Oxford Review of Economic Policy, 2023, **39**, 98–109
https://doi.org/10.1093/oxrep/grac046
Article

OXFORD

Building trust in digital trade will require a rethink of trade policy-making

Susan Ariel Aaronson*

* Elliott School of International Affairs, George Washington University, USA, e-mail: saaronso@gwu.edu

Parts of this paper were previously published as a CIGI Policy brief, CIGI Paper # 258, 'Listening to Users and Other Ideas for Building Trust in Digital Trade', https://www.cigionline.org/publications/listening-to-users-and-other-ideas-for-building-trust-in-digital-trade/.

Abstract:

In 2019, Shinzo Abe, then Prime Minister of Japan, stated that if the world wanted to achieve the benefits of the data-driven economy, members of the World Trade Organization should find a common approach to combining 'data free flow with trust'. However, he never explained what these rules should look like and how nations might find an internationally accepted approach to such rules. In this paper, I argue that trade policy-makers must pay closer attention to users' concerns if they truly want to achieve 'data free flow with trust'. I begin with an examination of what the most recent digital trade/ecommerce agreements say about trust and discuss whether they actually meet user concerns. Next, I turn to three different examples of online problems that users have expressed concerns about, namely internet shutdowns/censorship, disinformation, and ransomware, describing how these may yield both trade distortions and less trust online. I argue that policy-makers should address these issues if they believe trade agreements should build trust in cross-border data flows. Moreover, I argue how policy-makers respond to user concerns is as important as what they include in trade agreements. Finally, I note that trade negotiators will need to rethink how they involve the broad public in digital trade policy-making, while recognizing that trade policy agreements may not be the best place to address these problems.

Keywords: data, trade, trust, free-flow, feedback loop

JEL classification: F10, F29, L88, P16, M48

I. Introduction

When we go online, download an app, buy a sweatshirt, or peruse TikTok, we are taking a leap of faith—acting with agency in an environment without control or certainty. We *trust* the firms that provide these services will not only provide us with goods and services, but that they will also protect our personal data and do their best to prevent us—their stakeholders—from harm. As political theorist Francis Fukuyama has written: 'Trust is the expectation... of regular, honest, and cooperative behavior, based on commonly shared norms, on the part of other members of that community' (Fukuyama, 1996, p. 24). According to the OECD, 'trust is also the foundation upon which the legitimacy of public institutions is built and is crucial for maintaining social cohesion'.[1]Trust is essential to democratic capitalist functioning, and in particular to trade, because buyers and sellers don't know each other. But the same is true for users and providers online.

Yet no one knows how to build or sustain trust in the face of rapid data-driven change. Online 'trust must be negotiated with others whom users do not see, with faraway enterprises, under circumstances that are not wholly familiar, in a world exploding with information of uncertain provenance' (Rainie and Anderson, 2017).

Since the onset of the global pandemic, individuals, companies, and governments have become increasingly dependent upon the internet and data-driven services to work, learn, and socialize. These new services helped sustain the global economy and allowed many to connect, work, study, and prosper online through lockdowns (Internet Society, 2020; Anderson *et al.*, 2021). Yet because many of these services are built on the collection, analysis, and

[1] OECD, 'Trust in Government', https://www.oecd.org/gov/trust-in-government.htm

monetization of personal data, they also threaten our autonomy, individual rights, and systems of governance (Aaronson, 2018*a*; Office of the High Commissioner, 2021). The US National Intelligence Council has issued a stark warning that:

> privacy and anonymity may effectively disappear by choice or government mandate, as all aspects of personal and professional lives are tracked by global networks. Moreover, real-time, manufactured, or synthetic media could further distort truth and reality, destabilizing societies at a scale and speed that dwarfs current disinformation challenges. (National Intelligence Council, 2021, pp. 48–9)

These concerns about online security are reflected in surveys of users. In 2019, the Pew Foundation found that many people are afraid that their data are used without their consent, and concerned that firms use their clients' personal data to discriminate and manipulate them (Auxier *et al.*, 2019). Likewise, CIGI and IPSOS suggested 75 per cent of 25,000 users polled cited Facebook, Twitter, and other social media platforms as contributing to their lack of trust. In the same survey, 78 per cent of respondents were concerned about their online privacy, with over half more concerned than they were a year ago (CIGI-IPSOS, 2019). Similar concerns are seen in data collected by the Oxford Internet Institute in 2020 which showed that for those active online, around half are concerned about disinformation and 71 per cent of internet users are worried about a mixture of online threats, including disinformation, fraud, malware, spyware, and harassment (Knutila *et al.*, 2020).

