Institute for International Economic Policy Working Paper Series
Elliott School of International Affairs
The George Washington University

What Are We Talking About When We Discuss Digital Protectionism?

IIEP-WP-2017-9

Susan Ariel Aaronson
George Washington University

July 2017

Institute for International Economic Policy
1957 E St. NW, Suite 502
Voice: (202) 994-5320
Fax: (202) 994-5477
Email: **iiep@gwu.edu**
Web: **www.gwu.edu/~iiep**

What Are We Talking About When We Discuss Digital Protectionism?

Susan Ariel Aaronson, Elliott School of International Affairs, GWU

Working Paper for the Economic Research Institute of Asia (ERIA), July 2017

Abstract:

For almost a decade, executives, scholars, and trade diplomats have argued that filtering, censorship, localization requirements and domestic regulations are distorting the cross-border information flows that underpin the internet. Herein I make 5 points about digital protectionism.

1. Digital protectionism differs from protectionism of goods and other services because trade in information is different from trade in goods and other services. Information is intangible, highly tradable, and some information is a public good which governments must provide and regulate effectively.

2. It will not be easy to set international rules to limit digital protectionism without a shared set of norms and definitions. However, we can only obtain greater clarity with trade disputes and clearer trade rules.

3. The US, EU, and Canada have labeled other countries policies' protectionist, yet their arguments and actions sometimes appear hypocritical.

4. China allegedly has used a wide range of cyber-strategies including distributed denial of service (DDoS) attacks (bombarding a web site with service requests) to censor information flows and impede online market access beyond its borders. WTO members have yet to discuss this issue and the threat it poses to trade norms and rules.

5. Digital protectionism may be self-defeating. Governments that adopt digital protectionist strategies could experience unanticipated side effects, including reduced access to information, internet stability, and generativity. Digital protectionism may also undermine human rights and scientific progress.

Recommendations—Policymakers Should:

1. Ask the WTO Secretariat to examine whether domestic policies that restrict information (short of exceptions for national security, privacy, and public morals) constitute barriers to cross-border information flows that could be challenged in a trade dispute.

2. Convene a study group at the WTO to examine the trade implications of governmental use of malware or DDoS attacks to improve the competitiveness of their firms or censor the internet in other countries. *These tactics should be banned, although the WTO may not be the best forum for discussion of these problems.*

3. During each WTO member state's trade policy review process, the members of the WTO should monitor how each member's rules governing information flows potentially distort trade.

4. Propose and negotiate an international agreement that defines and limits digital protectionism and delineates clear and limited exceptions.

What Are We Talking About When We Discuss Digital Protectionism?

Susan Ariel Aaronson[1]

ERIA Paper, July 14, 2017

I. Introduction

Victor Hugo once wrote that "No army can withstand the strength of an idea whose time has come." In 2006, law professor Tim Wu put forward an idea about the trade regime and the internet. Stressing that the internet is built on global information flows, he noted that the global internet allows everyone to potentially become an importer or exporter of services and goods. "Hence, almost by accident, the WTO has put itself in an oversight position for most of the national laws and practices that regulate the Internet" (Wu 2006, 263-264). Wu concluded that members of the WTO would have to decide how much control of the internet is legitimate domestic regulation, and how much is a barrier to trade (Wu 2006, 287).

In truth, the WTO and other trade agreements say nothing about the internet or censoring (Burri 2013), and very little about human rights on or offline (Aaronson with Townes 2012). Nonetheless, Wu's idea gained traction. In 2007, Google asked the USTR to fight censorship as a barrier to trade (Rugaber 2007). Andrew McLaughlin of Google noted, "We take seriously Google's mission 'to organize the world's information and make it universally accessible and useful,' but government efforts to censor the internet makes that task much harder" (McLaughlin 2007).

Journalists,[2] business associations (CCIA 2008; NFTC 2010; Swedish Board of Trade 2016), and scholars soon picked up on the notion that censorship, blocking, and redirection of

[1] Research Professor and Cross-Disciplinary Fellow, Elliott School of International Affairs. I am grateful to ERIA for feedback and support. I am also grateful to the participants at an ERIA seminar in Bangkok, July 2017; to Hanna Norberg, trade economist; William Marczak, UC Berkeley; and Hosuk Lee Makiyama of ECIPE, Brussels.

[2] Duncan Riley, "Baidu Hijacking Google Traffic In China," October 18, 2007 https://techcrunch.com/2007/10/18/baidu-hijacking-google-traffic-in-china/; and John Biggs, "China Declares War on Western Search Sites," TechCrunch, October 18, https://techcrunch.com/2007/10/18/cyberwar-china-declares-war-on-western-search-sites/; Claudine Beaumont, "Foursquare Blocked in China," The Telegraph, June 4, 20102010,

internet traffic constituted a barrier to trade and a new form of protectionism (Gao 2011; Makiyama and Erixson 2010; Chander 2010; Chander and Le 2015; Broude and Hestermeyer 2013; Aaronson with Townes 2012). And one government acted: in 2011, the US Trade Representative sent a letter to the Chinese Ministry of Commerce requesting detailed information on the trade impact of Chinese policies that may block U.S. companies' websites in China, creating commercial barriers that especially hurt America's small business. The United States stated it would like to better understand China's rules governing website blocking so that service suppliers based outside of China may adopt appropriate policies to avoid encountering this problem (USTR 2011). The Chinese government never responded and the US did not move forward with a trade dispute.

Herein I examine the state and implications of digital protectionism. I use process tracing to examine how policies towards digital protectionism, particularly in the US and the EU, evolved over time. Scholars use process-tracing in social science to study causal mechanisms and to link causes with outcomes (Beach and Pederson 2013). I make five points;

1. Digital protectionism differs from protectionism of goods and other services because trade in information is different from trade in goods and other services. Information is intangible, highly tradeable, and some information is a public good which governments must provide and regulate effectively.

2. It will not be easy to set international rules to limit digital protectionism without a shared set of norms and definitions. However, we can only obtain greater clarity with trade disputes and clearer trade rules.

3. The US, EU, and Canada have labeled other countries policies' protectionist, yet their arguments and actions sometimes appear hypocritical.

4. China allegedly has used a wide range of cyber-strategies including DDoS attacks (bombarding a web site with service requests) to censor information flows and impede online

http://www.telegraph.co.uk/technology/social-media/7802992/Foursquare-blocked-in-China.html; Jordan Calinoff, "Beijing's Foreign Internet Purge," FOREIGN POLICY, January 15, 2010, http://foreignpolicy.com/2010/01/15/beijings-foreign-internet-purge/.

market access beyond its borders. WTO members have yet to discuss this issue or the threat it poses to trade norms and rules.

5. Digital protectionism may be self-defeating. Governments that adopt digital protectionist strategies could experience unanticipated side effects, including reduced internet stability, generativity, and decreased access to information (Force Hill 2014; Zittrain et al. 2017). Digital protectionism may also undermine human rights and scientific progress. (Swedish Board of Trade 2016, 52; OECD 2016; Aaronson 2016a).

This article proceeds as follows. In the first section, I define protectionism and digital protectionism, and I illuminate the relationship between digital protectionism, domestic regulations, and trade/market distortions. I also examine what trade agreements say about digital protectionism and explain why it will be so difficult to develop shared rules. I then discuss what the US and the EU say about digital protectionism and show that their practices appear confusing and/or contradictory at times. I then focus on Chinese digital protectionism and how it may distort trade not only in the home market but other countries as well, a challenge for trade policymakers. Finally, I develop some conclusions and offer recommendations.

Before readers turn to the analysis, I offer some definitions of key terms. In this paper, I utilize the term cross-border information flows rather than data flows. Many analysts use data and information interchangeably—they equate cross-border data flows with information flows. Herein I use information (instead of data). Data is unprocessed facts or details. When data are processed, organized, structured, or presented in a meaningful or useful manner, it becomes information. Conversely, information can be defined as processed, interpreted, organized, structured or presented data—i.e. something useful.[3] Information is therefore the building block of the Internet as well as digital trade (goods and services delivered vis the internet and associated technologies). Information flows often move across borders because individuals, companies, or governments authorize information to be transferred from one country (the source of information) to another country where the information may be processed (like payroll) or utilized (to better counteract criminal patterns) (USITC 2013, 2014; US Department of Commerce 2014).

[3] http://www.diffen.com/difference/Data_vs_Information

II. What is Digital Protectionism?

To best understand digital protectionism, we first need to understand the meaning of protectionism. Protectionism is both an ideology and a government act (Irwin 1996). Despite thousands of years of trade, and two centuries spent writing hundreds of trade agreements designed to limit protectionism, it has no exact definition (Swedish Board of Trade 2016, 5; McGee 1996).

In 1982, the Office of the Special Trade Representative (now called the US Trade Representative) drafted a primer on trade. It defined protectionism as "the setting of trade barriers high enough to discourage foreign imports or to raise their prices sufficiently to enable relatively inefficient domestic producers to compete successfully with foreigners" (USTR 1982, 149). In this view, policymakers use protectionist measures to reduce the supply and/or raise the cost of imported goods or services, at the behest of some of their citizens. In this view, protectionism is about altering market conditions and distorting trade in ways that favor domestic producers over their foreign competitors.

However, this definition is clearly out of date. Protectionism evolves as both economies and governance change over time. Moreover, protectionism ebbs and flows in all countries depending on a wide range of factors including: the state of the economy, the political clout of interest groups dependent on trade or protection, public awareness of trade, or the strength or weakness of protectionist ideas (Aaronson 2001, 11). For centuries, policymakers have used trade agreements to establish the rule of law in trade by obligating that signatories forbid certain types of protectionist practices. But policymakers have also long recognized that the policies that may appear protectionist may not have been designed to achieve trade distorting effects. For this reason, trade agreements also include "exceptions," which allow governments to breach the rules to achieve other important policy goals. As example, many governments adopt food safety regulations to protect consumers from harm, although these measures can distort trade. While these regulations may have a protectionist effect, they may lack protectionist intent (Swedish Board of Trade 2016, 5).

At first glance, digital protectionism may look like other forms of protectionism. Policymakers in country A might use border measures or domestic policies such as subsidies to

favor domestic providers or alter market conditions in country A. And as with trade in goods, officials might restrict trade in information to achieve other important policy objectives like protecting public morals or the privacy of their citizens. In so doing, they may, with or without intent, distort trade.

While the strategies to achieve digital protectionism may resemble protectionism of goods or services, digital protectionism differs from traditional protectionism in four key ways, delineated below.

