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

What Are We Talking about When We Talk about Digital Protectionism?

IIEP-WP-2018-13

Susan Ariel Aaronson
George Washington University

December 2018

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

World Trade Review (2018), 0: 0, 1–37
 doi:10.1017/S1474745618000198

What Are We Talking about When We Talk about Digital Protectionism?

SUSAN ARIEL AARONSON*

Elliott School of International Affairs, George Washington University, USA

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 use process tracing to examine the state and implications of digital protectionism. I make five points: First, I note that digital protectionism differs from protectionism of goods and other services. Information is intangible, highly tradable, and some information is a public good. Secondly, I argue that it will not be easy to set international rules to limit digital protectionism without shared norms and definitions. Thirdly, the US, EU, and Canada have labeled other countries policies' protectionist, yet their arguments and actions sometimes appear hypocritical. Fourth, I discuss the challenge of Chinese failure to follow key internet governance norms. 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. Finally, I note that digital protectionism may be self-defeating. I then draw conclusions and make policy recommendations.

1. Introduction

Victor Hugo once wrote, '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 the internet is built on global data flows, he noted the global internet allows everyone to potentially become an importer or exporter of services and goods, and thus, '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 WTO members 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).

* Email: saaronso@gwu.edu
The project benefited from funding from the Economic Research Institute of Asia.

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 United States Trade Representative (USTR) to fight censorship as a trade barrier (Rugaber, 2007). Google's Andrew McLaughlin 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, business associations, and scholars picked up on the notion that censorship, blocking, and redirection of internet traffic constituted a barrier to trade and new form of protectionism (Riley, 2007; Biggs, 2007; Beaumont, 2010; Calinoff, 2010; Computer and Communications Industry Association, 2008; NFTC, 2010; Swedish Board of Trade, 2016; Gao, 2011; Erixon and Lee-Makiyama, 2010, Chander, 2011). The United States explored challenging censorship. In 2011, USTR sent a letter to the Chinese Ministry of Commerce requesting information on the trade impact of Chinese policies that may block US companies' websites in China (USTR, 2011). The Chinese government never responded, and the United States did not launch a trade dispute. Without clarity from a trade agreement or dispute, policymakers do not know if censorship is distorting trade in data.

Moreover, when governments have attempted to make rules to govern data flows, they have placed such language in e-commerce chapters, which the United States and EU have recently renamed 'digital trade chapters' (USTR, 2017b; European Commission, 2017c). But policymakers still do not agree on how to define digital trade. According to the Organisation for Economic Co-operation and Development (OECD), digital trade is all cross-border trade transactions that are either digitally ordered, facilitated, or delivered (OECD and IMF, 2017: 4). The United States defines digital trade as goods and services delivered via the internet and/or associated technologies (Fefer *et al.*, 2017). Hence, without shared norms and definitions, policymakers will struggle to develop rules to limit barriers to data flows.

Herein, I examine how policymakers (and others) talk about and define barriers to cross-border data flows. I use process tracing to examine how policies towards digital protectionism, particularly in the United States and the EU, have evolved over time. Scholars use process-tracing in social science to study causal mechanisms and to link causes with outcomes (Beach and Pederson, 2013). Although individuals, firms and governments are quick to describe a policy as 'protectionist'; these same individuals, firms, and governments have not found common ground on defining or regulating such practices.

Herein I will put forward a clear terminology. First, many analysts use 'data' and 'information' interchangeably, equating cross-border data flows with information flows. But they are not the same. I define data as unprocessed facts or details, whereas information is processed, organized, or structured data. Thus, information is a subset of data and in many trade agreements put forward by countries such as

the US, EU, and Canada, they include language regarding such data flows in their e-commerce chapters. However, when describing barriers to data flows, scholars and policymakers often rely on 'digital protectionism' more than 'data protectionism'.[1] They may recognize that the term data protectionism can easily be confused with personal data protection (regulations to protect individuals' privacy online.) Yet digital protectionism is a broad term that refers to a wide range of barriers both to e-commerce and to cross-border data flows. In this article, I focus only on barriers to cross-border data flows.

I make five points:

1. Digital protectionism differs from traditional protectionism, because trade in data is different from trade in goods and other services. Data are intangible, highly tradeable, and some types of data, when processed, are 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. We have not yet achieved those shared norms and definitions.
3. Many allegations of digital protectionism are concerns about different approaches to regulating the data flows that underpin the internet within national borders. Although the United States and the EU are trying to create shared rules, the two trade giants have also been the most vociferous in describing other countries' approaches as 'protectionist'.
4. China provides a good example of how the failure to achieve shared norms before achieving clear regulations may lead to trade disputes. China allegedly has used a wide range of cyber strategies, including DDoS attacks (bombarding a website with service requests), to censor data flows and impede online market access beyond its borders. But nations have not yet openly discussed whether such practices distort trade, although they clearly destabilize all or parts of the internet.
5. Digital protectionism can lead to unanticipated side effects, including reduced internet stability, generativity, and access to information (Hill, 2014; Clark *et al.*, 2017). Such actions could also disrupt communications, increase costs, and reduce data security. These effects will not just be felt in the nation that relies on such protectionism. When one or more governments censor the internet, it can reduce the platform's openness and stability (Bildt, 2012; Box, 2016). Additionally, 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. To begin with, I discuss the importance of data to economic growth and trade. Next, I define 'protectionism' and 'digital

1 On 19 March 2018, a Google search, 'digital protectionism' yielded some 60,300 results, while 'data protectionism' yielded some 2,000 results. See https://tinyurl.com/ycbyp6q6 and https://tinyurl.com/yc8y2c3h.

protectionism' and illuminate the relationship between digital protectionism, domestic regulations, and trade/market distortions. I then examine what trade agreements say about digital protectionism and explain why it is so difficult to develop shared rules without shared definitions and norms. I discuss what the United States and EU say about digital protectionism and show that their practices, at times, appear confusing and/or contradictory. I argue that as technologies and public opinion about privacy and security evolve, citizens will demand greater regulation (e.g. regulation of artificial intelligence, which is built on cross-border data flows). In so doing, I examine perceptions of what is legitimate regulation. Furthermore, I focus on Chinese digital protectionism and how it may distort trade not only in the home market but other countries as well, which is a challenge for trade policymakers. Finally, I provide policy recommendations.

2. The role of data in trade

Data and information have long been a key component of trade, but recently data have created new forms of trade. However, all forms of data-driven trade are not all the same. We define-e-commerce as sales of physical goods both among businesses and between businesses and consumers. Digital trade is a broader term that encompasses goods and services delivered via the internet and associated technologies (such as cloud computing services and voice-over-internet calls. Firms and individuals have built on cloud computing to create brand new online services such as apps, internet-connected devices (Internet of Things [IoT]), and services built on artificial intelligence (AI) such as personal assistants.[2]

Data flows move across borders when individuals, companies, or governments authorize data to be transferred from one country (the source of data) to another country where the data may be processed (e.g. payroll) or used (e.g. to better counteract criminal patterns) (USITC, 2013, 2014; Nicholson and Noonan, 2014). Additionally, once the data have crossed from one country to another the source country may not control it.

Policymakers are just beginning to come up with ways to measure the impact of digital technologies upon trade (OECD and IMF, 2017: 15). In 2016, the McKinsey Global Institute estimated around 50% of the world's traded services were in digital form, while e-commerce accounted for approximately 12% of all goods traded across borders (Manyika *et al.*, 2016). The UN and OECD note the lack of shared definitions and ever-changing technologies make it difficult to effectively measure e-commerce, let alone digital trade (OECD, 2016, 2017; Barefoot *et al.*, 2018). Likewise, in 2017, the International Monetary Fund (IMF) and OECD observed:

2 Firms rent out space on their servers and provide storage and other services via cross-border data flows to customers' in-house computers.

> the intangible nature of digitalized services has created strong fiscal incentives for their source (country of origin) to be located wherever that may be most advantageous, which poses new challenges for the way international trade and investment policy-making is made as well as how international trade … is measured. In addition, significant income streams can now be generated through data itself, the collection and dissemination of which is subject to myriad national laws, for example, governing privacy … Barriers to data flows can give rise to barriers to trade. (OECD and IMF, 2017: 3)

Researchers and policymakers cannot even agree on an appropriate taxonomy. The US government distinguishes among categories of transactional data flows based on the relationship between the sender and recipient and the type of transaction that connects them (Nicholson and Noonan, 2014). In contrast, the OECD focuses on three attributes: (1) whether data are digitally ordered, (2) whether data are a good, a service, or information, and (3) who is engaged in the transaction: businesses, consumers, or government (OECD, 2017). Ciuriak and Ptashkina (2018) suggest a third taxonomy based on delivery modes and the nature of the parties to the transactions. Sen and Aaronson take a more granular approach. Sen (2017) distinguishes among personal data, company data, business data, and social data, and refers to metadata as business and social data. Aaronson differentiates between personal data, public data, confidential business data, machine-to-machine data, and metadata (Aaronson and LeBlond, 2018).

The types of data matter because most trade agreements include exceptions – where governments can breach their obligations to encourage trade flows to achieve legitimate policy objectives such as protecting privacy, national security, or public morals. Both Sen and Aaronson note that who controls the data and where the data are controlled should be key factors in any taxonomy or set of rules, because such aspects influence the benefits that firms and consumers can reap from trade and the purpose and purview of regulation designed to protect individuals' personal data, security, and other non-trade objectives Clearly, governments are regulating personal data and the services that use it more stringently than machine-to-machine data, recognizing that regulation is essential to maintaining trust online.