Given this situation, in 2019 Prime Minister Shinzo Abe of Japan decided that he could both reinvigorate negotiations over cross-border data flows at the World Trade Organization (WTO) and build trust in policy-makers' efforts to govern data. Policy-makers have been trying to negotiate such rules since the first e-commerce agreement (Australia/Singapore) in 2003 (Weber, 2015). Abe stated that he wanted the Osaka meeting of the Group of 20 nations (the G-20) 'to be long remembered as the summit that started world-wide data governance... under the roof of the WTO' (Abe, 2019). He noted that data-driven services are built on data collected from individuals in one country and often stored or analysed in another. Such cross-border flows underpin both the internet and the global economy. Hence, data free flow with trust meant that countries would allow medical, industrial, and other nonpersonal data to freely flow across borders, but 'put our personal data and data embodying intellectual property, national security intelligence, and so on, under careful protection' (Abe, 2019).

However, although Abe argued that certain types of data needed special rules to facilitate trust, he never explained what these rules should look like and how nations might find an internationally accepted approach to such rules. Despite the lack of clarity, other international organizations have underscored the concept that data will not flow freely without trust, including the G-20,[2] the OECD,[3,5] the World Economic Forum, and most recently the G-7.[4]

Despite this consensus on the need to link free flow and trust, the trade regime is not the only or best venue to discuss this issue. Policy-makers discuss trust and data flows at other venues including the UN[5] and the OECD.[6] But trade agreements are binding and generally disputable. Moreover, digital trade agreements generally include language making the free flow of data a default, with certain exceptions. These agreements also address measures that can distort the free flow of data, such as spam.

This author is deeply ambivalent about this focus on trade agreements as a tool to govern data. First, although data are constantly exchanged between entities in different countries, such exchange is not always accompanied by a transaction and may not be 'traded'. Moreover, data are multidimensional—they are not just a commercial asset but a public good and a national security problem. Policy-makers have not figured out how to encourage data sharing and the broad use of data to address wicked problems that transcend nations and borders, such as climate change (Aaronson, 2022). Finally, much of the data flowing across borders are aggregated and allegedly anonymized personal data. While users may benefit from services built on data, the people who are the sources of those data do not control them. The data are their assets, yet they cannot manage, control, exchange or account for them (World Economic Forum, 2011, p. 11). Individuals' data can essentially be weaponized to create malicious cross-border data flows, whether through disinformation, malware, spam, or other means. Nonetheless, trade

[2] OECD, 'Mapping Approaches to Data and Data Flows', Report for the G20 Digital Economy Task Force, Saudi Arabia 2020, https://www.oecd.org/sti/mapping-approaches-to-data-and-data-flows.pdf. The G-20 is comprised of the world's 20 largest economies.

[3] Organization for Economic Cooperation and Development, TAD/TC/WP (2020)15/, 'Mapping Commonalities in Regulatory Approaches to Cross-border Data Transfers', 7 April 2021.

[4] 'G-7 Roadmap for Cooperation on Data Free Flow with Trust', 28 April 2021, http://www.g8.utoronto.ca/ict/2021-annex2-roadmap.html. The G-7 (or Group of Seven) is an organization made up of the world's seven largest so-called advanced economies: Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States. https://www.bbc.com/news/world-49434667

[5] https://www.un.org/tr/desa/internet-forum-aims-build-trust-while-leaving-no-one-offline.

[6] https://goingdigital.oecd.org/dimension/trust.

agreements are vehicles to build trust because they are commitment devices. They build trust by clarifying how and when nations can trade and how and when they can violate trade rules.

Policy-makers are eager to build trust in how they govern data. But the process of negotiating trade agreements (which is secretive) could be problematic to engendering trust. Some believe that trade negotiations allow policy-makers to deliver on behalf of special interests such as large digital platforms, rather than the broad public Others argue that because the process is secretive, policy-makers can avoid catering to national special interests.[7] Hence, how policy-makers respond to what their citizens say they need or are concerned about is as important as what (the specific rules) when designing rules and institutions of governance.

