barriers or impediments to digital trade, including censorship, filtering, localization measures and regulations to protect privacy. The United States made efforts to limit digital protectionism a key part of the TPP.

The 12 negotiating parties made the TPP public in November 2015. The agreement states that "each party shall allow the cross-border transfer of information by electronic means."[3] In so doing, the TPP nations have supported the open Internet by making the free flow of information a default. The agreement also recognizes that

1 The digital economy is hard to define and scholars have not found common ground on a shared definition (Imlah 2013).

2 See US International Trade Commission [USITC] 2014, xv.

3 See https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf.

each party has its own regulatory requirements for the transfer of information. Finally, it includes exceptions. Governments may impose conditions or restrictions on the cross-border transfer of information as required to achieve public policy objectives, provided those measures are not discriminatory or a disguised restriction on trade. Hence, governments can restrict information flows to protect public morals or national security.

Because of this binding language, should the TPP go into effect, it will set an important precedent for Internet governance. The agreement will cover almost one-quarter of current Internet users and will affect the Internet in 12 significant trading nations. The US government argues that the "TPP will help preserve the open Internet" (Office of the United States Trade Representative [USTR] 2015a). Meanwhile, the TPP's critics assert that the agreement undermines Internet freedom and access to information. However, both proponents and critics of the TPP overestimate its likely effects upon the Internet.

This paper will examine how governments use trade agreements and policies to address cross-border Internet issues and to limit digital protectionism. The "digital trade imbalance" of the title refers to the imbalance between the United States' enthusiasm for and its major trade partners' ambivalence toward the creation of a system of trade rules to govern cross-border information flows. The imbalance also speaks to the divide over what is "protectionist" and what comprises a legitimate national policy. Because of such dissension, although trade agreements seem to be logical avenues for governing cross-border information flows, they might not be the best place to address these issues.

The paper concludes with several recommendations to government officials. Specifically, policy makers should encourage interoperability and the rule of law, define and challenge barriers to digital trade and do a better job of linking trade with other equally important objectives such as advancing digital rights.

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.[4]

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. Although more people can now participate in trade, the Internet has also facilitated cross-border trade in drugs,

4 According to the 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).

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).[5]

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.[6] 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

5 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."

6 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).[7] 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 paper 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 paper 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 paper 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.

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

The paper 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 paper 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 paper 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 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;[8] the Agreement on Trade-Related Aspects of Intellectual Property Rights, which protects trade-related intellectual property pertinent to information technology, such as computer programs;[9] 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.

8 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; USTR 2015b; see also https://ustr.gov/sites/default/files/ITA-expansion-product-list-2015.pdf).

9 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.[10] 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).[11] 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.[12] 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 US Trade Representative 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.[13] 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.).

10 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.).

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

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

13 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.[14] 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.[15] 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.[16] 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).[17] 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

14 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).

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

16 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).

17 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.[18]

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."[19] 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,[20] 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 US Trade Representative 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.

18 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).

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

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

Holleyman suggested that language in the agreement 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 2015c). 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.[21]

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

21 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.[22] Every EU citizen has the right to personal data protection and firms can only collect that data under specific conditions.[23] The European Union also requires member states to investigate privacy violations.[24] 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.[25]

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.[26] Meanwhile, other countries, such as the Philippines, have adopted EU data protection policies.[27] 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

22 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).

23 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.

24 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.

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

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

27 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.[28] 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.[29] 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.[30] 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).[31] 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*

28 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.

29 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).

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

31 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.[32] 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.[33] 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.

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

33 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."[34] 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.[35] 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.[36]

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

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

35 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.

36 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.[37]

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.[38] 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

37 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).

38 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.[39] 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 2015d, 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.

39 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 2015d, 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.[40] 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

40 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 paper'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 Commssion. 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." https://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.

Imlah, Bill. 2013. "The Concept of a 'Digital' Economy." Oxford Digital Economy Collaboration Group, September 13. http://odec.org.uk/the-concept-of-a-digital-economy/.

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." EFF 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." ArutzSheva, 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. "TPP: Summary — Electronic Commerce." https://ustr.gov/sites/default/files/TPP-Chapter-Summary-Electronic-Commerce.pdf.

———. 2015b. "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.

———. 2015c. "TPP: Chapter 29 — Exceptions." November 5. https://medium.com/the-trans-pacific-partnership/exceptions-1299fbf34b76#.rbm5y87nc.

———. 2015d. "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." 69. 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 CIGI

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

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

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

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

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

ABOUT CHATHAM HOUSE

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

CIGI MASTHEAD

Executive

President	Rohinton P. Medhora
Director of the International Law Research Program	Oonagh Fitzgerald
Director of the Global Security & Politics Program	Fen Osler Hampson
Director of Human Resources	Susan Hirst
Director of the Global Economy Program	Domenico Lombardi
Vice President of Finance	Mark Menard
Chief of Staff and General Counsel	Aaron Shull

Publications

Managing Editor, Publications	Carol Bonnett
Publications Editor	Jennifer Goyder
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Publications Editor	Kristen Scott Ndiaye
Publications Editor	Lynn Schellenberg
Graphic Designer	Sara Moore
Graphic Designer	Melodie Wakefield

Communications

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

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

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

FSC www.fsc.org
RECYCLED
Paper made from recycled material
FSC® C023070