3. How might we define digital protectionism?

To best understand digital protectionism, we first need to understand the meaning of protectionism. According to Irwin (1996), protectionism is both an ideology and a government act. 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, the USTR) drafted a primer on trade. It defined protectionism as 'the setting of trade barriers high enough to discourage imports or to raise their prices sufficiently to enable relatively

inefficient domestic producers to compete successfully with foreigners' (Office of the Special Trade Representative, 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. Protectionism is about altering market conditions and distorting trade in ways that favour domestic producers over their foreign competitors. However, this definition is outdated, since protectionism in all countries depends 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, and 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 signatories to forbid certain types of protectionist practices. But policymakers have also long recognized that policies that may appear protectionist may not have been designed to achieve trade-distorting effects. For this reason, trade agreements include 'exceptions', which allow governments to breach the rules to achieve other important policy goals. As an 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). And unsurprisingly, individuals have alleged that governments have distorted trade in data since the early days of computer services (Aaronson, 2017a; Drake *et al.*, 2016) But in the past four years, the number and allegations of digital protectionism have increased dramatically (Cory, 2018, 2017; Bauer *et al.*, 2014, 2016; Chander and Le, 2014; USITC, 2013, 2014; Froman, 2017). 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 regulations or subsidies to favour domestic providers of data or alter market conditions in country A. But protectionism in services is different from protectionism in goods, as the object of regulation is the producer, rather than the product (Hindley, 1988).

Digital protectionism differs from traditional protectionism in five key ways.

- First, many services from payroll to data analytics rely on access to cross-border data flows. These data flows may yield a good, a service, or both (Ariu, 2012). The United States and OECD characterize downloaded films or music as a good (OECD, 2016; Barefoot *et al.*, 2018). In contrast with physical goods, netizens can trade that same digital good simultaneously. Moreover, trade in digital services differs from trade in other services because suppliers and consumers do not need to be in the same physical location for a transaction to occur.). Given these attributes, 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, trade in data is fluid and frequent, and location is hard to determine on the borderless network. Trade in the same set of data can occur repeatedly in

nanoseconds (e.g. when millions of people download Beyoncé's latest song). Researchers and policymakers may find it hard to determine what is an import or export. They also struggle to ascertain when data are 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 cannot easily determine jurisdiction, because data can be routed through a US server to another jurisdiction. Consequently, data flows may travel through several countries before these flows reach their destination (de la Chapelle and Fehlinger, 2016).

- Third, economists generally agree that many types of data are public goods, which governments should provide and regulate effectively. Furthermore, when states restrict the free flow of data, they reduce access to information, which in turn can diminish economic growth, productivity, and innovation domestically and globally (Maskus and Reichman, 2004: 284–285; Khan, 2009; OECD, 2016). They can also affect the functioning of the internet (Hill, 2014: 32; Daigle, 2015; Clark *et al.*, 2017). Hence, if officials restrict cross-border data flows, they may create many unintended consequences.
- Fourth, although trade in data occurs on a shared platform (the internet) held in common, firms, users, and governments do not all have the same responsibility for its stability. Corporations run much of the internet but they can't respond to, or see many of, the threats. Meanwhile, many companies are essentially data collecting and selling firms; they provide free services to netizens in return for the use of their personal data (e.g. Google search and Facebook's social network). In this model, individuals do not understand or recognize their responsibility for internet security and stability. Recognizing this 'tragedy of the commons', governments are individually developing regulations to protect the safety and security of their netizens (Davidow, 2012). Some of these policies may, without intent, distort trade in cross-border data flows. For example, some countries may feel it necessary to regulate the data flows that fuel artificial intelligence (AI), while others may want to regulate the use of AI to delineate what news their citizens see (Aaronson, 2018; McAuley, 2018).
- Fifth, in contrast with their efforts to define legitimate regulation for e-commerce, there is no clear model that policymakers can use to distinguish between legitimate and trade-distorting data flow regulation. In a survey of its 194 members, UNCTAD found that some 77% of its members had e-transaction laws, 50% had consumer protection laws, 58% had privacy laws, and 72% had cybercrime laws to facilitate an appropriate enabling environment (UNCTAD, 2015). But policymakers have not yet figured out whether or how to regulate data analytics, AI, and other new technologies that rely heavily on personal data (Owen, 2018). Governments are also trying to ascertain whether and how to contest the monopoly power of the big platforms and opacity of algorithms used by many platforms to bring us news, connect us to friends, and organize and improve our lives. Responding to this lack of clarity, the OECD called for greater efforts to find

common ground on non-trade-distorting regulations designed to protect privacy and security. It pointed to the Sanitary and Phytosanitary Standards (SPS) and Technical Barriers to Trade (TBT) agreements at the WTO, which are designed to ensure that such measures should not represent disguised restrictions on trade nor be more trade-restrictive than necessary (Lopez Gonzalez *et al.*, 2016: 58). While threats to public or animal health (e.g. Severe Acute Respiratory Syndrome-SARS) can be global or affect many nations, threats to data security are more frequent then animal diseases or disputes about electrical standards. Moreover, domestic regulations that allow nations to censor or filter the internet or use DDoS attacks can affect not just market access in one or three countries, but the platform's stability (West, 2017). Hence, these agreements may help to describe what is or is not legitimate regulation but are probably less useful in providing guidance as to the broader effects upon the internet.

4. The ever-expanding US definition of digital protectionism

The United States was likely the first government to define digital protectionism because digital trade is particularly important to the US economy. The US International Trade Commission (USITC) estimated 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. USITC also asserted that the expansion of digital trade caused real wages to increase by 4.5% to 5% and boosted US aggregate employment by up to 1.8% while reducing average trade costs by 26% (USITC, 2014). This is not surprising, as the United States is home to 11 of the world's 15 largest internet businesses (Statista, 2017).[3] The US Department of Commerce reported that digitally delivered services accounted for about half of all services trade and in 2016 the digital economy accounted for 6.5% of current dollar US GDP (Fefer *et al.*, 2017: 8; Barefoot *et al.*, 2018: 3).

The US definition of digital protectionism keeps growing, as the internet and associated services change over time. In 2013, at the behest of the US Senate Finance Committee, USITC 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 (USITC, 2013). USITC 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,[4] 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

3 China is home to the other four.
4 Onlinecensorship.org 'What is Online Censorship?', https://onlinecensorship.org/.

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 WTO rules. Table 1 provides an overview of policies the United States labels as protectionist and provides examples of countries that have adopted these policies.

Table 2 below attempts to illuminate how these policies might affect markets. In column 1, I discuss market/trade effects as well as whether US experts and executives perceive that a measure is intended to distort trade. I rely on survey data collected by OECD (2016b) USITC (2013, 2014) about companies and their assessments of protectionist intent.

Table 3 uses the criteria of the SPS and TBT agreement to assess alleged barriers to cross-border data flows. It includes all the types mentioned in the other tables that the United States has described and new barriers such as regulations to prevent disinformation and DDoS attacks.

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

The United States 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 Canada faced a multitude of digital trade barriers (Goldfarb, 2011). The EU is also concerned, because it is the world's largest exporter of digital services (WTO, 2016: 124, Table A47; Hamilton and Quinlan, 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' (Malmström, 2016). On 20 June 2017, a prominent EU Parliament member, Marietje Shaake, warned:

> 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 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 justified protecting the internet sector as a matter of national security far beyond normal international practice (European Commission, 2015a: 6, 8). In its 2016 report, the Commission found

Table 1. Listing of barriers to digital trade

	Countries	Description
Tariff barriers		
Tariffs on digital goods	Only applied by non-members of the WTO, ITA, or FTAs	
Non-tariff trade barriers		
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 data in local servers or process it locally
IPR infringement	China	Cybertheft 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); US International Trade Commission (2013, 2014).

that since 2008, some countries have adopted over 35 data protectionist measures, including localization requirements (European Commission, 2016: 8, 11). In its 2017 report, the EU only commented on China's digital protectionism and heavy internet regulation (European Commission, 2017a).

Many of the United States' key trade partners do not 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 EU policies, such as data protection laws, as '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.

5. The need for a shared set of norms and definitions

The WTO is the best place to make rules to govern digital trade, because it covers 164 nations and is therefore global like the internet. But it is not the most up-to-date

Table 2. How alleged barriers to digital trade might affect markets/protectionist intent

	Market/trade effect	Surveyed business belief of protectionist intent
Tariff barriers		
Tariffs on digital goods	Discriminating, trade-distorting	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 data 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).

Table 3. SPS and TBT alleged barriers to cross-border data flows

Type state policy or action	Disguised restriction on trade	Do less trade restrictive strategies exist?
Regulations to limit disinformation	Maybe	Rely on exceptions?
Regulation to limit DDoS	Maybe	Rely on exceptions?
Localization requirements	Yes	Yes
Data flow restrictions	Maybe	Yes, but depends on objective
IPR infringement	Maybe	Sometimes
National standards and burdensome conformity assessment	Maybe	Yes
Filtering/blocking	Maybe	Yes, but more tailored/clearer regulation is needed
Net neutrality rules	No	Maybe
Malware or DDoS attacks	Yes	Yes

Sources: Fefer *et al.* (2017); USITC (2013, 2014); OECD (2015, 2016); World Trade Organization (2018).

multilateral trade agreement. The WTO includes several agreements that cover issues affecting digital trade, such as: the Information Technology Agreement (ITA), which eliminates duties for trade in digital products; the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs), which protects trade-related intellectual property pertinent to information technology; and the General Agreement on Trade in Services (GATS), which has chapters on financial services, telecommunications, and e-commerce that relate to cross-border data 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 2011, the United States questioned whether WTO commitments for goods and services trade should govern digital trade and if they could cover the mobile internet and cloud computing (WTO, 2011). Academics and business leaders have also argued that the WTO's rules are incomplete, outdated, and in need of clarification (Burri, 2013; Lee-Makiyama, 2011). Since the Doha Round in 2001, WTO member states have tried 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 (European Commission, 2018b; WTO, 2017).

According to the WTO Analytical Index,[5] the GATS e-commerce chapter sets rules governing how nations can trade electronically delivered services. The GATS has two sets of exceptions: the General Exceptions and the National Security Exception.[6] Under these exceptions, signatory nations can restrict trade in the interest of protecting public health, public morals, privacy, national security, or intellectual property, as long as such restrictions are necessary and proportionate and do not discriminate among WTO member states. 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, countries should ensure that they use these exceptions in a reasonable manner so as not to frustrate the rights that they have accorded to other members (Goldsmith and Wu, 2006). WTO does not have an exception to promote local culture. Table 4 shows whether practices that the United States has labelled 'protectionist' could be banned under existing WTO rules or viewed as practices allowed under the exceptions, if they are necessary and done in the least trade-distorting manner possible.