This paper focuses on both what policy-makers include in trade agreements and how they include these provisions. I focus on three concerns impeding trust online: internet shutdowns and censorship, disinformation, and ransomware (a form of malware).[8] I will show that these problems are increasingly visible, and trade distorting. Moreover, all three may undermine trust, which could lead consumers and firms to be more cautious in their online operations. Over time, that could reduce market growth for users and providers of data-driven services.

The paper proceeds as follows. In the next section I examine what trade agreements say about trust and discuss why the current strategy cannot meet the goal of building trust. Section III then examines the trade and governance implications of censorship, internet shutdowns, and ransomware. The paper then concludes with some recommendations on how Prime Minister Abe's vision of 'data free flow with trust' can be achieved, focusing on the role of public engagement and participation by end-users as well as the firms that provide data-driven services that have traditionally driven digital trade agreements (Internet Society, 2019*b*).

II. What do trade agreements say and why isn't it sufficient to sustain trust?

Trust involves an expectation that a person will perform a particular action. Trust and trade almost certainly evolved together, each reinforcing the other (Seabright, 2010; Ridley, 2011), while the concept of trust emerged in society when individuals began to believe that other people would follow the rules or experience shame and other forms of societal punishment.

Against this background, trade agreements are designed to build trust because they provide a formal commitment among governments that the rule of law will govern trade and that commitments will be kept (Anomaly, 2017). By building trust, trade diplomats believe trade agreements expand trade, which then reinforces policy-makers' willingness to participate in these commitment devices. In short, trade agreements are supposed to create a virtuous circle between trust and trade (Rose, 2004; Roy *et al.*, 2014).

Policy-makers have not, however, routinely thought about how to build trust in agreements governing digital trade. Digital trade in this context refers to commerce enabled by electronic means—by telecommunications and/or ICT services—and covers trade in both goods and services including trade in end-products, such as downloaded movies and streaming services, as well as products and services that rely on or facilitate digital trade, such as cloud data storage, communication services, and email.

Table 1 describes seven trade agreements which are currently in effect to illuminate their similarities and differences. Of the seven agreements, only four mention trust. But none says how it will use trade policies to build trust and address the concerns of users about the free flow of data across borders.

Most digital trade agreements require the signatories to allow data to flow freely among nations with limited exceptions to achieve national policy goals. In six of the seven agreements described above, these provisions are binding and disputable. Binding means the signatory must adhere to the agreement; disputable means that signatories can initiative a trade dispute to challenge barriers to the free flow of data, even when another signatory tries to justify such barriers as necessary under the exceptions (for example, to protect national security, social stability, public health, or privacy (the General Agreement on Trade in Services (GATS) exceptions)). However, under the Regional Comprehensive Economic Partnership (RCEP), nations can use the exceptions (as under any other trade agreement). But other nations cannot use a trade dispute to challenge the use of these exceptions as these provisions are not subject to dispute settlement. Instead, RCEP recommends that they solve these differences through good faith efforts and consultation.[9]

[7] https://www.washingtonpost.com/news/monkey-cage/wp/2015/09/24/do-trade-negotiations-have-to-be-done-in-secret-heres-what-experts-think/

[8] The actors who create and disperse ransomware may target users of all types—from the home user to the corporate network. Users attacked by ransomware may lose sensitive or proprietary information, incur financial loss, suffer reputational harm, and their operations may be disrupted (see Travelers Insurance, 'What is the Current Ransomware Landscape?', https://www.travelers.com/resources/business-topics/cyber-security/what-is-the-current-ransomware-landscape.

[9] RCEP Article 17, p. 7 https://www.bilaterals.org/IMG/pdf/rcep-e-commerce-chapter-2.pdf

Table 1: What seven digital trade agreements say about building trust

Provision	CPTPP	US–Japan DTA	USMCA	DEPA	AU/Sign Digital Economy Agreement	EU–UK TCA	RCEP
Came into effect	March 2018	October 2019	December 2019	June 2020	December 2020	December 2020	December 2021
Does the agreement mention trust?	No	No	No	Yes	Yes	Yes	Yes
Enforce domestic laws regarding privacy?	Yes	Yes	Yes	Yes	Yes	Yes	No Adopt or maintain laws
Enforce domestic laws regarding consumer protection?	Yes	Yes	Yes	Yes	Yes	Yes	No Adopt or maintain laws
Enforce domestic laws regarding spam?	Yes	Yes	Yes	Yes	Yes	Yes	No Adopt or maintain laws

Source: Table by Andrew Kraskewicz with S. Aaronson.