- First: information is not just one thing—it can be a good, a service, or both simultaneously. Consequently, it may be hard for researchers to ascertain exactly what a government wants to protect and whether a government is acting with protectionist intent.
- Second: information is different from goods or services in that it also a form of currency; it facilitates productivity, exchange, technology, and trade (Aaronson 2016a, 1-2). While goods are material, information is intangible. Goods can be stored, some of the characteristics of goods are observable before purchase, consumption of goods always follows production, and goods move in space over means of transportation (Ariu 2012). Trade in information differs from trade in other services in that it is highly tradeable, whereas many services require the suppliers and the consumers to be in the same physical location in order for the transaction to occur (Lennon 2009).
- Third: trade in information is fluid and frequent, and location is hard to determine on the borderless network. Trade in the same set of information can occur repeatedly in nanoseconds (as example when millions of people download Beyonce's latest song). Researchers and policymakers may find it hard to determine what is an import or an export. They also struggle to ascertain when information is subject to domestic law (such as IP law) and what type of trans-border enforcement is appropriate (Goldman 2011; de la Chapelle and Fehlinger 2016). Policymakers can't easily determine jurisdiction, because information can be routed through a US server to another jurisdiction. There is no global consensus as to where and who should draw digital borders, because information flows may travel through several countries before these flows reach their final destination and customer (de la Chapelle and Fehlinger 2016).

- Fourth: economists generally agree that many types of information are public goods which governments should provide and regulate effectively. When states restrict the free flow of such information, they reduce access to information which can diminish economic growth, productivity, and innovation, both domestically and globally (Maskus and Reichman 2004, 284-85; Khan 2009; OECD 2016). They can also effect the functioning of the Internet (Force-Hill 2014, 32; Daigle 2015, Zittrain et al. 2017). Hence, if officials restrict cross-border information flows, they may create many unintended consequences.

However, although some nations have agreed to language in trade agreements that limit some types of trade distorting policies, policymakers have yet to develop a shared definition of digital protectionism. Of the world's ten largest exporters of computer services, only the US has put forward a formal definition. Government officials such as Japanese Trade Minister Seko and EU Trade Commissioner Malmström have condemned digital protectionism but neither minister (nor trade policymaking web site) have defined what it is and is not.[4]

The US was likely the first government to define digital protectionism because digital trade is particularly important to the US economy. The US International Trade Commission (ITC) estimates that digital trade in certain digitally intensive industries resulted in a 3.4% to 4.8% increase in US GDP from 2011 to 2013, while online sales of products and services in 'digitally intensive' sectors were 6.3% of US GDP in 2012. The ITC also asserts that the expansion of digital trade caused real wages to increase by 4.5% to 5% and boosted US

[4] According to the WTO the major computer services exporters are the EU28, India, US, Israel, Canada, Philippines, Russia, Korea, Japan, and Ukraine (World Trade Statistical Review 2016, 124). I searched each of their trade ministries' English language sites using search terms digital trade, e-commerce, and digital protectionism, searching for a definition or mention of digital protectionism. Only the US, Japan, and the EU yielded results. India, http://commerce.gov.in/InnerContent.aspx?Id=9; the US, www.ustr.gov; Israel, http://economy.gov.il/English/InternationalAffairs/ForeignTradeAdministration/TradePolicyAgreements/Pages/TradeEconomicAgreements.aspx; Canada, http://www.international.gc.ca/trade-agreements-accords-commerciaux/index.aspx?lang=eng trade agency web sites; the Philippines, http://www.dti.gov.ph/component/search/?searchword=digitahttp://government.ru/en/department/54/events/l%20protectionism&searchphrase=all&Itemid=106; Russia, http://government.ru/en/department/54/events/; Korea, http://english.motie.go.kr/search/search.do; Japan, http://www.meti.go.jp/english/press/2017/0713_001.html; and Ukraine, http://www.me.gov.ua/Tags/DocumentsByTag?lang=en-GB&id=33385135-13a6-4c1b-9ee6-3cde3d7174ad&tag=TradeDevelopment

aggregate employment by up to 1.8% while reducing average trade costs by 26% (USITC 2014). This is not surprising, as the US is home to 11 of the world's 15 largest internet businesses. China is home to the other four.[5] The US Department of Commerce reported that digital delivered services accounted for about half of all services trade (Fefer et al. 2017, 8).

In 2013, at the behest of the US Senate Finance Committee, the ITC sought to examine the extent of digital protectionism, which it defined as the erection of barriers or impediments to digital trade, including censorship, filtering, localization measures, and regulations to protect privacy. Digital trade can be defined as trade in goods and services delivered via the internet and associated technologies (USITC 2013). The ITC also surveyed industry representatives and experts regarding what they considered major impediments to digital trade. These individuals "expressed concerns with respect to localization barriers, data privacy and protection, intellectual property-related issues, and online censorship, as well as impediments to digitally enabled trade" (USITC 2013, xxi). In 2017, the Congressional Research Service, which provides policy and research information to the US Congress, issued a broader list. In the tables that follow, I use this list to examine how these measures may distort trade, how they affect markets, and whether they are covered under the World Trade Organization (WTO) rules. The WTO is the only global international organization dealing with the rules of trade between nations. It contains several agreements negotiated and signed by some 164 states that make up the bulk of the world's trading nations.[6] Table 1 provides an overview of policies that the US labels as protectionist and provides examples of countries that have adopted such policies.

[5] Statista, 2017. "Market capitalization of the largest internet companies as of May 2017 (in billion U.S. dollars)," https://www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/

[6] "About the WTO," *World Trade Organization*.com, https://www.wto.org/english/thewto_e/thewto_e.htm

Table 1: Listing of Barriers to Digital Trade from Congressional Research Service

Tariff Barriers	**Countries**	**Description**
Tariffs on digital goods	Only applied by non-members of the WTO, ITA, or FTAs	
Nontariff Trade Barriers	**Countries**	
Localization Requirements	Russia, Turkey, Nigeria	Must conduct digital trade activities within country or require use of local content, like hardware or software
Data Flow Restrictions	Vietnam, China	Must keep certain types of information in local servers or process it locally
IPR Infringement	China	Cyber theft of intellectual property, free file sharing websites
National Standards and Burdensome Conformity Assessment	Russia	Requirement to divulge source code
Filtering/Blocking	China, Malaysia	Block access to certain sites or filter/block services like Facebook
Net Neutrality		Relates to management of internet traffic: all services must be treated the same regardless of size. Forbids paid prioritization of content or throttling of content
Cybersecurity Risks	Too little regulation (Vietnam); Too much regulation (China)	Inadequate cybersecurity can undermine trust and reduce willingness to use internet. Too much can distort trade, yet may be justified under trade "exceptions."

Sources: Fefer et al 2017; USITC 2013, 2014.

Table 2 below attempts to illuminate how these policies might affect markets. In column 1, I discuss market/trade effects (Does the policy discriminate or restrict trade between foreign and domestic providers? Does it distort markets?) as well as whether US experts and executives perceive that a measure is intended to distort trade. I rely on survey data collected by the OECD and/or USITC (2013, 2014) of companies regarding their assessment of protectionist intent.

Table 2: How Alleged Barriers to Digital Trade Might Affect Markets/Protectionist Intent

Tariff Barriers	Market/Trade Effect	Surveyed Business Belief of Protectionist Intent
Tariffs on Digital Goods	Discriminatory, trade restricting	Yes
Nontariff Trade Barriers		
Localization Requirements	May restrict trade, may restrict access to markets	Yes
Data Flow Restrictions	Often rationalized to protect privacy or security. May restrict trade, may affect firm's ability to adopt the most efficient technologies, may create missed opportunities for business/innovation	Sometimes
IPR Infringement	Not always due to government actions but often due to inadequate governance. Can discourage investment and information flows	Sometimes
National Standards and Burdensome Conformity Assessment	Raise costs, may be discriminatory, may make it harder to enter new market	Yes
Filtering/Blocking	Equivalent of a border wall: spills-over into other markets, and may affect internet stability and generativity	No
Net Neutrality	Raise costs of some providers	No
Cybersecurity Risks	Raise costs and impedes market access	Sometimes

Sources: Fefer et al : 2017; USITC 2013, 2014; OECD 2015, 2016.

The US Government actively monitors digital protectionism. In 2014, the US Congress asked the ITC to dig deeper into the practices of major US trade partners. The ITC found that 49 nations have adopted 'digital protectionist' policies, and justified these policies as necessary to protect privacy and cyber stability. In its 2017 report (based on 2016 trade data) the US Trade Representative found digital protectionism in many of its trade partners, including Indonesia, Russia, China, the EU, and Turkey (USTR 2016b, 2017).

The US is not alone in finding digital protectionism. Canadian firms also allege that other countries are increasingly using digital protectionism, and they are calling for rules to regulate it (McKenna 2013). A 2011 study by the Conference Board of Canada found that Canada faced a multitude of barriers to digital trade (Goldfarb 2011). The European Union is also concernedas the world's largest exporter of digital services (WTO 2016, 124, Table A47; Hamilton and

Quinlain 2016). In a November 2016 speech, DG Trade Commissioner Malmström noted, "Restrictions on cross-border data flows inhibit trade of all kinds: digital and non-digital, products and services. We cannot just pretend that this doesn't exist, or that data has nothing to do with global trade" (Malmström 2016). On June 20, 2017, a prominent member of the EU Parliament, Marietje Shaake, warned that:

> "governments around the world are drawing up barriers that hinder market access or create unfair advantages for domestic companies… These barriers also have negative impacts for people, whether it be higher costs, decreased access to products and content, violations of their human rights or uncertainty and distrust regarding the use or safety of certain products. If we believe the rule of law must prevail, then fair competition must be the goal in a hyper-connected world. There can be no place for digital protectionism" (Schaake 2017).

In both its 2015 and 2016 reports on global trade barriers, DG-Trade, the European Commission agency responsible for trade policy, reported that Russia and China were increasingly closed to digital trade. The EU criticized Russia's data localization requirements, and complained that China justifies protecting the internet sector as a matter of "national security' far beyond normal international practice" (European Commission 2015, 6, 8). In its 2016 report, the Commission found that since 2008, some countries have adopted over 35 protectionist measures including localization requirements (European Commission 2016b, 8, 11).

III. It Will Not Be Easy to Set International Rules to Limit Digital Protectionism Without A Shared Set of Norms and Definitions.

The WTO would be the best place to set rules to govern digital trade because it covers 164 nations, and is therefore more consistent with the global internet. But it is not the most up-to-date trade agreement. The WTO contains several agreements that cover issues affecting digital trade. They include the Information Technology Agreement, which eliminates duties for trade in digital products;[7] the Agreement on Trade-Related Aspects of Intellectual Property Rights, which protects trade-related intellectual property pertinent to information technology, such as computer

[7] The Ministerial Declaration on Trade in Information Technology Products (the ITA) was concluded by 29 participants at the Singapore Ministerial Conference in December 1996. Now it has 82 countries. https://www.wto.org/english/tratop_e/inftec_e/inftec_e.htm

programs;[8] 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. These chapters predate the internet and associated technologies. 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. In fact, in 2011, the US questioned whether digital trade should be governed by WTO commitments under trade in goods or services and if these rules could cover the mobile Internet and cloud computing (WTO 2011). 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). Since the Doha Round in 2001, member states have been trying to negotiate new rules to govern e-commerce and trade in computer or digital services through a new agreement called the Trade in Services Agreement (TiSA). But they have not yet found consensus.[9]

The GATS e-commerce chapter sets rules governing how nations can trade services that are electronically delivered. The GATS has two sets of exceptions: the General Exceptions[10] and the National Security Exception.[11] Under these exceptions, signatory nations can restrict trade in

[8] Also see 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.