5 WTO Analytical Index, www.wto.org/english/res_e/publications_e/ai17_e/ai17_e.htm.

6 General Agreement on Trade in Services (GATS), 'Marrakesh Agreement Establishing the World Trade Organization', Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167, 15 April 1994, www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm.

Meanwhile, although the GATS states nothing explicitly about data flows, WTO members have begun to apply these obligations when settling disputes about cross-border data flows (Wunsch-Vincent, 2006; Goldsmith and Wu, 2006). The WTO Dispute Settlement Body has adjudicated two trade disputes related to data flows.[7] In the first dispute, after Antigua challenged the US 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 (i.e. not discriminating between foreign and domestic providers).[8] In the second dispute, the WTO Appellate Body examined China's restrictions on publications and audio-visual products, noting that commitments for distribution of audio-visual products must extend to the distribution of such products on the internet.[9] However, neither dispute 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 negotiate new rules, we will not have clarity on why, how, or when governments can restrict cross-border data flows (Aaronson and Townes, 2012).

Meanwhile, in the absence of progress in digital trade negotiations at the WTO, the United States, 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. Only two such free trade agreements (FTAs) – the Comprehensive and EU Mexico – include binding language on digital trade and limits on some types of digital protectionism. (USTR, 2016a; Aaronson, 2016a).[10]

Under US President Barack Obama (2008–2016), the United States and its 11 TPP partners spent years negotiating a binding and disputable e-commerce chapter in the Trans-Pacific Partnership (TPP) that *requires* signatories to facilitate cross-border data flows. These 12 countries also delineated clear exceptions and stated that, when nations sought to use them, they must be necessary and executed in the least trade-distorting manner. This first version of TPP (with the United States) contained transparency requirements that could bring much needed clarity, due process, and increased political participation in trade and internet-related policymaking in countries with authoritarian or secretive regimes (e.g. Vietnam or Malaysia). Finally, TPP built on a 'carve-out' first delineated in

7 The two disputes are Appellate Body, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services* (hereinafter *US–Gambling*), WT/DS285/AB/R, adopted 20 April 2005, DSR 2005: XII, p. 5663 (and Corr.1, DSR 2006: XII, p. 5475); Appellate Body, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products* (hereinafter *China – Publications and Audiovisual Products*), WT/DS363/AB/R, adopted 19 January 2010, DSR 2010: I, p. 3.

8 *US – Gambling*.

9 *China – Publications and Audiovisual Products*.

10 EU-DG Trade, Modernization of EU GA, Digital Trade, http://trade.ec.europa.eu/doclib/docs/2018/april/tradoc_156811.pdf.

Table 4. Digital trade barriers and WTO rules

	Governed by existing WTO rules?	Permissible under GATS exceptions?
Trade barriers		
Tariffs on digital goods	Ban on tariffs (waiver)	
Non-tariff 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 cybertheft, 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).

NAFTA (the North American Free Trade Agreement)[11] that allows the Canadian government to subsidize or otherwise favour Canadian content over US 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 public. US companies want the United States to limit this carve-out when they renegotiate NAFTA (Fortnam, 2017a).

The Obama administration wanted to create the rules and processes governing digital trade to 'promote the digital economy through a free and open Internet' (Obama, 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 (AI) and apps. Hence, TPP parties banned certain types of practices that could fragment the internet, reduce access to information, and/or increase the cost and difficulty of doing business online (Drake *et al.*, 2016: 36; Aaronson, 2016a). Given China's global influence as the second-largest economy and the country with the most internet users, Obama administration officials were also particularly concerned about China's

11 Canada, the United States, and Mexico are NAFTA signatories.

efforts to enforce its concept of cyber-sovereignty, although other nations had introduced this concept in earlier debates about cross-border data flows.[12] 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). From the US perspective, the TPP allowed the United States and its allies, rather than China, to set the rules regarding data flows (Froman, 2017). However, in January 2017, in his first week in office, US President Donald Trump announced the United States' formal withdrawal from TPP (Baker, 2017). Hence, the United States, the leading demandeur of rules to govern digital trade and define and limit digital protectionism, gave up the only binding language regulating digital protectionism. The other 11 nations made some changes to the TPP, renamed it the CTPP, and signed it on 8 March 2018. It will take effect as soon as member states approve the agreement (Yaxley, 2018).

Despite the Trump Administration 's criticism of CPTPP, the US government is using CPTPP as a foundation to renegotiate NAFTA. The United States aims to secure commitments not to impose customs duties on digital products and to ensure non-discriminatory treatment of digital products transmitted electronically; '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 'establish rules to prevent governments from mandating the disclosure of computer source code'. But in truth USTR is less ambitious for NAFTA. USTR has not included language in NAFTA that encourages countries to adopt a floor for rules protecting personal data; nor has it stated that signatories are not allowed to condition market access on the provision of source code as in CPTPP. However, in reflection of the rising import of artificial intelligence, the United States proposed that NAFTA add a ban on mandating disclosure of proprietary algorithms (Fortnam, 2017a; Hoagland and Caporal, 2017; USTR, 2017b).

The EU has also not yet moved forward with binding provisions regarding digital protectionism. The EU and Japan 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 (European Commission, 2017c; Fortnam, 2017b and 2017c). After deliberating for months, the EU announced its approach to digital trade and digital protectionism in February 2018. The strategy has personal data protection at its core. In its trade agreements (e.g. the renegotiated EU–Mexico Global Agreement), the EU will

12 Cyber sovereignty, also known as data sovereignty, can be defined as banning unwanted influences in a country's data 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).

insist on three pillars: (1) a horizontal clause covering the free flow of both personal and non-personal data; (2) a ban on data and server localization requirements; and (3) language that safeguards the EU's right to regulate personal data, including language that the first two pillars cannot be subject to investor-state challenges or included in regulatory dialogues. In so doing, the EU made it clear that its vision of data protection cannot be challenged as a barrier to trade (European Commission, 2018a).

International organizations have tried to build greater understanding of the need to define and govern digital protectionism. In 2016, the OECD issued a report defining barriers to digital trade and their spillovers as well as a major study on the 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, 2015) has also tried to help countries put in place essential elements of an enabling environment and monitor national developments. In April 2017, the G-20 issued its priorities on digital trade noting 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. (Federal Ministry for Economic Affairs and Energy, 2017)

But the G-20 ministers did not define barriers to digital trade.

In fact, we do not know if the practices that the United States and EU describe as protectionist distort trade. The United States and 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 Centre for Economic Policy Research's *Global Trade Alert*[13] lists allegations of protectionist trade barriers, but it does not assess whether the allegations are correct or if these strategies distort trade. The European Centre for International Political Economy (ECIPE, 2018), a Brussels-based think tank, also publishes a list of barriers to digital trade and will shortly publish an index, the Digital Trade Restrictiveness Index (DTRI), that measures how countries in the world restrict digital trade. The DTRI is based on a wide spectrum of digital trade policies covering more than 100 policy measures across 64 countries worldwide. The index will be the first global initiative to provide transparency of applied digital trade restrictions and sheds light on how

13 http://www.globaltradealert.org/.

countries compare with each other (ECIPE, 2018). 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 also attempting to consolidate these measures into one complete index of barriers to digital trade. Meanwhile, scholars are only just beginning to examine if measures such as those described by the United States truly distort trade (Chander and Le, 2014, 2015; Berry and Reisman, 2012). Until scholars and governments find common ground on defining and measuring digital trade, we are simply listing and describing these alleged protectionist measures.

6. US and EU perspectives on what is legitimate regulation vs. trade-distorting

The United States and EU are the most vociferous in alleging digital protection. Yet, so far, the United States and EU have only been able to get their counterparts to agree to limit three protectionist measures: taxes on digital flows, data localization, and forced technology transfers (USTR, 2016a).

While both the United States and the EU condemn digital protectionism, both trade giants have policies and practices that they would target and label as trade-distorting were these policies and practices adopted by other countries. In fact, the government of Japan, which in July 2017 announced completion of its FTA with the EU, suggested the EU develop and clarify its position on the relationship between data protection and digital protectionism (Fortnam, 2017c).

Censorship: Censorship allows countries to determine what data will be available within their borders and control internal dissent (Chander and Le, 2014: 1, 47–49). When governments censor and filter the internet, and ignore their citizens' privacy rights, 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. The US Constitution sets limits on how and when individuals can censor free speech. However, various civil society groups and analysts allege that the United States allows internet service providers (ISPs) 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-censorship (Onlinecensorship.org; Chan *et al.*, 2011; Epstein, 2016; Hulcoop *et al.*, 2017). In addition, US policymakers may be under increasing pressure to limit access to some information posted online. In the wake of fake news and revelations that Americans who get their news from online platforms such as Facebook may have been manipulated algorithms, bots, and disinformation, there is growing pressure in the United States to regulate disinformation (Tufekci, 2018; West, 2017). Republican and Democratic congressmen are pressuring internet platforms such as Google, Facebook, and Twitter to do more to fight false information and stop foreign

infiltration. To some observers, however, this response smells of censorship (Kravets, 2017; Myers and Wee, 2017).

The US government routinely condemns censorship as a barrier to trade, although it has never challenged such behaviour in a trade dispute. However, in 2016, the United States cited China's Great Firewall as a trade barrier, which could mean that the United States is gathering evidence to challenge broad censorship (USTR, 2016b). In 2018, the United States asked the WTO services council to discuss China's cybersecurity rules as a barrier to the free flow of data (WTO, 2018).

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 an ISP approves the request, the information will remain online at the original site but will no longer appear under certain search engine queries. Some ISPs 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 occurred in a Canadian court case. In June 2017, in *Google Inc.* v. *Equustek Solutions Inc*,[14] 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, French Data Protection Authority (CNIL) declared that search engines implementing France's Right to Be Forgotten law must de-list such links globally and not simply take down such sites within the EU (Reventlo: 2017). On 19 July 2017, France's highest administrative court, the Conseil d'Etat (in English, the Council of State) referred the dispute between 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). A Paris-based NGO, Internet and Jurisdiction, closely monitors such cases noting that the number and impact of such cases increasingly distort cross-border data 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 international jurisdictional conflicts (Mackey *et al.*, 2017; Geist, 2017).