The EU model is slightly different. EU agreements, such as the EU/UK Trade and Cooperation Agreement, essentially say that non-personal data can flow freely across borders, but personal data of Europeans can only flow freely across borders to nations that it deems are adequate or have some equivalent data protection regime.

All of these agreements except RCEP require signatories to enforce their own laws regarding personal data protection, spam, and consumer protection. To some extent this is because there is no internationally accepted law to guide governments that seek to protect personal data, consumer welfare, or prevent spam. RCEP requires its signatories to adopt or maintain such laws but says nothing about enforcement. Moreover, all the other agreements encourage nations to work together towards interoperable approaches, but RCEP says 'the Parties shall endeavor to undertake forms of co-operation that build on and do not duplicate existing cooperation initiatives pursued in international fora'.[10] Such language is essentially suggesting that the trade regime is not the right place to foster interoperability or regulatory coherence.

Finally, as Table 2 shows, these agreements generally ban only two practices that may undermine trust among online market actors. All seven prohibit requirements that data be stored in local servers. RCEP states that 'the Parties recognize that each Party may have its own measures regarding the use or location of computing facilities, including requirements that seek to ensure the security and confidentiality of communications'. RCEP essentially says that there may be times that governments can legitimately rely on this practice.[11] All except RCEP forbid signatories from adopting performance requirements, such as when firms must divulge proprietary data in order to sell or produce goods in another nation.

Taken in sum, the seven agreements show that some nations, particularly in Asia, Europe, and North America, have made significant progress in setting rules governing cross-border data flows. However, such language is unlikely to build user trust.

First, signatories are supposed to use the exceptions only when necessary and in a non-discriminatory manner. However, there are few shared norms or trade disputes regarding how nations should behave when rules governing data flows conflict with the achievement of domestic policy objectives. Consequently, the exceptions risk becoming the rule without clear guidance on how and when their use can be limited.

Second, while some agreements mention the import of international cooperation on protecting personal data, they do not explain how nations can make their different approaches interoperable. Without such clarity, people will always be afraid that their personal data may be inadequately protected or misused in venues beyond their control.

Third, most trade agreements include vague aspirational language on cybersecurity. According to the OECD, these provisions generally stipulate that the parties recognize the importance of building the capacity of their national entities responsible for computer security incident response and will cooperate on matters related to

[10] RCEP Article 4, Cooperation, Electronic Commerce Chapter, pp. 2–3, https://www.bilaterals.org/IMG/pdf/rcep-e-commerce-chapter-2.pdf

[11] Article 15, 16, https://www.bilaterals.org/IMG/pdf/rcep-e-commerce-chapter-2.pdf

Table 2: Overview of recent digital trade agreements

Provision	CPTPP	US–Japan DTA	USMCA	DEPA	AU/Sign Digital Economy Agreement	EU–UK TCA	RCEP
Came into effect	March 2018	October 2019	December 2019	June 2020	December 2020	December 2020	December 2021
Language explicitly encouraging cross-border data	Yes	Yes	Yes	Yes	Yes	Yes	Yes Parties shall not prevent flows
GAT/GATS exceptions	Yes	Yes	Yes	Yes	Yes	Yes	Yes Self-judging and subject to dispute
Bans on performance requirements such as sharing source code and/or algorithms	Yes Source code only	Yes	Yes	Yes	Yes	Yes Source code only	No
Ban on data localization	Yes	Yes	Yes	Yes	Yes	Yes	No
Regulations banning divulgence of encryption	No	Yes	No	Yes	Yes	No	No
Language encouraging signatories to develop, cooperate on cybersecurity	Yes	Yes	Yes	Yes	Yes	Yes	Yes Using existing mechanisms

Source: Table by Andrew Kraskewicz with S. Aaronson.

cyber security, without specifying what these mechanisms might be (OECD, 2021, p. 21). The US–Mexico–Canada Agreement (USMCA) further requires each party to endeavour to employ risk-based approaches that rely on consensus-based standards and risk-management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.[12]

Finally, the agreements ban spam. Spam is not the same as disinformation, but they have some things in common. Both are malicious cross-border data flows. Deployers of spam, malware, and disinformation often rely on bots to disseminate such data across borders. Yet while almost every digital trade agreement discusses spam, these agreements do not address other issues such as disinformation or ransomware. Nor do they address censorship and internet shutdowns.