[9] NA, "New TISA Round Kicks Off In Geneva, To Include Ministerial Review," May 27, 2016, https://insidetrade.com/daily-news/new-tisa-round-kicks-geneva-include-ministerial-review; NA, "EU, U.S. consumer groups demand carve out for data protections in TISA," https://insidetrade.com/inside-us-trade/eu-us-consumer-groups-demand-carveout-data-protections-tisa

[10] The General Exceptions state "Nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures:
(a) necessary to protect public morals or to maintain public order; (b) necessary to protect human, animal or plant life or health;
(c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to:
(i) the prevention of deceptive and fraudulent practices or to deal with the effects of a default on services contracts;
(ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
(iii) safety."
-Article XIV of the GATS, https://www.wto.org/english/res_e/booksp_e/analytic_index_e/gats_02_e.htm

[11] Article XIV Security Exceptions
1. Nothing in this Agreement shall be construed:
(a) " to require any Member to furnish any information, the disclosure of which it considers contrary to its essential security interests; or

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. The public order exception may be invoked only where a genuine and sufficiently serious threat is posed to one of the fundamental interests of society. Moreover, WTO dispute settlement bodies have found that "measures must be applied in a manner that does not to constitute 'arbitrary' or 'unjustifiable' discrimination, or a 'disguised restriction on trade in services.'" Finally, when they use this exception, members should ensure that they use these exceptions in a reasonable manner so as not to frustrate the rights accorded other members by the substantive rules of the GATS (Goldsmith and Wu 2006). There is no exception in the WTO to promote local culture. In Table III, I address whether practices that the US has label "protectionist" could be banned under existing WTO rules or could be viewed as practices allowed under the exceptions, so long as they are necessary and done in the least trade-distorting manner possible.

(b) to prevent any Member from taking any action which it considers necessary for the protection of its essential security interests:
(i) relating to the supply of services as carried out directly or indirectly for the purpose of provisioning a military establishment;
(ii) relating to fissionable and fusionable materials or the materials from which they are derived;
(iii) taken in time of war or other emergency in international relations; or
(c) to prevent any Member from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.
https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm

Table III: Digital Trade Barriers and WTO Rules

Tariff Barriers	Governed by Existing WTO Rules?	Permissible under GATS Exceptions?
Tariffs on Digital Goods	Ban on tariffs (waiver)	
Nontariff Trade Barriers		
Localization Requirements	Should not violate MFN or national treatment rules	If done to protect national security?
Data Flow Restrictions		To protect privacy, security
IPR Infringement	Yes, but TRIPS is unclear about cyber-theft, piracy and DDoS attacks	
National Standards and Burdensome Conformity Assessment		
Filtering/Blocking		To protect national security, social stability, and/or public morals
Net Neutrality		
Cybersecurity Risks		To protect privacy, security

Sources: Fefer et al. 2017; USITC 2013, 2014

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).[12] 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.[13] 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 censor and filter websites (Mattoo and Schuknecht 2000, 19-20; Goldsmith and Wu 2006). Until members challenge these policies in a trade dispute or

[12] See www.wto.org/english/tratop_e/dispu_e/dispu_e.htm#disputes, Case 285.

[13] See www.wto.org/english/tratop_e/dispu_e/dispu_e.htm#disputes, Case 363.

negotiate new rules, we will not have clarity on why, how, or when governments can restrict cross-border flows (Aaronson with Townes 2012).

Meanwhile, in the absence of progress in digital trade negotiations at the WTO, the US, EU, Canada, and other nations have been actively pursuing FTAs both as a means of expanding trade in general and in setting rules to govern digital trade. However, they have only included aspirational language in these agreements, with one exception—the Trans-Pacific Partnership (TPP) (Aaronson 2016a).[14]

The US and its 11 TPP partners spent years negotiating a binding and disputable e-commerce chapter in the TPP that *requires* signatories to facilitate cross-border information flows. The signatories also delineated clear exceptions to the rules, and stated that when nations sought to use these exceptions, they must be necessary, and they must be executed in the least trade-distorting manner. The TPP contains transparency requirements that could bring much needed light, due process, and increased political participation to trade and internet-related policymaking in countries with authoritarian or secretive regimes, such as Vietnam or Malaysia. Finally, TPP builds on a "carve-out" first delineated in NAFTA (the North American Free Trade Agreement among Mexico, Canada and the US) that allows the Canadian government to subsidize or otherwise favor Canadian content over U.S. content as a way of preserving Canadian culture. "Cultural industries," as defined by NAFTA Article 2107, include those involving the publication, distribution, or sale of publications or printed music; the production, distribution, sale or exhibition of film, video recordings, audio, or music video recordings; and radio communications, intended to reach the general public. US companies want the US to limit this carve out when they renegotiate NAFTA (Fortnam 2017a).

The Obama Administration (2008-2016) negotiated TPP, and wanted to set the rules and processes governing digital trade to 'promote the digital economy through a free and open Internet' (White House 2015). As the talks progressed, US trade diplomats became increasingly concerned about digital protectionism, recognizing that it could threaten the dominance of US internet giants, which require relatively unrestricted access to operate and build new businesses like artificial intelligence and apps. Hence, TPP parties banned certain types of practices that

[14] As of July 2017, it is unclear whether the EU-Japan deal will have binding e-commerce provisions.

could fragment the internet, reduce access to information, and/or increase the cost and difficulty of doing business online (Drake, Cerf and Kleinwächter 2016, 36; Aaronson 2016a). The Obama Administration officials were also concerned about China's efforts to enforce its concept of cyber-sovereignty. Cyber-sovereignty, also known as information-sovereignty, can be defined as banning unwanted influences in a country's information space and shifting the governance of the internet from a multi-stakeholder forum to an international government body, such as the UN (Schia and Gjesvik 2017; Burgman 2016). While other nations had introduced this concept in earlier debates about cross-border information flows, US officials worried about China's policies, given the Asian nation's influence as the second largest economy and the country with the most internet users. From their perspective, the TPP allowed the US and its allies, rather than China, to set the rules regarding information flows (Froman 2017). However, in January 2017, in his first week in office US President Donald Trump announced that the US would formally withdraw from the agreement (Baker 2017). Hence, the US, the leading demander of rules to govern digital trade and to define and limit digital protectionism, gave up the only binding language regulating digital protectionism.

TPP may not be dead. At a March 2017 meeting of TPP parties, Australia and Canada stated that they plan to move forward with the TPP. Japan has already ratified the TPP, and it has passed the New Zealand legislature (Elms 2017; Caporal 2017). But as of August 2017, the Trump Administration remains wedded to "America- first strategies, and appears unwilling to reconsider TPP.

Despite Trump Administration criticism of TPP, the US Government is using TPP as a foundation to negotiate NAFTA. The US aims to secure commitments not to impose customs duties on digital products and to ensure non-discriminatory treatment of digital products transmitted electronically. The US also aims to "establish rules to ensure that NAFTA countries do not impose measures that restrict cross-border data flows and do not require the use or installation of local computing facilities" and to "establish rules to prevent governments from mandating the disclosure of computer source code." However, the USTR did not include language that encourages countries to adopt data privacy frameworks, nor does it include a demand that market access be allowed on the basis of turning over encryption codes, elements

that were included in the e-commerce and technical barriers to trade chapters of TPP (Fortnam 2017a; Hoagland with Caporal 2017).

The EU has also not yet moved forward with binding provisions regarding digital protectionism. The EU and Japan (and the EU and Mexico) drafted an e-commerce chapter which initially contained binding language regulating some aspects of digital protectionism, but instead of the chapter, the agreement includes a review clause that will allow the two sides to revisit the issue once the EU has a stated position. In July 2017, Inside US Trade reported that the European Commission trade and justice departments have been at odds over how to address cross-border data flows in trade agreements while ensuring that personal data is protected. Industry groups in the EU shot down a Commission concept paper that they thought allowed too many exceptions and trade distorting data protection (privacy) regimes. The concept paper was structured along the lines of TPP. The first paragraph laid out the principle of free cross-border data flows, followed by a paragraph laying out exceptions to the free flow of data. Similarly, the third paragraph established the principle of a ban on data localization, followed by a paragraph with exceptions to that ban. However, some observers argued that the exceptions were crafted so broadly that any measure instituted by an EU trading partner could fit into the exception, making potential trade barriers impossible to challenge (Fortnam 2017b, 2017c).

Many of America's key trade partners don't agree with all aspects of the US definition or that specific policies are protectionist in effect or intent. For example, in 2015, members of the EU Parliament objected to the US Government labelling its policies, such as data protection laws, "protectionist" (Schaake 2015). And as noted above, the Canadian government insists on cultural exceptions (which allows Canada to provide subsidies, quotas and restrictive investment policies) to maintain Canadian culture in the face of US and European competition.

In light of the failure to make progress at the WTO or through a binding FTA such as TPP, policymakers have turned to other venues in an effort to build greater understanding of the need to define and govern digital protectionism. In recent years, the OECD has issued a report defining barriers to digital trade and their spillovers as well as a major study on Economic and Social Benefits of Internet Openness (OECD 2016). In its *2016 World Development Report, Digital Dividends*, the World Bank noted that while many developing countries were beginning

to take advantage of "the digital revolution," they did not always have a policy or institutional environment for technology that enabled their citizens to benefit from digital technologies (World Bank 2016). The UN Conference on Trade and Development (UNCTAD) has also tried to help countries put in place essential elements of such an enabling environment and monitored national developments. They argue that the enabling environment includes e-transaction, consumer protection, privacy and data protection, and cyber-crime/cyber-security laws (UNCTAD 2015). In April 2017, the G-20 issued its priorities on Digital Trade noting that the G-20 should "invite relevant International Organizations, within their respective mandates, to prepare a report…under the upcoming Argentinian G20 Presidency. This report could identify factors affecting Digital Trade readiness and propose options for reducing barriers to Digital Trade and improving the performance of developing and least developed countries in this area to promote inclusive and sustainable growth." But the ministers did not define barriers to digital trade. [15]

In fact, we don't know if the practices that the US and EU describe as protectionist actually distort trade. The US and the EU publish annual reports delineating these digital trade barriers based on business or association allegations, but we do not yet have accurate statistics to measure how such policies make it harder for US or EU firms to compete in foreign markets. The Global Trade Alert, published by the Centre for Economic Policy Research, lists allegations of protectionist trade barriers, but it does not assess whether the allegations are correct and whether these strategies truly distort trade.[16] The European Centre for International Political Economy (ECIPE), a Brussels based think tank also publishes a list of barriers to digital trade.[17] The OECD publishes the Services Trade Restrictiveness Index, which measures the trade restrictiveness of sector specific policies such as telecommunications and computer services. The OECD is attempting to consolidate these measures into one complete index of barriers to digital trade.[18] Scholars are only just beginning to examine if measures such as those described by the

[15] G020 Priorities on Digital Trade, Annex Paper 3 to the Declaration of the Ministers Responsible for the Digital Economy, 4/7/2017 Dusseldorf, http://www.g20.utoronto.ca/2017/170407-digitalization-annex3.html
[16] http://www.globaltradealert.org/
[17] http://ecipe.org/dte/database/?country=US&chapter=
[18] OECD, "Expert Meeting on Using the STRI to map Restrictiveness in Digital Trade," 2/17/2017, Discussion paper.