Privacy and data protection: The right to privacy is an internationally accepted human right under the Universal Declaration of Human Rights. But the United

14 Supreme Court of Canada, *Google Inc.* v. *Equustek Solutions Inc.*, 2017 SCC 34 (2017), https://scc-csc.lexum.com/scc-csc/scc-csc/en/16701/1/document.do.

States has adopted an inconsistent approach to privacy as a barrier to trade, as it considers privacy both a human right and consumer right. In 2013, USTR argued that Canada's British Columbia and Nova Scotia provinces have privacy laws that discriminate against US suppliers, because they require that personal data be stored and accessed only in Canada (USTR, 2014). In 2014, the United States also complained about Japan's uneven and Vietnam's unclear approaches to privacy and argued that China's failure to enforce its privacy laws stifled e-commerce (USTR, 2014: 96, 216). Thus, the United Sates simultaneously criticizes foreign governments for failing to develop clear or adequate approaches to enforcing privacy and categorises privacy as a trade barrier. Moreover, the US government has argued that privacy protections bolster trust in the internet and are essential to stimulating the growth of digital technologies. Although the United States has worked with other governments to establish principles on privacy, it has done little to foster bridges among these various privacy principles. 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 (which would therefore be allowed under GATS and/or FTA exceptions).

The EU's approach to data protection also presents some inconsistencies. The 27 EU member states are working to create a digital single market (DSM) where data can flow freely among them and data will be regulated under one set of EU-wide rules. The main characteristic of the EU DSM is its high commitment to protecting personal data within EU. However, as noted above, the EU's approach to privacy will not be included in EU trade agreements as a topic for negotiation. EU Trade Commissioner Cecilia Malmström argued that personal data protection is not protectionist, stating:

> Let's not kid ourselves: some data restrictions out there are purely protectionist. Rules that require data to be localized in a 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)

The first iteration of the EU's commitment to online data protection was the 1998 Directive on Data Protection. It prohibits the transfer of personal data to non-EU countries that do not meet the 'adequacy' standard for privacy protection. To become adequate, the EU requires other countries to create independent government data protection agencies, register databases with those agencies, and, in some instances, obtain prior approval from the European Commission before personal data processing may begin (Institute for Government (UK), 2017). Hence, while the EU does not require other nations adhere to its approach, it is attempting to export its norms.

As new technologies emerged, in the EU, policymakers and the public realized their data protection framework needed updating. In 2016, the EU adopted the

General Data Protection Regulation (GDPR), which replaces the Data Protection Directive. The GDPR takes effect on 25 May 2018 and provides rules on the use of data that can be attributed to a person or persons (EU Council Regulation, 2016/679).[15] In October 2017, the European Commission also proposed a new regulation 'concerning the respect for private life and the protection of personal data in electronic communications' to replace the outdated e-Privacy Directive, while ensuring its consistency with the GDPR (European Commission, 2017b).

However, some see the EU's stringent approach to data protection as a form of censorship by regulating what other netizens can and cannot see (Solon, 2014; Hern, 2014). As noted above, EU citizens have the right to demand delisting of data that breaches privacy. But this right to delist is only available on the internet within the EU.[16] Google, as example, will use geo-location to ensure residents located in each EU country cannot see the search results on *any* version of its platform, even as those outside the country *can* see them (Fleischer, 2016; Pickrell, 2017).

The EU's commitment to data protection has costs and benefits. On the one hand, the EU approach to elevating data protection is attractive to many countries and netizens, but, on the other hand, it is extremely costly to digital firms. Despite these costs and benefits, the EU increasingly encourages its trade partners to accept its approach to data protection. In 2017, a French court required that websites outside of France must block foreign content to enforce the EU's 'right to be forgotten'. In so doing, the EU is imposing its values on other suppliers and consumers of data (Atkinson, 2017). Because the EU is a major market, several countries are adopting EU data protection policies or working towards being deemed 'adequate'. To date, on its website, the European Commission has recognized Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and the United States (limited to the Privacy Shield framework) as providing adequate protection, while Japan and South Korea are in discussions with the EU.[17]

The EU has also introduced a new approach to regulating the use of algorithms, designed to protect the privacy of users and empower them to contest misuse. After 25 May 2018, the GDPR's Article 21 gives anyone the right to opt out of algorithm-tailored advertisements (e.g. what one finds when searching on Google). Article 22 allows EU citizens to contest legal or significant decisions made by algorithms and appeal for human intervention. In contrast, the United States is using its

15 EU Council Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal of the European Communities* L 119/59, May 3, 2016, pp. 1-89, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN.

16 Google prefers the term 'right to be delinked'.

17 European Commission, Adequacy of the protection of personal data in non-EU countries, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

trade agreements to prevent such transparency, although it is unclear whether its NAFTA partners (and other nations) will agree to this language.

Cybertheft: The US government argues that companies as well as government entities are victims of cybertheft. According to the US Defence Science Board (2013), other nations use the internet to scour, penetrate, and steal data 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. Once they have obtained these secrets, these hackers allegedly provided that data to Chinese companies. In 2015, the US China Security and Economic Commission reported that data were stolen from US government agencies, including the United States Postal Service (USPS), universities such as Penn State University, Johns Hopkins University, Carnegie Mellon University, and Massachusetts Institute of Technology, and companies such as United Airlines. All the cyberthefts are attributed to Chinese actors that appear to be aligned with the Chinese government; but this allegation is difficult to prove (USCC, 2015, 192, 198, 199–204). In 2015, China agreed with the United States that neither country's government will conduct cyber-enabled theft of intellectual property, although again cybertheft was not clearly defined (USCC, 2015, 209). Meanwhile, the US government has stressed it does not use surveillance for commercial theft. Nonetheless, in the summer of 2015, WikiLeaks provided evidence that the US government had spied on Japanese companies and policymakers to obtain prior knowledge of positions related to trade negotiations, President Obama called Japanese Prime Minister Abe to apologize. Also, in 2015, Chancellor Angela Merkel's office said it found that the US government had used Germany's top spy agency to watch European corporate targets. However, the US government still insists that it is not stealing corporate property and giving it to US companies. Thus, citizens and government officials in the United States and abroad may find it hard to distinguish between cyber monitoring to prevent crime and terrorism and cyber probing to steal technologies (Aaronson, 2016a).

Regulatory Context: The United States argues that governments which fail to make an appropriate regulatory context for the free flow of data are effectively distorting trade. In 2015, it chided China, South Africa, Thailand, and the United Arab Emirates (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 Trump administration has taken some steps that reduce US credibility as an advocate for the free flow of data across borders. US regulators have rejected the net neutrality principle, whereby individuals should be free to access all content and applications equally, regardless of the source and without ISPs discriminating against specific online services or websites. In 2015, the Federal Communications Commission (FCC) decided that

several internet firms were dominating the market and jeopardizing access and fair pricing. The FCC agreed to regulate broadband and mobile ISPs as a utility to ensure that these providers did not achieve monopoly prices in markets where competition was limited. These rules, they argued, would promote net neutrality (Public Knowledge).[18] However, the new FCC Chair reversed that decision, stating that in so doing the United States was taking a hands-off approach to regulating the internet within its borders. Critics have contended, however, that this new approach allows US ISPs to discriminate among services, service providers, and websites (Borchers, 2017).

EU member states have several policies that could be considered trade-distorting. For example, EU member states 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), while others do not. (Blaney, 2015).

Cybersecurity regulations demonstrate the importance of finding common ground on the relationship between domestic regulation and cross-border data flows. Given the rise in malware, hacking, and disinformation, governments may at times seek to restrict cross-border flows to maintain political stability, trust, and personal security (Zetter, 2016; Poulsen, 2017; Valeriano, 2016; Hulcoop *et al*., 2017; Scott, 2017; Mozur and Scott, 2016). In June 2017, WTO members debated if cybersecurity strategies could distort trade. Some members were concerned that cybersecurity regulations would negatively impact trade in information technology products, potentially discriminating against foreign companies and possibly leading to unnecessary disclosure of commercially confidential and technical data. Others argued that cybersecurity rules are needed to address national security issues and ensure consumer privacy, and that the measures in question are non-discriminatory (WTO, 2017a). In looking at the debate between China's cybersecurity regulations and US insistence that these regulations are protectionist, Director of Cato Institute's Herbert A. Stiefel Center for Trade Policy Studies Dan Ikenson concluded that the objectives of both governments have less to do with cybersecurity than with protectionism (Ikenson, 2017). However, others may not believe it is so easy to ascertain protectionist intent.

7. China's censorship at home and abroad: new tactics and market access consequences

China's approach to regulating censorship both within and beyond its borders provides a good example of the difficulty in determining if a measure undermines

18 Public Knowledge, Net Neutrality, www.publicknowledge.org/issues/net-neutrality. According to Public Knowledge, net neutrality is the principle that individuals should be free to access all content and applications equally, regardless of the source and without internet service providers discriminating against specific online services or websites.

market access (Krebs, 2016; Schneier, 2016). If censorship is a barrier to cross-border data flows, China has learned how to censor the internet beyond its borders. As noted above, China is one of the world's largest and fastest-growing internet markets. In 2016, only some 50% of its citizens were online, so the internet in China has plenty of room for growth (UNESCO, 2016). As a result, many firms believe they must have an online presence in China. However, the Chinese internet is also likely the world's most restrictive and monitored platform. 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' (US–China Economic and Security Review Commission, 2008a: 3). The government blocks sites by internet protocol (IP) address, and blocks and filters uniform research locators (URLs) and search engine results. The country supposedly employs two million individuals to censor the internet. In 2017, Chinese officials argued that the nation must restrict the web to maintain social stability and security amid threats like terrorism (Xu and Albert, 2017). However, China has different censorship systems for foreign and domestic sites (Erixon *et al.*, 2009). Most Chinese netizens cannot access websites such as Facebook and Twitter, foreign media such as the *New York Times*, and many Google services. In 2017, the American Chamber of Commerce in China reported that 79% of US companies in China have experienced blocked access to web tools and services, which raise their business costs (Associated Press, 2017). In addition, Chinese censorship rules lead firms to self-censor and can hobble user privacy and security (USCC, 2015: 211).