In an earlier article, I showed how censorship and malware could be seen by trade policy-makers and business executives as barriers to trade because they could violate WTO norms of non-discrimination (most favoured nation and national treatment, as well as market access (Aaronson, 2018*b*). Table 3 focuses on the three problems mentioned earlier: censorship, disinformation, and ransomware. I show how these problems could distort trade and discuss how in the absence of rules, trade diplomats could adopt responses that could also be seen as trade distorting. Although these problems are of significant concern to users, they are not yet governed by any trade agreement. Given that these problems undermine trust and policy responses could also distort trade, it is clear that policy-makers should try to bring these threats into the rules-based system or clarify how policy-makers can respond through trade disputes.

The next section describes how these issues could affect both trade and trust.

III. Shutdowns, censorship, and ransomware: case studies

(i) Internet shutdowns and censorship

Internet shutdowns have become a frequent online occurrence. The digital rights group Access Now defines internet shutdowns as an intentional disruption of internet or electronic communications, rendering them inaccessible or

[12] USMCA, Art. 19.15.2

Table 3: Online threats and their trade implications

Online threats and how they may violate trade norms	Policy responses to limit online threats that reduce trust	Is a proposed policy response a potential trade barrier?
Disinformation can undermine market access and stability. Could also violate the WTO norm of 'like product', which means nations cannot discriminate among two similar products from different nations.	Policies to limit cross-border disinformation, e.g. ban automated bots which are created to send disinformation across borders.	Could violate national treatment.
Ransomware could undermine market access and stability. Could also violate like product.	Policies to limit cross-border flows of ransomware, such as reporting requirements.	Could violate national treatment.
Censorship could undermine market access and stability.	Policies to clarify when governments can censor under the exceptions.	Could lead to a trade dispute to establish clarity (e.g. is China's Great Firewall a trade barrier).

Sources: Aaronson (2019, 2022).

effectively unusable, for a specific population or within a location, often to exert control over the flow of information.[13] Many countries routinely restrict the internet (e.g. China, Iran) while others use protests, elections, national exams, or other events to justify shutting off the internet (India, Cuba, Ethiopia, Belarus, etc.).[14] While most countries doing blanket shutdowns are authoritarian states, leaders in some democratic states including the US,[15] India,[16] and Brazil[17] have restricted access to apps and various platforms. Such 'partial' shutdowns by democratic policy-makers make it harder to credibly argue that the internet requires the free flow of data across borders to function efficiently.

According to a 2020 analysis by the *Wall Street Journal*, firms such as AT&T, Telenor, or Vodaphone that provide internet access must often sign contracts approved by various governments. In these contracts, these firms are not allowed to delineate when such shutdowns occurred or why. To uncover or confirm shutdowns that are not disclosed, some human rights and internet monitoring groups rely on diagnostic tools that measure changes in network activity (Solomon, 2020).

Full and even partial internet shutdowns directly affect users. They undermine access to information and make it almost impossible for users to express their opinions or participate politically since so many activities are now solely online (OECD, 2016; Aaronson, 2018*a*). Not surprisingly, these shutdowns can undermine trust in government as well as in providers of internet services (Shandler, 2018; Shandler *et al.*, 2019; UN Human Rights Council, 2016).

Internet shutdowns have both direct and indirect economic effects. They can hamper productivity, frustrate business confidence, and raise firm and consumer costs (Deloitte, 2016). Internet shutdowns can lead to less business, lost tax revenues, and lower worker productivity (West, 2016). When officials place limitations on which firms can participate in the network, they reduce its overall size and generativity. They can also increase costs to local businesses, affect global value chains, and reduce technology diffusion, thereby undermining development and trade (Box and West, 2016, p. 2).