US truly distort trade (Chander and Le 2014, 2015; Berry and Reisman 2012). However, until scholars and governments find common ground on defining and measuring digital trade, we are simply estimating the effects of alleged protectionist measures.

IV. Inconsistencies and Confusion Regarding Digital Protectionism

The US and the EU are the most vociferous in alleging digital protection. Yet so far, the US and EU have only been able to get their counterparts to limit two protectionist measures. First they agreed to ban tariffs on goods and services traded online in the WTO. Secondly, for those signatories of the TPP, participating nations agreed to ban two types of alleged protectionist behavior—data localization and barring forced technology transfers. Under such forced transfers, companies in one country might be required to hand over source code or proprietary algorithms to do business in another country (USTR 2016a).

While both the US and the EU trade bureaucracies condemn digital protectionism, both trade giants have policies and practices that these bureaucracies would target and label as trade distorting were these policies and practices adopted by others. In fact, the government of Japan, which in July 2017 announced completion of a free trade agreement with the EU, suggested that the EU must develop and clarify its position on the relationship between data protection and digital protectionism.[19]

a. Censorship: Censorship allows countries to determine what data will be available within their borders and to control internal dissent (Chander and Le 2014, 1, 47-49). When governments censor and filter the Internet and ignore the privacy rights of their citizens, people may become more reluctant to engage in free speech, participate in politics, or search for information, because such activities could make them targets of government monitoring. Various civil society groups and analysts allege that the US allows internet service providers to make unfair, opaque decisions about site takedowns, often to protect online copyrights holders. These critics see such takedowns as a form of censorship. Meanwhile in the wake of the spread of misinformation across social media platforms, a growing number of platforms practice self-

[19] NA, Japan urges EU to develop data flow provisions despite political agreement on FTA, Inside US Trade, July 7, 2017, https://insidetrade.com/daily-news/japan-urges-eu-develop-data-flow-provisions-despite-political-agreement-fta

censorship.[20] In another example, the US Government routinely condemns censorship as a barrier to trade, although it has never challenged such behavior in a trade dispute. However, in 2016, the US cited China's Great Firewall as a barrier to trade, which could mean that the US is gathering evidence to challenge such broad censorship (USTR 2016b).

The EU also criticizes censorship (including the Great Firewall) as a barrier to trade. Yet the EU provides its citizens with a right to request delinking of sites—the 'right to be forgotten.' If an individual asks to be forgotten and if an internet provider approves the request, the information will remain online at the original site, but will no longer appear under certain search engine queries. The EU provides this provision to its citizens in an effort to help its citizens protect their privacy. Some internet service providers may interpret such requests as onerous and trade-distorting, while some human rights activists believe that delinking undermines the public's access to information (Manjoo 2015; Toobin 2014).

Governments increasingly require internet firms to take down site content internet-wide that may be breach local intellectual property rules. Some observers consider such takedown requirements a form of censorship that can distort trade, especially when a government's court requires that the decision be enforced internet wide. As example, in June 2017, in Google Inc. v. Equustek Solutions Inc., 2017 SCC 34,[21] a majority of the Supreme Court of Canada upheld a worldwide interlocutory injunction that required Google to globally de-index the webpages of a defendant in a separate intellectual property infringement proceeding. In 2016, France's data protection regulators, CNIL, declared that search engines implementing France's Right to Be Forgotten must de-list such links globally and not simply take down such sites within the EU (Tummarelo 2016). On July 19, 2017, France's highest administrative court, the Conseil d'Etat, referred the dispute between the French data protection authority CNIL and Google over the legality of applying the right to be de-indexed globally to the Court of Justice of the European Union (CJEU). Given the growing number of court orders to delink or take down sites, on July 24, 2017, Google filed an injunction with the US District Court for Northern California, to

[20] https://onlinecensorship.org/; https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/us_policy.html; https://www.usnews.com/opinion/articles/2016-06-22/google-is-the-worlds-biggest-censor-and-its-power-must-be-regulated; https://citizenlab.org/2017/05/tainted-leaks-disinformation-phish/

[21] The case is at https://scc-csc.lexum.com/scc-csc/scc-csc/en/16701/1/document.do

challenge the Canadian decision.[22] A Paris based NGO, Internet and Jurisdiction, closely monitors such cases, noting that the number and impact of such cases increasingly distort cross-border information flows (Internet and Jurisdiction 2017). If other countries mandate similar decisions regarding site takedowns, firms such as Google would struggle to comply with potentially conflicting laws, and these national decisions could yield international jurisdictional conflicts (Mackey, McSherry and Ranieri 2017; Geist 2017).

But jurisdictional problems are not the only spillovers of national regulations and cross-border information flows. Scholars at the Berkman Klein Center for Internet and Society did the first empirical study of Internet filtering in 45 countries and found that as more and more websites and social media platforms have moved from HTTP to secure HTTPS connections, governments that choose to censor must broadly block content if they want to censor effectively. Moreover, the researchers found that once a government has surmounted the administrative, technical, legal and political obstacles to filtering, the government tends "to extend blocking to include political and social content as well as to the core tools and platforms." The researchers concluded that 26 of the 45 countries they sampled engaged in extensive filtering or censorship. Moreover, a growing number of countries disrupt the internet as a whole when they filter (Clark et al. 2017). The NGO Access now documented 15 internet shutdowns in 2015 and 56 by 18 countries in 2016.[23] When governments disrupt the internet, the platform can become less trusted and secure.

b. Privacy/data protection: The US Trade Representative (USTR) has adopted an inconsistent approach to privacy as a barrier to trade. The right to privacy is an internationally accepted human right under the Universal Declaration of Human Rights. Moreover, privacy is both a human right and a consumer right. In 2013, USTR argued that Canada's provinces (British Columbia and Nova Scotia) have privacy laws that discriminate against US suppliers, because they require that personal information be stored and accessed only in Canada (USTR 2014). The US also complained about Japan's uneven and Vietnam's unclear approach to privacy and argued that China's failure to enforce its privacy laws stifled e-commerce (USTR 2014, 96, 216).

[22] On France, https://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMTctMDcifQ==;on Google, https://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMTctMDcifQ==

[23] https://www.accessnow.org/keepiton/

Thus, the US simultaneously criticizes foreign governments for failing to develop clear or adequate approaches to enforcing privacy and cites privacy as a barrier to trade. Moreover, the US Government has long argued that privacy protections bolster trust in the Internet, and that they are essential to stimulating the growth of digital technologies. Although the US has worked with other governments to establish principles on privacy, it has done little to foster bridges among these various privacy principles including those by Asia-Pacific Economic Cooperation and the Organization for Economic Co-operation and Development. As a result, we do not have a shared understanding of whether privacy regulations distort trade or are legitimate regulations designed to protect human rights (and are therefore allowed under the exceptions).

EU member states also have some inconsistencies. As noted above, Commissioner Malmström has talked about digital protectionism but made it clear that data protection is not protectionist. "Let's not kid ourselves: some data restrictions out there are purely protectionist. Rules that require data to be localized in a particular place, or that impose limits on transferring data, often have no justification, other than to inhibit market access by overseas companies. That is not data protection, it is protectionism; that is our trade partners not playing fair. And that is a legitimate topic for trade deals" (Malmström 2016). However, some see the EU's stringent approach to data protection as a form of censorship (Solon 2014, Hern 2014). As noted above, European citizens have the right to demand delisting of information that breaches privacy. As it began to implement the right to be forgotten, Google said that it will censor content worldwide that it removes under the European Union's right to be forgotten mandate. But "worldwide" censorship will only apply to those searching from the EU country where the request was originally made. Google will close a loophole that currently allows people in a European country to view search results that had otherwise been deleted under the "right to be forgotten" (Google prefers the term "right to be delinked"). Google will use geo-location to ensure residents located in a given EU country can't see the search results on *any* version of the site, even as those outside the country *can* see them. Interestingly although Mexico also requires companies to protect the right to be forgotten, Google is not yet compliant (Fleisher 2017, Pickrell 2017).

The EU has announced that it aims to create a Digital Single Market (DSM) among the 27 (without the UK) EU member states. Citizens will have better online access to digital goods

and services with shared rules, and the digital economy will be better positioned to drive growth. Although the EU has one approach to data protection (the General Data Protection Regulation), many EU member have data localization requirements that make it hard to transfer data among the EU 27. These states argue that these rules are necessary to protect the privacy of their citizens.[24] Moreover, one observer contends that there are some 40 provisions in this regulation that will still allow individual member states to set their own data protection standards (Qassim 2016).