Unsurprisingly, USTR (2015: 70–72, 77–79) describes China's internet regulatory regime as restrictive and opaque. Legal scholar Henry Gao describes it as arbitrary and often unreasonable (Gao, 2011: 371). Greatfire.org, a website monitoring Chinese censorship, found China censored 878 of 1233 Wikipedia pages and 769 of 947 Google pages.[19] Under WTO rules, China is supposed to provide a system of judicial or administrative review of such blockage, but it has not yet done so (Schruers, 2015; US–China Economic and Security Review Commission, 2008b).

China's approach to censorship is evolving. The government does not only rely on paid censors but also on the acquiescence of companies providing internet services within China. These companies must follow local law or withdraw from the market (e.g. 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 same month, Apple removed several apps from its Apple store in China that allow

19 Online Censorship in China, GreatFire.org.

individuals to use VPNs (Mozur, 2017). Furthermore, on 3 August 2017, all internet data centres and cloud companies located in China were ordered to participate in a three-hour drill to hone their 'emergency response' skills. They were essentially ordered 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.

Since 2008, researchers have found evidence that the Chinese government has exported censorship beyond its borders. In a 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 United States, United Kingdom, Canada, and elsewhere since 2008. He noted that these methods deny access to information by disabling the sources of data (rather than blocking requests for data as filtering systems do). Researchers find it hard to pinpoint the source of such attacks, so governments can deny ever using such methods (US–China Economic and Security Review Commission, 2008a, 4). Moreover, with DDoS, China can censor abroad without asserting the heavy hand of government.

In 2015, researchers at The Citizen Lab and several other organizations asserted that hackers in China essentially took down two US-based websites: GitHub and GreatFire (Marczak *et al.*, 2015).[20] 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 the Chinese government 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' cannot only shut down the connection, but apparently the hackers hijacked traffic to these web addresses and replaced benign unencrypted web content with malicious content (US China Economic and Security Review Commission, 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 Citizen lab analysts could 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.

However, China is not the only country to use a DDoS attack to disable a website. Both the United States and the United Kingdom have allegedly tampered with internet traffic to launch attacks (Marczak *et al.*, 2015). However, neither country did so to censor information. The Citizen Lab's researchers concluded

20 The Citizen Lab report was corroborated by Graham (2015) and Hjelmvik (2015).

that deployment of the 'Great Cannon' was a significant escalation in state-level data control because censorship was enforced by 'weaponizing users', rather than by direct government action. Moreover, China's alleged tactics create a dangerous precedent, contrary to international norms, and puzzling those attempting to ascertain why China chose to act in this way (Marczak *et al.*, 2015). In 2015, the *South China Morning Post* (2015) reported that the Chinese government had been planning the attack for over a year.

While several research organizations pinned the GitHub attack on China, we do not know who is behind the rise in DDoS attacks in the United States. Moreover, while the attacks may have come from Chinese entities that may be affiliated with the Chinese government, it is impossible to prove that the Chinese government ordered these attacks. Although several private firms and organizations have attributed these attacks to actors in China, they can't *prove* that China is behind these actions. Nor can we assert that China is the only country behind the increase in these DDoS attacks (Schneier, 2016; US–China Economic and Security Review Commission, 2016: Chapter 4; Kawanmoto, 2017).[21]

According to William Marczak, a senior research fellow at The Citizen Lab, China has not used this tactic since 2015.[22] Yet the allegations of DDoS by Chinese-affiliated entities in the United States and United Kingdom have important implications for trade and trust in the internet. These DDoS attacks can reduce market access conditions in the attacked company's home country, since an attacked company (e.g. Twitter) cannot serve its customers if its site is unavailable. These attacks reduce market access and raise costs for firms who must hire researchers to ascertain who is responsible for these attacks while simultaneously spending money to get their sites back online. DDoS attacks also reduce internet stability and diminish the predictability of data flows (Google, 2010; Gao, 2011; US–China Economic and Security Review Commission, 2008b). To put it differently, these tactics essentially export Chinese censorship to the United States and other countries and undermine the functioning of the internet. Yet the WTO is just beginning to examine how the Great Firewall and other Chinese policies may affect cross-border data flows (WTO, 2018).

8. The costs of digital protectionism: direct costs and unanticipated spillovers

Digital protectionism may be self-defeating. As noted above, while there is no consensus regarding how to define, measure, let alone remedy, digital

21 The cybersecurity firm, Kaspersky, does an annual assessment. In 2017, it found that some 86 countries faced major DDoS attacks. The top 10 countries hit with attacks included the United States, China, South Korea, Hong Kong, the United Kingdom, Russia, Italy, France, Canada, and the Netherlands. The United States, China, and South Korea also have the most servers. For a map of digital attacks, see http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=17613&view=map.

22 Skype interview by author with William Marczak, 5 August 2017.

protectionism, a growing number of researchers find costly spillover effects (USITC, 2013, 2014; OECD, 2017). ECIPE estimated that data localization regulations cost EU citizens about $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 the economic impact of internet censorship, filtering, and blocking was $2.4 billion, which was noted as an understatement of the actual economic damage of lost tax revenues, the negative impact of worker productivity, among other costs (West, 2016). The OECD's Sarah Box argues that such reductions on 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; Cory, 2017). Digital protectionism may not only increase costs to firms, but legal disputes could escalate while individuals and firms could have fewer incentives to innovate (Hill and Noyes, 2018; de la Chapelle and Fehlinger, 2016). 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. 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 an 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 4 March 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 the Great Firewall may make it harder for China to become 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 favoured 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 (Hill, 2014: 32; Daigle, 2015; Drake *et al*., 2016). Finally, digital protectionism 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).

9. Conclusion: the need for common ground

The idea of using trade agreements to regulate digital protectionism may well be the idea whose time has arrived. Digital protectionism 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 EU efforts to establish the Digital Single Market as an EU-wide approach to protectionism. On 13 September 2016 in a *New York Times* article, Mark Scott 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.'. In contrast, Nicky Stewart, a former internet strategist for the UK Cabinet asserted 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 for why they may seek to limit cross-border data flows. For example, many of them 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 it may not be their original intent. Policymakers also want to encourage the rule of law online and prevent unlawful behaviour, such as the dissemination of hate speech or child pornography, fraud, identity theft, cyberattacks, and money laundering. These policies, too, may be necessary to achieve important domestic objectives, yet they may discriminate against foreign firms (Aaronson, 2016b). Finally, what may appear protectionist to one country could be seen as legitimate and necessary regulation in another country (*Financial Times*, 2018).

Digital protectionism also differs from traditional protectionism because data are both a good and service and, at times, a public good. But some policymakers who seek protectionism are developing new tactics to protect such data 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 their implications for market access and rules-based trade.

Countries need to find common ground regarding which practices truly distort digital trade, what should be banned, and what should be limited and clarified under the exceptions. Hence, in developing norms and rules, decision-makers must first define how and when governments can control data and limit their flows. They must ensure that these rules are internationally accepted and transparent to ensure predictability and accountability. With shared understanding, the

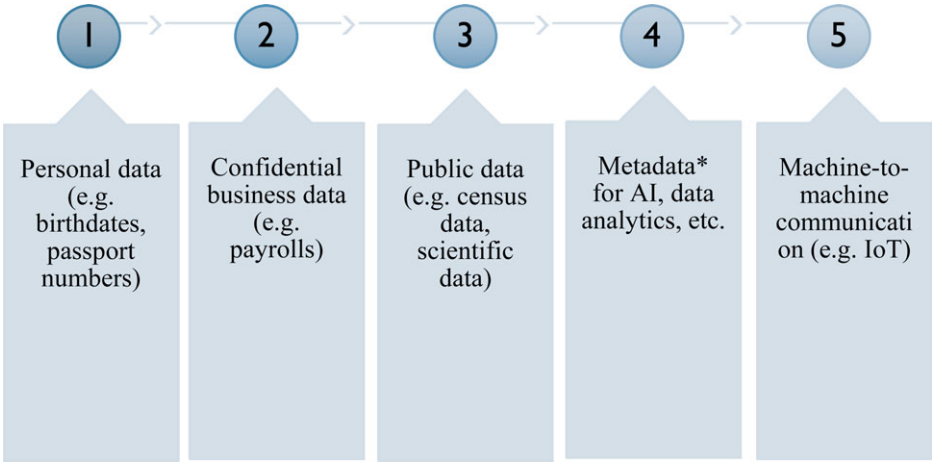
internet would be less likely to fragment, more people would have greater access to information, and individuals could create and share more data (Tietje, 2011).

To address these issues, policymakers must work multilaterally. Specifically, policymakers should ask the WTO Secretariat to:

1. Examine whether domestic policies that restrict data (short of exceptions for national security, privacy, and public morals) constitute barriers to cross-border data flows that could be challenged in a trade dispute.
2. Convene a study group to examine the trade implications of malware and DDoS attacks as a means of distorting trade. *These tactics should be banned, although the WTO may not be the best forum to discuss these problems.*
3. Monitor each other's digital trade practices during the WTO trade policy review process.
4. Policymakers should rethink how we regulate data internationally in trade agreements. A forward-looking approach would distinguish among the five types of data, who controls the data, and where the data are controlled (see Figure 1) (Aaronson, 2017b). Control of data is important to any taxonomy or set of rules, because it influences the benefits that firms and consumers can gain from trade and it can build trust online (Aaronson and LeBlond, 2018).

A new approach built on data type might allow policymakers to better distinguish between regulations designed to control the use of certain types of data and trade-distorting rules. Moreover, it could empower users in the developing world. Netizens in developing countries may be suppliers of personal data, but

Figure 1. Types of data traded across borders



Note: Metadata is aggregated and supposedly anonymized personal data.
Source: Author's original analysis.

their firms probably do not control or process data. Policymakers from these states can decide to shape their own markets by developing rules that require companies to pay their citizens for their personal data. Developing countries with large populations are likely to have the most leverage to adopt regulations that require firms to pay rents for their citizens' data. In so doing, they may be able to upend the market power of huge internet firms. Hence, it could create new demandeurs for trade as a tool to regulate data flows.

References

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

——— (2016a), 'The Digital Trade Imbalance and Its Implications for Internet Governance', Centre for International Governance Innovation, February, www.cigionline.org/sites/default/files/gcig_no25_-web_0.pdf.