It is hard to quantify the financial costs of internet shutdowns. Current estimates are small relative to the size of the internet economy. One estimate by West (2016) put the global cost of internet shutdowns in 2016 at $2.4 billion. Two researchers who regularly track these shutdowns estimate the global costs of these shutdowns in 2021 as $5.45 billion, which is up 36 per cent from 2020 figures.[18] These estimates are likely inexact as it is difficult to survey each user and website to ascertain how the shutdown affected them and for how long. However, the cost to

[13] https://www.accessnow.org/cms/assets/uploads/2021/02/Read-Me_-How-to-view-the-Access-Now-Internet-Shutdown-Tracker-Updated-Mar-2021.pdf, p. 4, fn 1. Access Now found that in 2019, 1,706 days of internet access were disrupted by 213 internet shutdowns across 33 countries.

[14] https://netblocks.org/reports.

[15] The Trump Administration tried to ban two Chinese-owned apps for alleged national security reasons, but the courts did not uphold the bans and the Biden Administration has abandoned this plan. https://www.bbc.com/news/technology-54205231; and https://www.bankinfosecurity.com/biden-assesses-us-policies-on-china-cybersecurity-issues-a-16000.

[16] https://www.reuters.com/article/us-india-china-apps/india-retains-ban-on-59-chinese-apps-including-tiktok-idUSKBN29U2GJ.

[17] https://techcrunch.com/2016/07/19/whatsapp-blocked-in-brazil-again/.

[18] S. Woodhams and S. Migliano, 'The Global Cost of Internet Shutdowns in 2021', https://www.top10vpn.com/research/cost-of-internet-shutdowns/2021/.

human rights—including access to information—are sizeable. Woodhams and Migliano estimated that some 486.2 million people were affected by these shutdowns, up 80 per cent from 2020. Sixty-nine per cent of all internet disruptions were also associated with restrictions on freedom of assembly; 29 per cent with election interference; and 29 per cent with infringements on freedom of the press.[19]

Policy-makers may intend to only affect the internet within their borders, seen by their citizens, but such shutdowns resonate globally because the internet is a shared resource and shutdowns may reduce internet stability and diminish the predictability of data flows (Google, 2010; OECD, 2016): shutdowns export these negative effects to other markets (Aaronson, 2018*a*). By blocking all content, internet shutdowns are a form of indiscriminate censorship, directly affecting a wide range of users and providers online. And by encompassing all forms of digital communication from email, to social networks, to mobile phone services, they not only block content but rather the act of communication (Wagner, 2012).

No trade agreement thus far says anything about internet shutdowns despite their cross-border implications. As noted by the Internet Society, governments must apply their national legislation to cross-border platform firms and 'unless they are able to get effective collaboration from such platforms, this cross-border complexity may lead some governments to instead opt for the more heavy-handed approach of shutting down the ability to access to these platforms entirely'. (Internet Society, 2019*a*) Failure to address shutdown risks collaboratively may lead governments to more drastic solutions.

Policy-makers have never challenged shutdowns or censorship in a trade dispute. The US (and for a time the EU), however, has at times flirted with the idea of examining censorship as a trade barrier (Aaronson, 2018*b*). However, in 2020, the US Senate Finance Committee Chairman requested that the US International Trade Commission (USITC) examine if censorship is a barrier to trade and then measure the costs of such censorship to trade. The requestors defined censorship broadly as 'the prohibition or suppression of speech or other forms of communication', and stated that foreign governments use many tools to carry out censorship, including technological measures that restrict digital trade. The Committee said that these tools, and the policies that enable them, allow authorities in foreign markets to limit speech by controlling the flow of information and services.[20]

The USITC issued its first response in February 2022 (USITC, 2022). The Commission identified six markets: China, Russia, Turkey, Vietnam, India, and Indonesia, which censored US digital exports. The investigators concluded

> the evolution of censorship policies and practices in the past five years in the key markets has largely been driven by the growing importance of the internet. US internet companies report ever-growing numbers of government requests for the takedown of online content. Moreover, governments are using multiple levers—from data and personnel localization requirements to threats of retaliation—to pressure compliance with censorship policies. Technological developments, such as the growing reliance on artificial intelligence by governments and internet companies to identify and suppress large quantities of online content, also present substantial challenges. Finally, 'foreign governments' censorship policies and practices may be augmented by extraterritoriality and self-censorship. Extraterritorial censorship occurs when governments seek to suppress speech outside of their borders.[21]

The USITC study has the potential to establish the basis for developing a common approach to addressing a wide range of barriers, from censorship to distributed denial-of-service (DDoS) attacks that impede market access as well as human rights. However, nations don't agree on whether such a common approach to defining shutdowns or censorship as a barrier is ultimately useful. Trade diplomats from countries such as India that frequently shut down the internet can always justify their actions as appropriate under the exceptions. Again, for this reason, trade disputes might provide clarity.