Hence, data protection regulations are a patchwork even among the 28 (soon to be 27) nations within the EU that aim to foster a common market. This fact should lead trade policymakers that are unfamiliar with this situation to educate themselves and announce that we need to find common ground on data protection rules and cross-border information flows to avoid a mismatch among national rules.

c. Cyber-theft: The US Government argues that US companies as well as government entities are victims of cyber theft. According to the US's Defense Science Board (2013), other nations use the Internet to scour, penetrate and steal information on critical technologies, including drones, robotics, communications, and surveillance technologies. The US Government is increasingly concerned about China, noting that hackers working for the Chinese government, or with the government's support and encouragement, have infiltrated computer networks of US agencies and companies and stolen trade secrets. These hackers have often provided that information to Chinese companies. In 2015, the US China Security and Economic commission reported that information was stolen from US government agencies including the Postal service, universities such as Penn State, Johns Hopkins, Carnegie Mellon, and MIT, and companies such as United Airlines. All the thefts are attributed to Chinese actors which appear to be aligned with the government but his allegation is difficult to prove) (USCC 2016, 192, 198, 199-204). In 2015, China agreed with the US that neither country's government will conduct cyber-enabled theft of intellectual property, although again, cyber theft was not clearly defined (USCC 2016, 209). Meanwhile, the US government has stressed that it does not use surveillance for commercial

[24] https://ec.europa.eu/digital-single-market/en/news/facilitating-cross-border-data-flow-digital-single-market; and https://mc.gov.pl/files/free_flow_of_data_-_non-paper_od_lm_eu_member_states_dec._2.pdf

theft. Nonetheless, in the summer of 2015, WikiLeaks provided evidence that the US Government had 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 US Government had used Germany's top spy agency to watch European corporate targets. The US Government still insists that it is not stealing corporate property and giving it to US companies. However, citizens and government officials in the US and abroad may find it hard to distinguish between cyber monitoring to prevent crime and terrorism and cyber probing to steal technologies (Aaronson 2016a).

d. *Regulatory Context*: The US argues that governments which fail to make an appropriate regulatory context for the free flow of information are effectively distorting trade. In 2015, 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 (USTR 2015). Meanwhile, the EU member states have several policies that could be considered distorting to trade. For example, not only do EU member states have different approaches to privacy, they also have different approaches to cultural "protection." Some EU members such as France have cultural exceptions (e.g. percentage of cultural goods and services that must be locally produced and broadcast). In another example, some EU member states also allow geo-blocking—the practice of denying access to users in one jurisdiction to services based on the user's geographic location.[25]

Cybersecurity regulations provide an example of the importance of finding common ground on the relationship between domestic regulation and cross-border information flows. Given the rise in malware, hacking, and disinformation,[26] governments may at times seek to

[25] http://www.screendaily.com/news/meps-make-recommendations-on-dsm-strategy/5097228.article
[26] https://www.wired.com/2016/01/the-biggest-security-threats-well-face-in-2016/; https://www.thedailybeast.com/articles/2017/03/08/who-s-behind-the-massive-cia-leak; http://cdn.defenseone.com/b/defenseone/interstitial.html?v=7.6.0&rf=http%3A%2F%2Fwww.defenseone.com%2Fideas%2F2016%2F01%2Frise-cyber-repression%2F125095%2F; and https://citizenlab.org/2017/05/tainted-leaks-disinformation-phish/; https://www.nytimes.com/2017/06/07/technology/facebook-britain-election-europe.html?ribbon-ad-idx=3&rref=technology&module=Ribbon&version=context&region=Header&action=click&contentCollection=Technology&pgtype=article; https://www.nytimes.com/2016/11/18/technology/fake-news-on-facebook-in-foreign-elections-thats-not-

restrict cross-border flows to maintain political stability, trust and personal security. In June 2017, members of the WTO debated whether or not cybersecurity strategies could distort trade. Some members were concerned that such regulations would negatively impact trade in information technology products, potentially discriminating against non-domestic companies and technologies, and possibly leading to unnecessary disclosure of commercially confidential and technical information. Others argued that cybersecurity rules are needed to address national security issues and to ensure consumer privacy, and that the measures in question were non-discriminatory (WTO 2017). In looking at the debate between China's cybersecurity regulations and US insistence that these regulations are protectionist, researcher Dan Ikenson concluded that the objectives of both governments have less to do with cybersecurity than they do with protectionism (Ikenson 2017). However, others may not believe it is so easy to ascertain protectionist intent.

V. China's Censorship at Home and Abroad: New Tactics and Market Access Consequences

China is one of the world's largest and fastest growing internet markets. Only some 50% of its citizens are online as of 2016, so the internet in China has plenty of room for growth (UNESCO 2016). Thus, many online firms believe they must compete in China. However, the Chinese internet is likely the world's most restrictive and monitored. The Open Net Initiative, a collaborative project that monitors internet censorship using both qualitative and quantitative analysis, claims that China operates "the most extensive, technologically sophisticated and broad-reaching system of internet filtering in the world" (Deibert 2008, 3). The government blocks sites by Internet protocol address and blocks and filers uniform research locators (URLs) and search engine results. The country supposedly employs 2 million individuals to censor the internet. Chinese officials argue that the nation must restrict the web to maintain social stability and security amid threats like terrorism (Reuters 2016). However, China has different censorship systems for foreign and domestic sites (Erixson, Hindley, and Makiyama 2009). Most Chinese netizens cannot access the websites for Facebook, Twitter, foreign media such as the New York Times, and many Google services. The American Chamber of Commerce in China reported that

new.html?action=click&contentCollection=Technology&module=RelatedCoverage&region=EndOfArticle&pgtype=article

79% of US companies in China have experienced blocked access to web tools and services, which raise their business costs (McDonald 2017). In addition, Chinese censorship rules lead firms to self-censor and can hobble user privacy and security (USCC 2016, 211).

Not surprisingly, the US Trade Representative describes China's internet regulatory regime as restrictive and opaque (USTR 2015, 70-72, 77-79). Legal scholar Henry Gao describes it as arbitrary and often unreasonable (Gao 2011, 371). Greatfire.org, a website monitoring Chinese censorship found 878 of 1233 Wikipedia pages and 769 of 947 google pages were censored in China.[27] Under WTO rules, China is supposed to provide a system of judicial or administrative review of such blockage, but no such system is available (Schruers 2015; Kaplan 2008).

Moreover, China's approach to censorship is evolving. The government does not only rely on paid censors, but upon the acquiescence of companies providing internet services within the country. These companies must follow local law or withdraw from the market. Take for example Amazon, which provides cloud services to customers based in China. In July 2017, Amazon's partner in China told its customers that that VPN software (software that provides a virtual private network with which individuals in China can jump over the Great Firewall) is now banned. That month, Apple removed several apps from its apps store in China that allow individuals to use VPNs (Rauhala 2017; Mozur 2017). Furthermore, on August 3, 2017, all internet data centers and cloud companies located in China were ordered to participate in a three-hour drill to hone their "emergency response" skills. They were essentially to practice taking down websites that had been deemed harmful (Jiang: 2017). With these steps, China has made it almost impossible to get around the Great Firewall.

However, China is not only censoring and effecting market access in its home market. Since 2008, researchers have found evidence that the Chinese government has exported censorship beyond its borders. In testimony before the US China Economic and Security Review Commission, Ron Deibert, the Director of the Citizen Lab at the University of Toronto, asserted that China used distributed denial of service (DDoS) attacks in Tibet, the US, UK, Canada and elsewhere since 2008. He noted that these methods deny access to information by disabling the

[27]Online Censorship in China, GreatFire.org. The site allows users to test keywords and urls. https://en.greatfire.org/analyzer

sources of information (rather than blocking requests for information as filtering systems do). Researchers find it hard to pinpoint the source of such attacks so governments can deny ever using such methods (Deibert 2008, 4). Moreover, with DDoS, China can censor abroad without asserting the heavy hand of government.

In 2015, researchers at the Citizen lab (Marczak et al. 2015) and several other organizations asserted that China essentially took down two US based websites, GitHub and GreatFire.org.[28] Github is an open source site which manages and stores revisions of projects using code and serves as a platform for online collaboration. Github hosts GreatFire.org (which monitors the Great Firewall) and the *New York Times* Chinese edition. In examining the attack, the Citizen Lab alleged that the government of China used a "Great Cannon" to harness internet traffic headed to China's most popular search engine Baidu and redirect it to flood these two overseas websites. The Great Cannon can not only shut down the connection, but apparently the hackers hijacked traffic to these addresses and replaced benign unencrypted web content with malicious content (CECC 2016, 200-201; Perlroth 2015).

The researchers noted that the attacker targeted services designed to circumvent Chinese censorship. Meanwhile, Baidu denied that their servers were compromised, although the analysts were able to prove that the hackers had injected malicious javascript into Baidu connections (Marczak et al. 2015, 1, 8-9). Hence, a Chinese company, Baidu, was hijacked and victimized as part of the attack.

China is not the only country to use a DDoS attack to disable website. Both the US and UK tampered with internet traffic to launch attacks (Marczak et al. 2015). However, neither country did so to control information. The researchers concluded that deployment of the Great Cannon was a significant escalation in state-level information control because censorship was enforced by "weaponizing users," rather than by direct government action. Moreover, China's alleged tactics created a dangerous precedent-contrary to international norms, puzzling those attempting to ascertain why China chose to act in this way (Marczak et al. 2015).

[28] The Citizen Lab report was corroborated by Robert Graham, Errata Security, "Pin-pointing China's attack against GitHub," April 1, 2015, http://blog.erratasec.com/2015/04/pin-pointing-chinas-attack-against.html?m=1; Erik Hjelmvik, March 31, 2015, China's Man-on-the-Side Attack on GitHub, http://www.netresec.com/?page=Blog&month=2015-03&post=China%27s-Man-on-the-Side-Attack-on-GitHub

DDoS attacks have occurred repeatedly in the US during 2016-2017, with attackers taking down key providers of web services like Dyn. (Dyn is a web host for part of the internet's Domain Name System, or DNS. The DNS translates user-friendly web addresses like www.fbi.gov into numerical addresses that allow computers to speak to one another and exchange information.) As example, during an October 21, 2016 attack, netizens could not visit a wide variety of sites in the US and the UK including Twitter, Reddit, CNN.com, Credit Karma, Etsy Github, the Wall Street Journal and many others (Perlroth 2016, Turton 2016). Verisign is the registrar for many popular top-level Internet domains, like .com and .net, and it monitors web conditions. In 2016, the company reported that the attacks have become more frequent, complex, and persistent. According to security expert Bruce Schneier, these attacks are calibrated to determine how well the companies can defend themselves, and what would be required to take them down. Schneier added, "We don't know who is doing this, but it feels like a large nation-state. China and Russia would be my first guesses" (Perlroth 2016; Schneier 2016). In 2017, researchers alleged (without proof) that someone used a distributed denial of services (DDoS) attack to take down the twitter site of Guo Wengu, the Chinese billionaire who now lives in the US, and who is slowly providing information on corruption among senior officials in China (Charlie 2017; Perlroth 2016).

While several research groups pinned the GitHub attack on China, we do not know who is behind the rise in DDoS attacks in the US. Moreover, while the attacks may have come from Chinese entities that may be affiliated with the Chinese government, it is impossible to provide that the Chinese government ordered these attacks. Attribution, although accepted in some courts, do not "prove" that China is beyond these actions or prove that the rise in DDoS attacks to China alone (Schneier 2016; USCC 2016). That said, the South China Morning Post reported that the government had been planning the attack for over a year.[29]

According to Bill Marczak, the leader of the Citizen Lab team, China has not used this tactic since 2015.[30] Yet the allegations of DDoS by Chinese affiliated entities in the US and UK have important implications for trade and trust in the internet. These DDoS attacks change

[29] NA, "China's 'Great Cannon' programme has been in development for about a year, sources say" http://www.scmp.com/news/china/article/1764378/chinas-great-cannon-programme-has-been-development-about-year-sources-say

[30] Communication on skype between William Marczak and Susan Aaronson, August 5, 2017.

market access conditions in the attacked company's home country since a company attacked (such as Twitter) can't serve its customers if its site is down. Thus, attacks reduce market access, raise costs for firms who must hire researchers to ascertain who is responsible for these attacks while also spending money to get their sites back These DDoS attacks also reduce internet stability and diminish the predictability of information flows (Google 2010; Gao 2011; Kaplan 2008). To put it differently, these tactics essentially bring Chinese censorship to the US and other countries. These attacks should prod policymakers to raise the question of whether the trade regime can and should address such issues.