——— (2016b), 'Digital Protectionism? Or Label the US Government Uses to Criticize Policy It Doesn't Like?', Council on Foreign Relations, March 3, www.cfr.org/blog-post/digital-protectionism-or-label-us-government-uses-criticize-policy-it-doesnt.

——— (2017a), 'What Might Have Been and Could Still Be: The Trans-Pacific Partnership's Potential to Encourage an Open Internet and Digital Rights', *Journal of Cyber Policy*, **2**(2): 232–254.

——— (2017b), 'Information Please: A Comprehensive Approach to Digital Trade Provisions in NAFTA 2.0', Centre for International Governance Innovation, 13 November, www.cigionline.org/sites/default/files/documents/Paper%20no.154web.pdf.

——— (2018), 'Artificial Intelligence Is Trade Policy's New Frontier', Centre for International Governance Innovation, 11 January, www.cigionline.org/articles/artificial-intelligence-trade-policys-new-frontier.

Aaronson, S. A. and M. D. Townes (2012), 'Can Trade Policy Set Information Free?', Institute for International Economic Policy, www2.gwu.edu/~iiep/signatureinitiatives/governance/taig/CanTradePolicySetInformationFreeFINAL.pdf.

Aaronson, S. A. and P. LeBlond (2018), 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO', Journal of International Economic Law, forthcoming.

Ariu, A. (2012), *Services* v. *Goods Trade: Are They the Same?* Brussels: National Bank of Belgium, www.nbb.be/doc/ts/publications/wp/wp237en.pdf.

Associated Press (2017), 'China Clamping Down on Use of VPNs to Evade Great Firewall', *Business Insider*, 20 July, www.businessinsider.com/ap-china-clamping-down-on-use-of-vpns-to-evade-great-firewall-2017-7.

Atkinson, R. D. (2017), 'Can Nations Actually Collaborate for Growth in the Digital Economy?', *Connect-World*, https://drive.google.com/file/d/1LYFZ2agJWaqwnhCoRPaJ02G8nz3GJfOm/view.

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

Barefoot, K., D. Curtis, W. Joliff, J. R. Nicholson, and R. Omohundro (2018), 'Defining and Measuring the Digital Economy', US Department of Commerce Bureau of Economic Analysis, Washington, DC, 15 March, www.bea.gov/digital-economy/_pdf/defining-and-measuring-the-digital-economy.pdf.

Bauer, M., H. Lee-Makiyama, E. van der Marel, and B. Verschelde (2014), 'The Costs of Data Localization: Friendly Fire on Economic Recovery', *European Centre for International Political Economy (ECIPE)*, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

Bauer, M., M. F. Ferracane, and E. van der Marel (2016), 'Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization', *Centre for International Governance Innovation*, www.cigionline.org/sites/default/files/gcig_no30web_2.pdf.

Beach, D. and R. B. Pedersen (2013), *Process-Tracing Methods: Foundations and Guidelines*, Ann Arbor, MI: University of Michigan Press.
Beaumont, C. (2010), 'Foursquare Blocked in China', *The Telegraph*, 4 June, www.telegraph.co.uk/technology/social-media/7802992/Foursquare-blocked-in-China.html.
Berry, R. and M. Reisman (2012), *Policy Challenges of Cross Border Cloud Computing*, US International Trade Commission, www.usitc.gov/research_and_analysis/documents/Final_Cloud_Computing_Seminar_61912_0.pdf.
Biggs, J. (2007), 'China Declares War on Western Search Sites', *TechCrunch*, 18 October, https://techcrunch.com/2007/10/18/cyberwar-china-declares-war-on-western-search-sites/.
Bildt, C. (2012), 'A Victory for the Internet', *New York Times*, 5 July, www.nytimes.com/2012/07/06/opinion/carl-bildt-a-victory-for-the-Internet.html.
Blaney, M. (2015), 'MEPS Make Recommendations on Digital Single Market Strategy', 23 November, www.screendaily.com/news/meps-make-recommendations-on-dsm-strategy/5097228.article.
Borchers, C. (2017), 'Trump's FCC Chairman Is Pitching Internet Deregulation as a Return to Bill Clinton's Policy', *Washington Post*, 27 November, www.washingtonpost.com/news/thefix/wp/2017/11/27/trumps-fcc-chairman-is-pitching-internet-deregulation-as-a-return-to-bill-clintons-policy/?utm_term=.9983da130554.
Box, S. (2016), 'Internet Openness and Fragmentation: Toward Measuring the Economic Effects', *Centre for International Governance Innovation*, May.
Burgman, Jr., P. R. (2016), 'Securing Cyberspace: China Leading the Way in Cyber Sovereignty', *The Diplomat*, 18 May, http://thediplomat.com/2016/05/securing-cyberspace-china-leading-the-way-in-cyber-sovereignty/.
Burri, M. (2013), *Should There be New Multilateral Rules for Digital Trade? Think Piece for the E15 Expert Group on Trade and Innovation*, Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum, December, http://e15initiative.org/wp-content/uploads/2015/09/E15-Innovation-Burri-FINAL.pdf.
Calinoff, J. 'Beijing's Foreign Internet Purge', *Foreign Policy*, 15 January 2010, http://foreignpolicy.com/2010/01/15/beijings-foreign-internet-purge/.
Chan, C., A. Dao, J. Hou, T. Jin, and C. Tuong (2011), 'US Censorship', *Free Speech vs. Maintaining Social Cohesion*, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/us_policy.html.
Chander, A. and Uyen P. Le (2014), 'Breaking the Web: Data Localization vs. the Global Internet', *Emory Law Journal*, https://ssrn.com/abstract=2407858orhttp://dx.doi.org/10.2139/ssrn.2407858.
—— (2015), 'Data Nationalism', *Emory Law Journal*, **64**(3), https://ssrn.com/abstract=2577947.
Chu, Cho-Wen (2017), 'Censorship or Protectionism? Reassessing China's Regulation of Internet Industry', *International Journal of Social Sciences and Humanity*, **7**(1).
Ciuriak, D. and M. Ptashkina (2018), *The Digital Transformation and the Transformation of International Trade*, Geneva: International Centre for Trade and Sustainable Development and Inter-American Development Bank, http://e15initiative.org/wp-content/uploads/2015/09/RTA-Exchange-Digital-Trade-Ciuriak-and-Ptashkina-Final.pdf.
Clark, J., R. Faris, R. Morrison-Westphal, H. Noman, C. Tilton, and J. Zittrain (2017), 'The Shifting Landscape of Global Internet Censorship', Berkman Klein Center for Internet & Society Research Publication, June, http://nrs.harvard.edu/urn-3:HUL.InstRepos:33084425.
Computer and Communications Industry Association (2008), Internet Censorship and Online Freedom.
Cory, N. (2017), 'Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? Information Technology and Innovation Foundation', May, https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.
—— (2018), 'The Global Rise of "Data Localism"'. *BRINK*, 31 January, www.brinknews.com/the-global-rise-of-data-localism/.
Daigle, L. (2015), 'On the Nature of the Internet', Centre for International Governance Innovation.
Davidow, B. (2012), 'The Tragedy of the Internet Commons', *The Atlantic*, 18 May, www.theatlantic.com/technology/archive/2012/05/the-tragedy-of-the-internet-commons/257290/.

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

de la Chapelle, B. and P. Fehlinger (2016), 'Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation', Centre for International Governance Innovation, 1 April.

Drake, W., V. Cerf, and W. Kleinwächter (2016), 'Internet Fragmentation: An Overview', World Economic Forum, www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

ECIPE (2018), DTE Report, http://ecipe.org/dte/dte-report/.

Elms, D. (2017), 'Moving Ahead with the TPP 11', *Asian Trade Centre*, 11 January, www.asiantradecentre.org/talkingtrade//moving-ahead-with-the-tpp11.

Epstein, R. (2016), 'The New Censorship', *US News*, 22 June, www.usnews.com/opinion/articles/2016-06-22/google-is-the-worlds-biggest-censor-and-its-power-must-be-regulated.

Erixon, F. and H. Lee-Makiyama (2010), 'Chinese Censorship Equals Protectionism', *The Wall Street Journal*, 6 January, www.wsj.com/articles/SB10001424052748704842604574641620942668590.

Erixon, F., B. Hindley, and H. Lee-Makiyama (2009), 'Protectionism Online: Internet Censorship and International Trade Law', European Centre for Political Economy (ECIPE), http://ecipe.org/app/uploads/2014/12/protectionism-online-internet-censorship-and-international-trade-law.pdf.

European Commission (2015a), *Trade and Investment Barriers Report 2015*, COM(2015) 127, http://trade.ec.europa.eu/doclib/docs/2015/march/tradoc_153259.pdf.

——— (2016), *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, http://trade.ec.europa.eu/doclib/docs/2016/june/tradoc_154665.pdf.

——— (2017a), *Report from the Commission to the European Parliament and the Council on Trade and Investment Barriers 1 January–31 December 2016*, http://trade.ec.europa.eu/doclib/docs/2017/june/tradoc_155642.pdf.

——— (2017b), *Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, COM 2017/0003, https://goo.gl/Saevs4.

——— (2017c), 'EU–Mexico Free Trade Agreement: EU Textual Proposal on Digital Trade', April, https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

——— (2018a), 'Horizontal Provisions for Cross-border Data Flows and for Personal Data Protection (in EU trade and Investment Agreements)', www.politico.eu/wp-content/uploads/2018/02/Data-flow-provisions-POLITICO.pdf.

——— (2018b), EU-DG Trade, Modernization of EU GA, Digital Trade, http://trade.ec.europa.eu/doclib/docs/2018/april/tradoc_156811.pdf.

European Commission 'Adequacy of the Protection of Personal Data in non-EU Countries', https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

Fefer, R., S. I. Akhtar, and W. M. Morrison (2017), 'Digital Trade and US Trade Policy', CRS Report No. R44565), Congressional Research Service, Washington, DC.

Federal Ministry for Economic Affairs and Energy (2017), *G20 Digital Economy Ministerial Declaration*, www.g20.utoronto.ca/2017/g20-digital-economy-ministerial-declaration-english-version.pdf.

Financial Times. 'Digital Protectionism and National Security: Where Are the Limits of Government Interference in the Tech Industry? 26 March 2018, www.ft.com/content/112e233c-2912-11e8-b27e-cc62a39d57a0.