(ii) Disinformation

Disinformation can be home-grown or imported as a form of cross-border data flows. But trade diplomats are reluctant to use trade agreements to regulate it. After all, disinformation is a form of self-expression and nations have evolved different visions of what speech should be regulated online, what should be removed, and who should decide these questions (business, government, civil society?). The US sits on one end of a continuum, where law

[19] Ibid.
[20] https://usitc.gov/secretary/fed_reg_notices/332/332_585_notice_01262021sgl.pdf.
[21] USITC (2022), 'Foreign Censorship, Part 1: Policies and Practices Affecting US Businesses', February 2022, p. 12, https://www.usitc.gov/publications/332/pub5244.pdf.

and culture dictate that there should be relatively few restrictions on speech and government plays a limited role in regulating social networks. US policies are guided by Section 230 of the 1996 Communications and Decency Act which says that 'No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.' The protected intermediaries include not only regular Internet Service Providers (ISPs), but also a range of 'interactive computer service providers', including basically any online service that publishes third-party content from Target, Yelp, Amazon, or Trip Advisor.[22]

China, Iran, and Vietnam are examples of countries at the other end of the continuum. In these countries, free speech is extremely restricted and government censors decide appropriate and inappropriate content (Levush, 2019; Morar and Dos Santos, 2020). Most democracies sit somewhere in between these positions.

Around the world, policy-makers (and firms) are not only using content moderation regulations to address disinformation.[23] They are trying to develop technical fixes; new regulations; political advertising; training citizens to recognize disinformation; funding investigations and enforcement actions; and helping other governments address disinformation. The Carnegie Endowment for International Peace, the *Washington Post* and *The Guardian* recently published descriptions of innovative ideas to address disinformation.[24]

Given this patchwork of approaches, policy-makers recognize the need for collective action. The members of the G-7 who met in Canada in June 2018 agreed to the 'Charlevoix Commitment on Defending Democracy from Threats'. The G-7 agreed to establish a G-7 Rapid Response Mechanism (RRM) to strengthen coordination to identify and respond to diverse and evolving threats and to information sharing.[25] France has tried to organize nations to band together to find effective solutions to the problems of disinformation and cyber-insecurity.[26]

However, these strategies can do little to mitigate cross-border disinformation flows or prod firms to address some of the problems with their current business model. As with labour and environment, uncoordinated national strategies to address the problem could lead to a race to the bottom among some nations to encourage firms to locate in their countries. Trade agreements are not the best place to address disinformation, but they are a venue where the international aspects could be addressed. Trade diplomats could adopt a more coordinated approach, which I describe later in this paper.

(iii) Ransomware

Ransomware has become one of the most dangerous online threats, primarily to firms and service providers. Ransomware is just one of many different types of malware (malicious data flows). Malware is widely available online, can infect almost any type of internet device, and is a growing service sector.[27] Bad actors can use ransomware to steal data and credentials, or even wipe data.[28] Given these diverse effects, it is hard to estimate the costs of ransomware to the global or national economy. According to Sonic Wall, a cybersecurity firm, from January to June 2021, the number of global ransomware attacks was 304.7 million, surpassing 2020's full-year total (304.6 million)—a 151 per cent year-to-date increase.[29] The European Union Agency for Cybersecurity

[22] https://uscode.house.gov/view.xhtml?req=(title:47%20section:230%20edition:prelim) and https://www.eff.org/issues/cda230. The Trump Administration proposed several reforms, https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996.