VI. The Costs of Digital Protectionism: Direct Costs and Unanticipated Spillovers.

Digital protectionism may be self-defeating. While there is no consensus regarding how to define, let alone remedy, digital protectionism, a growing number of researchers find costly spillover effects. The ECIPE estimated that data localization regulations cost EU citizens an estimated $193 billion per year, in part due to higher domestic prices (Bauer et al. 2014). However, the costs of digital protectionism are not always economic; they can also affect the stability of the internet as a whole (Bildt 2012). In 2011, the OECD reported that Egypt's shutdown of the internet for five days led to 'direct costs of at minimum USD 90 million' (OECD 2011). A 2016 Brookings study estimated that the economic impact of internet censorship filtering and blocks was $2.4 billion, which the author noted as an understatement of the actual economic damage of lost tax revenues, the negative impact of worker productivity, etc. (West 2016). Sarah Box of the OECD says that such reductions in internet openness can affect global value chains and reduce technology diffusion, thereby undermining development and trade (Box 2016, 2). Governments that adopt digital protectionist strategies could hurt their own consumers and place their firms at a competitive disadvantage since such measures may increase costs to business (Elms 2017). In short, digital protectionist strategies can backfire.

Analysts recognize that there is no easy way to measure internet openness or closure, or the effects of digital protectionism upon the internet as a whole. Nevertheless, they agree that "the dynamism of the Internet depends in large part upon its openness" and that variants of protectionism, like censorship or data localization, can reduce that openness (Bildt 2012; Box 2016; OECD 2016). As example, some Chinese officials admit that the Great Firewall is not only

costly to maintain (with staff and constant vigilance), but also that it may deter foreign investment and innovation. On March 4, 2017, Luo Fuhe, the vice-chairman of the Chinese People's Political Consultative Conference, the top advisory body to China's parliament, stated that China's sprawling internet censorship regime is harming the country's economic and scientific progress and discouraging foreign investment. Fuhe and a few other Chinese leaders acknowledged that the Great Firewall may make it harder for China to becoming an innovation-driven economy (Gao 2017; Chu 2017; Haas 2017).

Some scholars also assert that digital protectionism undermines internet stability and interoperability. Data localization policies, filtering, or censorship can alter the architecture of the internet, which has long favored technical efficiency over state politics. When officials place limitations on which firms can participate in the network, they may reduce the overall size of the network, and once again potentially raise costs (Force-Hill 2014, 32; Daigle 2015; Drake, Cerf, and Kleinwächter 2016). Finally, digital protection can undermine access to information, reducing innovation and the ability of citizens to monitor and hold their governments to account (OECD 2016; Aaronson 2016a, 2016b).

VII. Conclusion: The Need for Common Ground

The idea of using trade agreements to regulate digital protectionism may well be one whose time has arrived. Digital protectionism is an issue that is both increasingly visible and contested. Trade policymakers are struggling to define it, develop shared norms, and regulate it. For example, some corporate officials consider European efforts to establish the digital single market as an EU wide approach to protectionism. Mark Scott of the New York Times noted, "The latest digital reforms—either on purpose or by coincidence, depending on people's viewpoints—take aim at that dominance, and potentially give European publishers and telecom companies a helping hand to compete head-on with their American rivals" (Scott 2016). On the other hand, Nicky Stewart, a former internet strategist for the UK Cabinet said the EU was simply trying to develop rules that conformed to EU values (Stewart 2017).

Digital protectionism has some commonalities with traditional protectionist objectives and strategies. Government officials have a wide range of legitimate reasons why they may seek to limit cross-border information flows. For example, many want to develop an indigenous tech

sector, requiring them to develop an effective enabling environment that includes competition, digital literacy, and infrastructure policies. In this pursuit, officials might sometimes take steps that discriminate against foreign market actors and in so doing, distort trade, even though this may not be their original intent. Policymakers also want to encourage the rule of law online and prevent unlawful behavior like the dissemination of hate speech or child pornography, fraud, identity theft, cyberattacks, and money laundering. Here again, these policies may be necessary to achieve important domestic objectives, yet they may discriminate against foreign firms (Aaronson 2016b). What may appear protectionist to one country may be seen as a legitimate and necessary regulation in another.

Advanced industrialized countries like the US and Germany are not finding it easy to put in place an effective enabling environment for digital trade at home without distorting cross-border flows. But finding this balance is even more difficult for developing countries. Many developing country policymakers lack the skill, expertise, and funds to establish an effective domestic enabling environment.[31] Digital technologies are constantly evolving and policymakers struggle to catch up.

Digital protectionism is also different from traditional protectionism because information is both a good and service, and often a public good. But some policymakers who seek to protect are also developing new tactics to protect beyond tariffs, quotas, and exchanged controls. China's alleged efforts to use DDoS attacks to censor global websites also seems to make it harder and more expensive for firms to access their home (and other) markets. Although these attacks are increasingly visible and numerous, trade officials have yet to openly discuss what this means for the meaning of market access and rules based trade.

The countries of the world need to find common ground on which practices truly distort digital trade, what should be banned, and what should be limited and clarified under the

[31] https://blogs.worldbank.org/category/tags/cybersecurity; https://blogs.worldbank.org/publicsphere/quote-week-edward-snowden; https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/world-bank-cyber-security-new-model-protecting-network; and http://www.cto.int/media/events/pst-ev/2017/cybersecurity%202017/Sandra%20Sargent%20The%20World%20Bank.pdf; http://unctad.org/en/pages/MeetingDetails.aspx?meetingid=1100

exceptions. For these reasons, government officials should work at the WTO to discuss these issues. Specifically, policymakers should:

1. Ask the WTO Secretariat to examine whether domestic policies that restrict information (short of exceptions for national security, privacy, and public morals) constitute barriers to cross-border information flows that could be challenged in a trade dispute.

2. Some governments engage in hacking or encourage state sponsored hackers to use malware or DDoS attacks to improve the competitiveness of their firms or censor the internet in other countries. Policymakers should call on the WTO to convene a study group to examine the trade implications of these tactics as a means of distorting trade and how the WTO can deal with these implications. *These tactics should be banned, although the WTO may not be the best forum to discuss these problems.*

3. The members of the WTO should monitor each other's digital trade practices during the WTO trade policy review process.

Finally, another thoughtful scholar suggested that given the unique nature of information flows, policymakers should negotiate a separate agreement. Hosuk Lee Makiyama called the proposed agreement the International Digital Economy Agreement or IDEA (Lee-Makiyama 2011). In that regard, policy makers should:

4. Propose and negotiate an international agreement that defines and limits digital protectionism and delineates clear and limited exceptions.

Bibliography

Aaronson, Susan Ariel. 2001. *Taking Trade to the Streets: The Lost History of Public Efforts to Shape Globalization.* Ann Arbor, MI: University of Michigan Press.

Aaronson, Susan Ariel. 2016a. "The Digital Trade Imbalance and Its Implications for Internet Governance." *Global Commission on Internet Governance Series*, Paper No. 25, February.

Aaronson, Susan Ariel. 2016b. "Digital Protectionism? Or Label the U.S. Government Uses to Criticize Policy It Doesn't Like?" *Council on Foreign Relations Blog*: *Net Politics*, March 3. https://www.cfr.org/blog-post/digital-protectionism-or-label-us-government-uses-criticize-policy-it-doesnt

Aaronson, Susan Ariel with Miles D. Townes. 2012. "Can Trade Policy Set Information Free?" Institute for International Economic Policy, GWU. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2189153

Ariu, Andrea. 2012. "Services vs Goods Trade: Are They the Same?" Stanford University Economics Department. https://editorialexpress.com/cgi-bin/conference/download.cgi?db_name=MWITSpring2012&paper_id=59

Ashu, Solo, ed. 2014. *Handbook of Research on Political Activism in the Information Age*. Hershey: Pa, IGI Global, p. 176. http://projekbrunei.com/asean-regional-bloggers-conference-2011.html.

Baker, Peter. 2017. "Trump Abandons Trans-Pacific Partnership, Obama's Signature Trade Deal." *The New York Times*, January 23. https://www.nytimes.com/2017/01/23/us/politics/tpp-trump-trade-nafta.html?_r=0

Bauer, Matthias, Hosuk Lee-Makiyama, Erik van der Marel, and Bert Verschelde. 2014. "The Costs of Data Localization: Friendly Fire on Economic Recovery." *ECIPE Occasional Paper Series*, Paper 3. http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf

Bauer Matthias, Martina F. Ferracane, and Erik van der Marel. 2016. "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization," https://www.cigionline.org/sites/default/files/gcig_no30web_2.pdf

Beach, Derek and Rasmus Brun Pedersen. 2013. *Process-Tracing Methods: Foundations and Guidelines*. Ann Arbor, MI: University of Michigan Press.

Behsudi, Adam. 2017. "What's Next for Canada on Trade?" *Politico*, March 15.

Berry, Renee and Matthew Reisman. 2012. "Policy Challenges of Cross Border Cloud Computing." U.S. International Trade Commission.

https://www.usitc.gov/research_and_analysis/documents/Final_Cloud_Computing_Seminar_61912_0.pdf

BIAC. No Date. "The Flow of Data Across Borders: A BIAC Trade Policy Perspective." http://biac.org/major_publications/the-flow-of-data-across-borders-a-biac-trade-committee-perspective/

Bildt, Carl. 2012. "A Victory for the Internet." *The New York Times*, July 5. http://www.nytimes.com/2012/07/06/opinion/carl-bildt-a-victory-for-the-Internet.html

Box, Sara. 2016. "Internet Openness and Fragmentation: Toward Measuring the Economic Effects." *Global Commission on Internet Governance Paper Series* No. 30, May. CIGI and Chatham House.

Broude, Tomer and Holger P. Hestermeyer. 2013. "The First Condition of Progress? Freedom of Speech and the Limits of International Trade Law." *Virginia Journal of International Law*, Research Paper No. 05-13. https://ssrn.com/abstract=2260969

Burgman, Jr. Paul R. 2016. "Securing Cyberspace: China Leading the Way in Cyber Sovereignty." *The Diplomat,* May 18. http://thediplomat.com/2016/05/securing-cyberspace-china-leading-the-way-in-cyber-sovereignty/

Burri, Mira. 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.