Fleischer, P. (2016), 'Adapting Our Approach to the European Right to Be Forgotten', Google, 4 March, www.blog.google/topics/google-europe/adapting-our-approach-to-european-rig/.

Fortnam, B. (2017a), 'Canada Expected to Stand Firm on Maintaining "Cultural Carveout" in NAFTA', Inside US Trade, 3 August, https://insidetrade.com/daily-news/canada-expected-stand-firm-maintaining-cultural-carveout-nafta.

——— (2017b), 'EU Punts on Data Flow Language in Japan Deal, Leaving Position Unresolved', Inside US Trade, 6 July, https://insidetrade.com/inside-us-trade/eu-punts-data-flow-language-japan-deal-leaving-position-unresolved.

——— (2017c), 'Japan Urges EU to Develop Data Flow Provisions Despite Political Agreement on FTA', Inside US Trade, 7 July, https://insidetrade.com/daily-news/japan-urges-eu-develop-data-flow-provisions-despite-political-agreement-fta.

Froman, M. United States Trade Representative (2017), *Trade,* Growth, and Jobs: US Trade Policy in the Obama Administration, Washington, DC: Executive Office of the President.

Gao, H. S. (2011), 'Google's China Problem: A Case Study on Trade, Technology and Human Rights under the GATS', *Asian Journal of WTO & International Health Law and Policy*, **6**: 347–385.

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

Goldfarb, D. (2011), 'Canada's Trade in a Digital World', The Conference Board of Canada, April, www.conferenceboard.ca/reports/briefings/tradingdigitally/default.aspx.

Goldman, E. (2011), 'The OPEN Act: Significantly Flawed, but More Salvageable than SOPA/PROTECT-IP', Ars Technica, 12 December, https://arstechnica.com/tech-policy/2011/12/the-open-act-significantly-flawed-but-more-salvageable-than-sopaprotect-ip/.

Goldsmith, J. 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.

Graham, R. (2015), 'Pin-Pointing China's Attack against GitHub', Errata Security, 1 April, http://blog.erratasec.com/2015/04/pin-pointing-chinas-attack-against.html?m=1.

Haas, B. (2017), 'Chinese Official Calls for Easing of Internet Censorship', The Guardian, 3 March, www.theguardian.com/world/2017/mar/04/chinese-official-slams-internet-censorship.

Hamilton, D. S. and J. P. Quinlan (2016), 'The Transatlantic Economy 2016: Annual Survey of Jobs, Trade and Investment between the United States and Europe', Center for Transatlantic Relations, Washington, DC, www.transatlanticbusiness.org/wp-content/uploads/2014/05/160301-TAE-FULL-BOOK.pdf.

Hill, J. F. (2014), 'The Growth of Data Localization Post Snowden: Analysis and Recommendations for US Policymakers and Industry Leaders', Lawfare Research Paper Series, 2(3), https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf.

Hill, J. F. and M. Noyes (2018), 'Rethinking Data Geography and Jurisdiction: Towards a Common Framework for Harmonizing Global Data Flow Controls', New America, 22 February, https://goo.gl/BHbg38.

Hjelmvik, E. (2015), 'China's Man-on-the-Side Attack on GitHub', Netresec.com, 31 March, www.netresec.com/?page=Blog&month=2015-03&post=China%27s-Man-on-the-Side-Attack-on-GitHub.

Hern, A. (2014), 'Wikipedia Swears to Fight "Censorship" of "Right to Be Forgotten" Ruling', The Guardian, August, wwwkipedia-censorship-right-to-be-forgotten-ruling.

Hindley, B. (1988), 'Service Sector Protection: Considerations for Developing Countries', *The World Bank Economic Review*, **3**(2): 205–224, http://documents.worldbank.org/curated/en/504431468739778099/pdf/multi-page.pdf.

Hoagland, I. and J. Caporal (2017), 'Lawmakers, Analysts Underwhelmed by USTR's NAFTA Digital Trade Objectives', *Inside US Trade*, 20 July, https://insidetrade.com/inside-us-trade/lawmakers-analysts-underwhelmed-ustrs-nafta-digital-trade-objectives.

Hulcoop, A., J. Scott-Railton, P. Tanchak, M. Brooks, and R. Deibert (2017), 'Tainted Leaks: Disinformation and Phishing with a Russian Nexus', *The Citizen Lab*, 25 May, https://citizenlab.org/2017/05/tainted-leaks-disinformation-phish/.

Ikenson, D. J. (2017), 'Cybersecurity or Protectionism? Defusing the Most Volatile Issue in the US–China Relationship', CATO Institute, 13 July, www.cato.org/publications/policy-analysis/cybersecurity-or-protectionism-defusing-most-volatile-issue-us-china.

Institute for Government (UK), (2017), Data Adequacy, 24 August, www.instituteforgovernment.org.uk/explainers/data-adequacy.

Internet and Jurisdiction (2017), 'Cross-Border Content Takedowns Across Jurisdiction', www.internet-jurisdiction.net/uploads/pdfs/Papers/Content-Jurisdiction-Program-Paper.pdf.

Irwin, D. (1996), *Against the Tide: An Intellectual history of Free Trade*, Princeton, NJ: Princeton University Press.

Jiang, S. (2017), 'China Holds Drill to Shut Down "Harmful" Websites', *Reuters*, 3 August, www.reuters.com/article/us-china-internet-idUSKBN1AJ1XL.

Kawanmoto, D. (2017), 'Chinese Telecom DDoS Attack Breaks Record', *Dark Reading*, 2 August, www.darkreading.com/attacks-breaches/chinese-telecom-ddos-attack-breaks-record-/d/d- id/1329518?

Khan, A. W. (2009), 'Universal Access to Knowledge as a Global Public Good', Global Policy Forum, June, www.globalpolicy.org/social-and-economic-policy/global-public-goods-1-101/50437-universal-access-to-knowledge-as-a-global-public-good.html.

Kravets, D. (2017), 'Facebook, Google, Twitter Tell Congress Their Platforms Spread Russian-Backed Propaganda', *Arstechnica.com*, 31 October, https://arstechnica.com/tech- policy/2017/10/facebook-google-and-twitter-tell-congress-they-spread-russian-propaganda/.

Krebs, B. (2016), 'The Democratization of Censorship', Krebs on Security, 16 September, krebsonsecurity.com/2016/09/the-democratization-of-censorship/.

Lee-Makiyama, H. (2011), 'Future-Proofing World Trade in Technology: Turning the WTO IT Agreement (ITA) into the International Digital Economy Agreement (IDEA)', *Aussenwirtschaft*, **3**.

Lopez Gonzalez, J., J. Messent, M. Rentzhog, D. Flaig, M.-A. Jouanjean, and P. Walkenhorst (2016), 'Localising Data in a Globalised World', Organisation for Economic Co-operation and Development, http://unctad.org/meetings/es/Presentation/dtl_eweek2016_JLopez-Gonzalez.pdf.

Mackey, A., C. McSherry, and V. Ranieri (2017), 'Top Canadian Court Permits Worldwide Internet Censorship', Electronic Frontier Foundation, 28 June, www.eff.org/deeplinks/2017/06/top-canadian-court-permits-worldwide-internet-censorship.

Malmström, C. (2016), 'Trade in a Digital World', Speech, Conference on Digital Trade, European Parliament. European Commission, Brussels, Belgium, 17 November 2016, http://trade.ec.europa.eu/doclib/docs/2016/november/tradoc_155094.pdf.

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

Manyika, J., S. Lund, J. Bughin, J. Woetzel, K. Stamenov, and D. Dhingra (2016), 'Digital Globalization: The New Era of Global Flows', McKinsey Global Institute, www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digitalglobalization-the-new-era-of-global-flows.

Marczak, B., N. Weaver, J. Dalek, R. Ensafi, D. Fifield, S. McKune, A. Rey, J. Scott-Railton, R. Deibert, and V. Paxxson (2015), 'An Analysis of China's "Great Cannon"', Foci 15 Conference, www.usenix.org/system/files/conference/foci15/foci15- paper-marczak.pdf.

Maskus, K. 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 Group, http://elibrary.worldbank.org/doi/pdf/10.1596/1813-9450-2380.

McAuley, J. (2018), 'France Weighs a Law to Rein in "Fake News", Raising Fears for Freedom of Speech', *The Washington Post*, 10 January, www.washingtonpost.com/world/europe/france-weighs-a-law-to-rein-in-fake-news-raising-fears-for-freedom-of-speech/2018/01/10/78256962-f558-11e7-9af7a50bc3300042_story.html?utm_term=.40f0ac086662.

McGee, R. W. (1996), 'The Philosophy of Trade Protectionism, Its Costs and Its Implications', *SSRN Policy Analysis*,10 (July), http://dx.doi.org/10.2139/ssrn.91369.

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

McLaughlin, A. (2007), 'Censorship as Trade Barrier', *Google Public Policy Blog*, 22 June, https://public-policy.googleblog.com/2007/06/censorship-as-trade-barrier.html.

Mozur, P. and M. Scott (2016), 'Fake News in US Election? Elsewhere, That's Nothing New', *New York Times*, 16 November, https://goo.gl/ZHn3q7.

Mozur, P. (2017), 'Apple Removes Apps from China Store that Help Internet Users Evade Censorship', *New York Times*, 30 July, www.nytimes.com/2017/07/30/technology/china-apple-censorhip.html?action=click&contentCollection=Business%20Day&module=RelatedCoverage&region=Marginalia&pgtype=article.

Myers, S. L. and S.-L. Wee (2017), 'As US Confronts Internet's Disruptions, China Feels Vindicated', *New York Times*, 16 October 16, www.nytimes.com/2017/10/16/world/asia/china-internet-cyber-control.html.

National Foreign Trade Council (NFTC) (2010), 'Promoting Cross-Border Data Flows: Priorities for the Business Community', www.nftc.org/default/Innovation/PromotingCrossBorderDataFlowsNFTC.pdf.

Nicholson, J. R. and R. Noonan (2014), *Digital Economy and Cross-Border Trade: The Value of Digitally Deliverable Services*, Washington, DC: US Department of Commerce, http://esa.doc.gov/sites/default/files/digitaleconomyandcross-bordertrade.pdf.

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

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

Organisation for Economic Co-operation and Development (OECD) (2011), 'The Economic Impact of Shutting Down Internet and Mobile Phone Services in Egypt', 4 February, www.oecd.org/countries/egypt/theeconomicimpactofshuttingdownInternetandmobilephoneservicesinegypt.htm.

——— (2015), 'Emerging Policy Issues: Localisation Barriers to Trade', TAD/TC/WP(2014)17/FINAL, 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* 257, http://www.oecd-ilibrary.org/docserver/download/5jlwqf2r97g5-en.pdf?expires=1522148375&id=id&accname=guest&checksum=8CEF222DA9DD2CE7019A22B17-B95BD56.

——— (2017), *Measuring Digital Trade: Towards a Conceptual Framework*, OECD/CSSP/WPTGS(2017)3, https://goo.gl/VwRv5L.

Organisation for Economic Co-operation and Development (OECD) and International Monetary Fund (IMF) (2017), *Measuring Digital Trade: Results of OECD/IMF Stocktaking Survey*, BOPCLOm-17/07, Paris, France: International Monetary Fund, www.imf.org/external/pubs/ft/bop/2017/pdf/17-07.pdf.

Owen, T. (2018), 'Ungoverned Space: How Surveillance Capitalism and AI Undermine Democracy', Centre for International Governance Innovation, March 20, www.cigionline.org/articles/ungoverned-space.

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

——— (2016), 'Hackers Used New Weapons to Disrupt Major Websites Across US', *New York Times*, 21 October, www.nytimes.com/2016/10/22/business/internet-problems-attack.html.

Pickrell, E. (2017), 'Renegotiated NAFTA Might Help Bridge Mexico–US Privacy Issues', *Bloomberg Law*, 4 May, www.bna.com/renegotiated-nafta-help-n57982087521/.

Poulsen, K. (2017), 'Russia Turns WikilLeaks CIA Dump Into Disinformation', *Daily Beast*, 8 March, www.thedailybeast.com/articles/2017/03/08/who-s-behind-the-massive-cia-leak.

Reventlow, N. J. (2017), 'The French Court Case that Threatens to Bring the "Right to be Forgotten"', *NetPolitics*, 19 April, www.cfr.org/blog/french-court-case-threatens-bring-right-be-forgotten-everywherere.

Riley, D. (2007), 'Baidu Hijacking Google Traffic In China', *TechCrunch*, 18 October, https://techcrunch.com/2007/10/18/baidu-hijacking-google-traffic-in-china/.

Rugaber, C. S. (2007), 'Google Asks Gov't to Fight Censorship', *USA Today*, 22 June, https://usatoday30.usatoday.com/tech/products/2007-06-22-2859711256_x.htm.

Schaake, M. (2015), 'MEPs Statement on Digital Protectionism', 22 September, www.marietjeschaake.eu/wp-content/uploads/2015/09/2015-09-22-MEPs-Statement-on-Digital-Protectionism.pdf.

——— (2017), 'Working Document, Towards a Digital Trade Strategy', 20 June, https://marietjeschaake.eu/en/towards-a-digital-trade-strategy.

Schneier, B. (2016), 'Someone Is Learning How to Take Down the Internet', The Lawfare Institute, 13 September, www.lawfareblog.com/someone-learning-how-take-down-internet.

Schia, N. N. and L. Gjesvik (2017), 'China's Cyber Sovereignty', Norwegian Institute of International Affairs, www.jstor.org/stable/resrep07952?seq=1#page_scan_tab_contents.

Schruers, M. (2015), *Commercial Espionage and Barriers to Digital Trade in China: Testimony before the US–China Economic and Security Review Commission*, 114th Cong. 15 June 2015, www.ccianet.org/wp-content/uploads/2015/06/Barriers-to-Digital-Trade-in-China-Testimony-6.15.15.pdf.

Scott, M. (2017), 'Facebook's Role in European Elections Under Scrutiny', *New York Times*, 7 June, https://goo.gl/XTVTTr.

Sen, N. (2017), 'Trade in the Digital Economy: Understanding the role of WTO in international data flows', Paper presented at the WTO MC11 Think Conference, Buenos Aires, 13 December 2017.

Solon, O. (2014), 'EU "Right to be Forgotten" Ruling Paves Way For Censorship', *Wired*, 13 May 13, www.wired.co.uk/article/right-to-be-forgotten-blog.

South China Morning Post (2015), 'China's "Great Cannon" Programme Has Been in Development for about a Year, Sources Say', *South China Morning Post*, 12 April, www.scmp.com/news/china/article/1764378/chinas-great-cannon-programme-has-been-development-about-year-sources-say.

Statista (2017), 'Market Capitalization of the Largest Internet Companies Worldwide as of May 2017 (in billion US dollars)', www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/.

Stewart, N. (2017), 'We Need a Grown-Up Debate on Data Localisation Rules without Self-Interest on Show', *Diginomica*, 8 May, 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', www.kommers.se/Documents/dokumentarkiv/publikationer/2016/Protectionism%20in%20the%2021st%20Century_webb.pdf.

Tietje, C. (2011), *Global Information Law – Some Systemic Thoughts*, Halle and Wittenberg, Saxony-Anhalt, Germany: Martin Luther University Halle-Wittenberg, http://telc.jura.uni-halle.de/sites/default/files/BeitraegeTWR/Heft%20107.pdf.

Toobin, J. (2014), 'The Solace of Oblivion – In Europe, the Right to be Forgotten Trumps the Internet', Annals of Law, *The New Yorker*, 29 September 29, www.newyorker.com/magazine/2014/09/29/solace-oblivion.

Tufekci, Z. (2018), 'Facebook's Surveillance Machine', *New York Times*, 18 March, www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html.

Turton, W. (2016), 'This Is Why Half the Internet Shut Down Today', *Gizmodo*, 21 October, 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', TD/B/C.II/EM.5/2, 14 January,htt p://unctad.org/meetings/en/SessionalDocuments/ciiem5d2_en.pdf.

UNESCO (2016), 'China, India Now World's Largest Internet Markets', 15 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) (2015), *Commercial Cyber Espionage and Barriers to Digital Trade*.
—— (2008a), 'Hearing: Access to Information and Media Control in the People's Republic of China', 110th Cong. 2 (2008) (statement of Ronald J. Deibert, Citizen Lab Director), www.uscc.gov/sites/default/files/6.18.08%20Deibert.pdf.
—— (2008b), 'Hearing: Access to Information and Media Control in the People's Republic of China, 110th Cong. 2 (2008) (statement of Gilbert Kaplan, King & Spalding LLP), www.uscc.gov/sites/default/files/6.18.08Kaplan.pdf.
US International Trade Commission (USITC) (2013), *Digital Trade in the US and Global Economies, Part 1*, Investigation No. 332-532, www.usitc.gov/publications/332/pub4415.pdf.
—— (2014), *Digital Trade in the US and Global Economies, Part 2*, Investigation No. 332-540, Publication 4485, September, www.usitc.gov/publications/332/pub4485.pdf.
United States Trade Representative (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.
—— (2014) *2014 National Trade Estimate Report on Trade Barriers*, Washington, DC: United States Trade Representative, https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2014-NTE-Report.
—— (2015), 2015 National Trade Estimate Report on Trade Barriers, Washington, DC: United States Trade Representative, https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2015/2015-national-trade-estimate.
—— (2016a), 'The Trans-Pacific Partnership', https://ustr.gov/sites/default/files/TPP-Promoting-Digital-Trade-Fact-Sheet.pdf.
—— (2016b), 2016 National Trade Estimate Report on Trade Barriers, Washington, DC: United States Trade Representative, https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2016/2016-national-trade-estimate.
—— (2017a), 2017 National Trade Estimate Report on Trade Barriers, Washington, DC: Office of the United States Trade Representative, https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2017/2017-national-trade-estimate.
—— (2017b), 'Summary of Objectives for the NAFTA Renegotiations', United States Trade Representative, Washington, DC, https://ustr.gov/sites/default/files/files/Press/Releases/Nov%20Objectives%20Update.pdf.
Valeriano, B. (2016), 'The Rise of Cyber Repression', Defense One, 13 January, www.defenseone.com/ideas/2016/01/rise-cyber-repression/125095/.
West, D. M. (2016), 'Internet Shutdowns Cost Countries $2.4 billion Last Year', Brookings Institution, October, www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf.
—— (2017), 'How to Combat Fake News and Disinformation', Brookings Institution, 18 December, www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/.
World Bank, (2016), 'World Development Report 2016: Digital Dividends', http://www.worldbank.org/en/publication/wdr2016.
World Trade Organization (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, 20 September.
—— (2016), World Trade Statistical Review 2016, www.wto.org/english/res_e/statis_e/wts2016_e/wts2016_e.pdf.
—— (2017a), 'Members Debate Cyber Security and Chemicals at Technical Barriers to Trade Committee', 14–15 June, www.wto.org/english/news_e/news17_e/tbt_20jun17_e.htm.
—— (2017b), Work Programme on Electronic Commerce, Mininstrial Decision of 13 DECEMBER 2017, WT/MIN(17)/65 WT/L/1032, 18 December 2017, www.wto.org/english/tratop_e/ecom_e/ecom_e.htm.
—— (2018), WTO Council for Trade in Services, Report of the Meeting Held on 2 March 2018, Note by the Secretariat, S/C/M/134, 5 April 2018.

Wu, T. (2006), 'The World Trade Law of Censorship and Internet Filtering', Chicago Journal of International Law, 7(1), 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): 319–355.

Xu, B. and E. Albert (2017), 'Media Censorship in China: Council on Foreign Relations', 17 February, www.cfr.org/backgrounder/media-censorship-china.

Yaxley, L. (2018), 'TPP Resurrected: Here's What's in the Latest Trans-Pacific Partnership Trade Deal and What It Means for You', ABC News, 25 January, www.abc.net.au/news/2018-01-24/what-is-the-new-tpp-and-what-does-it-mean-for-australia/9357020.

Zetter, K. (2016), 'The Biggest Security Threats We'll Face in 2016', Wired, 1 January, www.wired.com/2016/01/the-biggest-security-threats-well-face-in-2016/.