Caporal, Jack. 2017. "U.S. Wants to Keep TPP Standards in Bilateral Deals: Chilean Ambassador." *Inside US Trade,* March 23. https://insidetrade.com/daily-news/us-wants-keep-tpp-standards-bilateral-deals-chilean-ambassador

Chander, Anupam. 2010. "Googling Freedom (May 26, 2010)." *California Law Review*, 99: 1. And *UC Davis Legal Studies Research Paper* No. 217. https://ssrn.com/abstract=1616313

Chander, Anupam, and Le Uyen P. 2014. "Breaking the Web: Data Localization vs. the Global Internet." *SSRN*, April. http://ssrn.com/abstract=2407858

——. 2015. "Data Nationalism (March 13, 2015)." *Emory Law Journal*, 64 (3). https://ssrn.com/abstract=2577947

Charlie. 2017. "Is China establishing cyber sovereignty in the United States?" May 23. https://en.greatfire.org/news/blog

Chu, Cho-Wen. 2017. "Censorship or Protectionism? Reassessing China's Regulation of Internet Industry." *International Journal of Social Sciences and Humanity*, 7 (1), January.

Clark, Justin, Robert Faris, Ryan Morrison-Westphal, Helmi Norman, Casey Tilton, and Jonathan Zittrain. 2017. "The Shifting Landscape of Global Internet Censorship." Berkman Klein Center for Internet and Society, July 14. https://dash.harvard.edu/bitstream/handle/1/33084425/The%20Shifting%20Landscape%20of%20Global%20Internet%20Censorship-%20Internet%20Monitor%202017.pdf

Computer and Communications Industry Association. 2008. "Internet Censorship and Online Freedom." May, 2008.

Daigle, Leslie. 2015. "On the nature of the Internet." *Global Commission on Internet Governance Paper Series* No. 7, Waterloo.

Deibert, Ronald J. 2008. Written Statement to USCC, June 8. https://www.uscc.gov/Hearings/hearing-access-information-and-media-control-people%E2%80%99s-republic-china

de la Chapelle, Bertrand and Paul Fehlinger. 2016. "Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation." *Global Commission on Internet Governance Paper Series* No. 28, April 1.

Digital Europe. 2016. "GLOBAL INDUSTRY URGES TRADE MINISTERS TO ADVANCE A DIGITAL TRADE AGENDA IN TiSA NEGOTIATIONS." *Inside US Trade*, June 1. https://insidetrade.com/sites/insidetrade.com/files/documents/jun2016/wto2016_1326a.pdf

Drake, William, Vincent Cerf, and Wolfgang Kleinwächter. 2016. "Internet Fragmentation: An Overview." *World Economic Forum*. http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

Elms, Deborah. 2017. "Moving Ahead with the TPP 11." *Asian Trade Centre,* January 11. http://www.asiantradecentre.org/talkingtrade//moving-ahead-with-the-tpp11

Erixson, Frederick, Brian Hindley, and Hosuk Lee Makiyama. 2009. "Protectionism Online: Internet Censorship and International Trade Law." *ECIPE Working Paper Series* No. 12/2009. http://ecipe.org/app/uploads/2014/12/protectionism-online-internet-censorship-and-international-trade-law.pdf

European Commission. 2015. "Report From The Commission To The European Council: Trade and Investment Barriers Report 2015." Brussels, 17.3.2015 COM 127. http://trade.ec.europa.eu/doclib/docs/2015/march/tradoc_153259.pdf

European Commission. 2016a. "Digital Single Market." https://ec.europa.eu/commission/priorities/digital-single-market_en

European Commission. 2016b. "Report from the Commission to the Council and the European Parliament on Trade and Investment Barriers and Protectionist Trends." 1 July 2014—31 December 2015, SWD (2016) 204. https://ec.europa.eu/digital-single-market/en/news/facilitating-cross-border-data-flow-digital-single-market; and https://mc.gov.pl/files/free_flow_of_data_-_non-paper_od_lm_eu_member_states_dec._2.pdf

http://trade.ec.europa.eu/doclib/docs/2016/june/tradoc_154665.pdf

Fefer, Rachel, Shayerah Ilias Akhtar, and Wayne M. Morrison. 2017. "Digital Trade and US Trade Policy." *Congressional Research Service Reports*, CRS Report R44565.

Ferracane Martina F. and Hosuk Lee-Makiyama. 2017. "China's Technology Protectionism and Its non-negotiable Rationales." June. http://ecipe.org/publications/chinas-technology-protectionism/

Fleischer, Peter. 2014. "Adapting Our Approach to the European Right to Be Forgotten." *Google Blog*, March 4. https://www.blog.google/topics/google-europe/adapting-our-approach-to-european-rig/

Force-Hill, Jonah. 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.

Fortnam, Brett. 2017a. "Canada expected to stand firm on maintaining 'cultural carveout' in NAFTA." *Inside US Trade*, August 3. https://insidetrade.com/daily-news/canada-expected-stand-firm-maintaining-cultural-carveout-nafta

Fortnam, Brett. 2017b. "EU punts on data flow language in Japan deal, leaving position unresolved." *Inside US Trade*, July 6. https://insidetrade.com/inside-us-trade/eu-punts-data-flow-language-japan-deal-leaving-position-unresolved

Fortnam Brett. 2017c. "Japan urges EU to develop data flow provisions despite political agreement on FTA." *Inside US Trade*, July 7. https://insidetrade.com/daily-news/japan-urges-eu-develop-data-flow-provisions-despite-political-agreement-fta

Froman, Michael. 2017. "Cabinet Exit Memo: Trade, Growth, and Jobs: U.S. Trade Policy in the Obama Administration." *Inside US Trade*, January 5. https://insidetrade.com/sites/insidetrade.com/files/documents/jan2017/USTR%20Exit%20Memo.pdf

G-20 Meeting Hamburg. 2017. "Digital Economy Ministerial Declaration: Shaping Digitalisation for an Interconnected World." Düsseldorf, April 7. http://www.g20.utoronto.ca/2017/170407-digitalization.html

Gao, Henry. 2011. "Google's China Problem: A Case Study on Trade, Technology and Human Rights Under the GATS." SSRN, December 24. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1976611

Geist, Michael. 2017. "Blog: Global Internet Takedown Orders Come to Canada as the Supreme Court Upholds International Removal of Google's Search Results." June 28. http://www.michaelgeist.ca/2017/06/global-internet-takedown-orders-come-canada-supreme-court-upholds-international-removal-google-search-results/

Goldfarb, Danielle. 2011. "Canada's Trade in a Digital World." Conference Board of Canada, April. http://www.conferenceboard.ca/reports/briefings/tradingdigitally/default.aspx

Goldman, Eric 2011. "The OPEN Act: significantly flawed, but more salvageable than SOPA/PROTECT-IP." *Ars Technica*, December 12. https://arstechnica.com/tech-policy/2011/12/the-open-act-significantly-flawed-but-more-salvageable-than-sopaprotect-ip/

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

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

Haas, Benjamin. 2017. "Chinese Official Calls for Easing of Internet Censorship." *The Guardian*, March 3. https://www.theguardian.com/world/2017/mar/04/chinese-official-slams-internet-censorship

Hamilton, Dan and Joseph P. Quinlan. 2016. "The Transatlantic Economy in 2016, Annual Survey of Jobs, Trade and Investment." Center for Transatlantic Relations, Johns Hopkins University. http://www.transatlanticbusiness.org/wp-content/uploads/2014/05/160301-TAE-FULL-BOOK.pdf

Hern, Alex. 2014. "Wikipedia swears to fight 'censorship' of 'right to be forgotten' ruling." *The Guardian*, August 6. https://www.theguardian.com/technology/2014/aug/06/wikipedia-censorship-right-to-be-forgotten-ruling

Hoagland, Isabelle with Jack Caporal. 2017. "Lawmakers, analysts underwhelmed by USTR's NAFTA digital trade objectives." *Inside US Trade*, July 20. https://insidetrade.com/inside-us-trade/lawmakers-analysts-underwhelmed-ustrs-nafta-digital-trade-objectives

Ikenson, Dan. 2017. "Cybersecurity or Protectionism? Defusing the Most Volatile Issue in the U.S.–China Relationship." *CATO Policy Analysis* No. 815.

https://www.cato.org/publications/policy-analysis/cybersecurity-or-protectionism-defusing-most-volatile-issue-us-china

Internet and Jurisdiction. 2017. "Framing Content Takedowns Across Jurisdiction." May 12. https://www.internetjurisdiction.net/publications/paper/content-jurisdiction-program-paper

Irwin, Douglas. 1996. *Against the Tide: An Intellectual history of Free Trade*. Princeton: Princeton University Press.

Jiang, Sijia. 2017. "China holds drill to shut down 'harmful' websites." *Reuters*, August 3. http://www.reuters.com/article/us-china-internet-idUSKBN1AJ1XL

Kaplan, Gilbert. 2008. "Access to Information and Media Control in the People's Republic of China." Testimony before USCC, June 18. https://www.uscc.gov/sites/default/files/6.18.08Kaplan.pdf

Khan, Abudul Waheed. 2009. "Universal Access to Knowledge as a Global Public Good." Global Policy Forum Web Site, June. https://www.globalpolicy.org/social-and-economic-policy/global-public-goods-1-101/50437-universal-access-to-knowledge-as-a-global-public-good.html

Lacey, Simon. 2016. "The TPP and the Digital Economy: The Agreement's Potential as a Benchmark for Future Rule-Making." SSRN, November 30. https://ssrn.com/abstract=2977160

Lee Makiyama, Hosuk. 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.

Lee Makiyama, Hosuk and Frederick Erixson. 2010. "Online Protectionism Equals Censorship." *The Wall Street Journal*, January 6. https://www.wsj.com/articles/SB10001424052748704842604574641620942668590

Lennon, Carolina. 2009. "Trade in Services and. Trade in Goods: Differences and Complementarities." *Vienna Institute of International Economic Studies Series* No. 53. https://wiiw.ac.at/trade-in-services-and-trade-in-goods-differences-and-complementarities-dlp-1897.pdf

Mackey, Aaron, Corynne McSherry, and Vera Ranieri. 2017. "Top Canadian Court Permits Worldwide Internet Censorship." Electronic Frontier Foundation, June 28. https://www.eff.org/deeplinks/2017/06/top-canadian-court-permits-worldwide-internet-censorship

Malmström, Cecilia. 2016. "Trade in a digital world." European Parliament, November 17. http://trade.ec.europa.eu/doclib/docs/2016/november/tradoc_155094.pdf

Marczak, Bill, Nicholas Weaver, Jakub Dalek, Royal Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ron Deibert, and Vern Paxxson. 2015. "An Analysis of China's Great Cannon." Foci 15 Conference. https://www.usenix.org/system/files/conference/foci15/foci15-paper-marczak.pdf

Manjoo, Farhad. 2015. "The Right to be Forgotten Online is Poised to Spread." *The New York Times*, August 5. https://www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html?_r=0

Maskus, Keith E. and J. H. Reichman. 2004. "The Globalization of Public 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

McDonald, Joe. 2017. "China clamping down on use of VPNs to evade Great Firewall." *The Washington Post*, July 20. https://www.washingtonpost.com/world/asia_pacific/china-clamping-down-on-use-of-vpns-to-evade-great-firewall/2017/07/20/f3f0e51a-6d0b-11e7-abbc-a53480672286_story.html?utm_term=.15b1b5cba63e

McGee, Robert W. 1996. "The Philosophy of Trade Protectionism, Its Costs and Its Implications." *SSRN Policy Analysis* No. 10. July. https://ssrn.com/abstract=91369 or http://dx.doi.org/10.2139/ssrn.91369

McKenna, Barrie. 2013. "Businesses Push for Freedom to Share Personal Data Across Borders." *The Globe and Mail*, July 7. http://www.theglobeandmail.com/report-on-business/economy/businesses-push-for-freedom-to-share-personal-data-across-borders/article13054771/

McLaughlin, Andrew. 2007. "Censorship as Trade Barrier." Google Public Policy Blog, June 22. https://publicpolicy.googleblog.com/2007/06/censorship-as-trade-barrier.html

Mishra, Neha. 2015. "Data Localization Laws in a Digital World: Data Protection or Data Protectionism?" *The Public Sphere* (2016), December 4. https://ssrn.com/abstract=2848022

NA. 2016. "EU, U.S. consumer groups demand carveout for data protections in TISA." *Inside US Trade*, October 26. https://insidetrade.com/inside-us-trade/eu-us-consumer-groups-demand-carveout-data-protections-tisa

NA. 2016. "New TISA Round Kicks Off In Geneva, To Include Ministerial Review." *Inside US Trade*, May 27. https://insidetrade.com/daily-news/new-tisa-round-kicks-geneva-include-ministerial-review

NA. 2017a. "EU punts on data flow language in Japan deal, leaving position unresolved." *Inside US Trade*, July 7. https://insidetrade.com/inside-us-trade/eu-punts-data-flow-language-japan-deal-leaving-position-unresolved

NA. 2017b. "EU digital trade proposal in Mexican FTA talks shows it still lacks data flows position." *Inside US Trade*, May 11. https://insidetrade.com/inside-us-trade/eu-digital-trade-proposal-mexican-fta-talks-shows-it-still-lacks-data-flows-position

NA. 2017c. "Japan urges EU to develop data flow provisions despite political agreement on FTA." *Inside US Trade*, July 7. https://insidetrade.com/daily-news/japan-urges-eu-develop-data-flow-provisions-despite-political-agreement-fta

National Foreign Trade Council (NFTC), ACLI, Coalition for Services Industries, and others. 2010. "Promoting Cross-Border Data Flows: Priorities for the Business Community." http://www.nftc.org/default/Innovation/PromotingCrossBorderDataFlowsNFTC.pdf

OECD. 2011. "The Economic Impact of Shutting Down Internet and Mobile Phone Services in Egypt." February 4. http://www.oecd.org/countries/egypt/theeconomicimpactofshuttingdownInternetandmobilephoneservicesinegypt.htm

OECD. 2015. "Emerging Policy Issues: Localisation Barriers to Trade." TAD/TC/WP(2014)17/FINAL, May. http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2014)17/FINAL&docLanguage=En

——. 2016. "Economic and Social Benefits of Internet Openness." *OECD Digital Economy Papers*, No. 257. June. http://www.oecd-ilibrary.org/science-and-technology/economic-and-social-benefits-of-internet-openness_5jlwqf2r97g5-en;jsessionid=25r63um1elsw1.x-oecd-live-02

Office of the Special Trade Representative (now USTR). 1982. *A Preface to Trade*. Washington, DC: U.S. Government Printing Office.

Perlroth. Nicole. 2015. "China Is Said to Use Powerful New Weapon to Censor Internet." *The New York Times,* April 10. https://www.nytimes.com/2015/04/11/technology/china-is-said-to-use-powerful-new-weapon-to-censor-internet.html

Perlroth, Nicole. 2016. "Hackers Used New Weapons to Disrupt Major Websites Across U.S." *The New York Times*, October 21. https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html

Pickrell, Emily. 2017. "Renegotiated NAFTA Might Help Bridge Mexico-U.S. Privacy Issues." *Bloomberg Law*, May 4. https://www.bna.com/renegotiated-nafta-help-n57982087521/

Qassim, Ali. 2016. “Lack of EU Data Reg Guidance has Companies Uncertain.” *Bloomberg BNA*, April 26.

Rugaber, Christopher S. 2007. “Google asks gov't to fight censorship.” *Associated Press*, reprinted in *USA Today*, June 22. https://usatoday30.usatoday.com/tech/products/2007-06-22-2859711256_x.htm

Schaake, Marietje. 2015. “MEPs Statement on Digital Protectionism.” September 22. https://www.marietjeschaake.eu/wp-content/uploads/2015/09/2015-09-22-MEPs-Statement-on-Digital-Protectionism.pdf

Schaake, Marietje. 2017. “Working Document, Towards a Digital Trade Strategy.” June 20. https://marietjeschaake.eu/en/towards-a-digital-trade-strategy

Schneier, Bruce. 2016. “Someone Is Learning How to Take Down the Internet.” Lawfare Blog, September 13. https://www.lawfareblog.com/someone-learning-how-take-down-internet

Schia, Niels Nagelhus, and Lars Gjesvik. 2017. “China’s Cyber Sovereignty.” *Norwegian Institute of International Affairs*, Policy Brief 2, February.

Schruers, Matt. 2015. “Commercial Espionage and Barriers to Digital Trade in China, June 15.” Testimony before the US-China Economic and Security Review Commission.

Scott, Mark. 2016. “E.U. Rules Look to Unify Digital Market, but U.S. Sees Protectionism.” *The New York Times*, September 13. https://www.nytimes.com/2016/09/14/technology/eu-us-tech-google-facebook-apple.html

Solon, Olivia. 2014. “EU ‘right to be forgotten’ ruling paves way for censorship.” *Wired*, May 13. http://www.wired.co.uk/article/right-to-be-forgotten-blog

Statista. 2017. “Market capitalization of the largest internet companies worldwide as of May 2017 (in billion U.S. dollars).” https://www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/

Stewart, Nicky. 2017. “We need a grown-up debate on data localisation rules without self-interest on show.” Diginomica, May 8. http://diginomica.com/2017/05/08/need-grown-debate-data-localisation-rules-without-self-interest-show/

Swedish Board of Trade. 2016. “Protectionism in the 21st Century.” http://www.kommers.se/Documents/dokumentarkiv/publikationer/2016/Protectionism%20in%20the%2021st%20Century_webb.pdf

Tan, Yvette. 2017. “China just banned livestreaming because it's too hard to censor.” Mashable, June 23. http://mashable.com/2017/06/23/china-bans-livestreaming/#9XSzVtRSyqq3

Toobin, Jeffrey. 2014. “Annals of Law: The Solace of Oblivion – In Europe, the Right To Be Forgotten Trumps the Internet.” *The New Yorker*, September 29. http://www.newyorker.com/magazine/2014/09/29/solace-oblivion

Tummarello, Olivia. 2016. “We Won’t Let You Forget It: Why We Oppose French Attempts to Export the Right to Be Forgotten Worldwide.” Electric Frontier Foundation, November 29. https://www.eff.org/deeplinks/2016/11/we-wont-let-you-forget-it-why-we-oppose-french-attempts-export-right-be-forgotten

Turtin, William. 2016 “This is Probably Why Half the Internet Shut Down Today.” Gizmodo, Oct 21. http://gizmodo.com/this-is-probably-why-half-the-internet-shut-down-today-1788062835

UNCTAD. 2015. “Cyberlaws and regulations for enhancing e-commerce: Case studies and lessons learned Note by the UNCTAD secretariat.” TD/B/C.II/EM.5/2M 1.14.2015, January 14.

UNESCO. 2016. “China, India now world’s largest Internet markets.” September 15. http://www.unesco.org/new/en/media-services/single-view/news/china_india_now_worlds_largest_internet_markets/

US China Economic and Security Review Commission (USCC). 2016. “Annual Report: Commercial Cyber Espionage and Barriers to Digital Trade.” Chapter 4. https://www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%201%2C%20Section%204%20%20Commercial%20Cyber%20Espionage%20and%20Barriers%20to%20Digital%20Trade%20in%20China.

US Department of Commerce, Economics and Statistics Administration. 2014. “Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services.” January 27. http://www.esa.doc.gov/reports/digital-economy-and-cross-border-trade-value-digitally-deliverable-

US Department of Defense, Defense Science Board. 2013. “Task Force Report: Resilient Military Systems and the Advanced Cyber Threat.” January. http://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf

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.

USTR. 2011 “United States Seeks Detailed Information on China’s Internet Restrictions.” https://ustr.gov/about-us/policy-offices/press-office/press-releases/2011/october/united-states-seeks-detailed-information-china%E2%80%99s-i

USTR. 2014. “National Trade Estimate Report on Trade Barrier.” https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2014-NTE-Report

——. 2015. “National Trade Estimate Report on Trade Barriers.” https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2015/2015-national-trade-estimate

——. 2016a. “TPP Promoting Digital Trade Fact Sheet.” https://ustr.gov/sites/default/files/TPP-Promoting-Digital-Trade-Fact-Sheet.pdf

——. 2016b. “National Trade Estimate Report on Trade Barriers.” https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2016/2016-national-trade-estimate

——. 2017. “National Trade Estimate Report on Trade Barriers.” https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2017/2017-national-trade-estimate

West, Darrell. 2016. “Internet Shutdowns Cost Countries $2.4 billion Last Year.” Center for Technology Innovation at the Brookings Institution, October. https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf

White House, President Barack Obama. 2015. “Fact Sheet: How the Trans-Pacific Partnership (TPP) Boosts Made in America Exports, Supports Higher-Paying American Jobs, and Protects American Workers.” October 5. https://www.whitehouse.gov/the-press-office/2015/10/05/fact-sheet-how-trans-pacific-partnership-tpp-boosts-made-america-exports

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.

WTO. 2016. “World Trade Statistical Review: 2016.” https://www.wto.org/english/res_e/statis_e/wts2016_e/wts2016_e.pdf

WTO. 2017. “Members debate cyber security and chemicals at technical barriers to trade committee.” https://www.wto.org/english/news_e/news17_e/tbt_20jun17_e.htm

Wu, Tim. 2006. “The World Trade Law of Censorship and Internet Filtering.” *Chicago Journal of International Law*, 7 (1), Article 12. http://chicagounbound.uchicago.edu/cjil/vol7/iss1/12

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.

Web sites

“Data vs. Information.” Diffen.com. http://www.diffen.com/difference/Data_vs_Information

Open Net Initiative. 2012. Access Contested, China. http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-china.pdf