[23] A listing of national laws regarding fake news is provided at https://www.reuters.com/article/us-singapore-politics-fakenews-factbox/factbox-fake-news-laws-around-the-world-idUSKCN1RE0XN. On the corporate side, for example, Twitter is asking its users to identify disinformation (to crowdsource it). https://www.cnn.com/2021/01/25/tech/twitter-birdwatch/index.html?btee=fzNssD67tONL%2B6XKocxD6pIR7KzJ7ZRyaSpXYdK4Tt0D6a8MLR2%2FaoG25sc1hGD9 &btts=1611634136462; while Facebook is trying to make its campaign advertising business more transparent and its algorithms more sensitive to verified news and to curb political advertising during times of political volatility. https://www.axios.com/facebook-to-downplay-politics-on-its-platform-78364717-3f52-4cd2-b8e7-8efe6d8f4960.html?stream=technology&utmsource=alert&utmmedium=email&utmcampaign=alertstechnology. See also Chakravorti, 'Social media companies are taking steps to tamp down coronavirus misinformation—but they can do more', *The Conversation*, 30 March 2020, https://theconversation.com/social-media-companies-are-taking-steps-to-tamp-down-coronavirus-misinformation-but-they-can-do-more-133335.

[24] https://carnegieendowment.org/2020/12/14/mapping-worldwide-initiatives-to-counter-influence-operations-pub-83435; https://www.theguardian.com/media/2021/jan/16/how-to-fix-social-media-trump-ban-free-speech?CMP=ShareiOSAppOther&twitterimpression=true&s=03; 'Joe Heim, "Disinformation can be a very lucrative business, especially if you're good at it," media scholar says', *Washington Post*, 19 January 2021.

[25] https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation-2-0/.

[26] https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/fight-against-organized-criminality/cyber-security/.

[27] https://www.oecd.org/coronavirus/policy-responses/dealing-with-digital-security-risk-during-the-coronavirus-covid-19-crisis-c9d3fe8e/.

[28] Christine Runnegar, 'Hit Pause: Take a Moment to Reflect on the Repercussions of the Recent Ransomware Attacks', 6 July 2017, Internet Society Blog, https://www.internetsociety.org/blog/2017/07/hit-pause-take-a-moment-to-reflect-on-the-repercussions-of-the-recent-ransomware-attacks/.

[29] Helpnet Security, 'Ransomware Attacks Skyrocketed in H1 2021', 3 August 2021,https://www.helpnetsecurity.com/2021/08/03/ransomware-attacks-h1-2021/.

(ENISA) reports that between May 2021 and June 2022, about 10 terabytes of data were stolen each month by ransomware threat actors.[30]

As with internet shutdowns, these estimates may seem small. But they are inexact, as victims are often embarrassed to report such attacks.[31] In recognition that ransomware was a growing problem that was not accurately reported by victims (who wants to admit that their defences are inadequate?), the Senate Homeland Security Committee investigated. In March 2022, Congress passed and President Biden enacted a law requiring critical infrastructure owners and operators to report to the Cybersecurity and Infrastructure Security Agency (CISA) within 24 hours if they make a ransomware payment and within 72 hours if they experience a substantial cybersecurity incident.[32]

In the wake of the rise in numbers of malware and other online threats, most countries have adopted cybersecurity strategies. These strategies serve to define threats and illuminate how government is responding. The International Telecommunications Union found over 100 countries have cybersecurity strategies, not including those in draft.[33]

Malicious cross-border data flows are trade problems, but efforts to address these flows (cybersecurity strategies) can also distort trade (Meltzer and Kerry, 2019). Members of the WTO discussed this problem in 2017. The European Union, the United States, Japan, Canada, and Australia asked China to define the scope of its cyber security regulations and clarify the definitions of key terms such as 'secure and controllable services and products' that are covered by Chinese cybersecurity laws. While members acknowledged the importance of safeguarding against 'network intrusions', and 'cyber-attacks', as well as protecting users' personal information and sensitive data, they urged China to implement relevant measures in a non-discriminatory manner and in line with the WTO Technical Barriers to Trade (TBT) Agreement.[34] In so doing, they urged China to understand that cybersecurity regulations should not become technical barriers to trade. Any such regulation should be necessary, consistently applied to all WTO members, and transparently administered.[35]

Malware is not just a trade problem; as with shutdowns, it can affect internet openness and generativity (OECD, 2016). It is also a shared problem. According to Microsoft,

> it takes new levels of collaboration to meet the ransomware challenge. The best defences begin with clarity and prioritization, which means more sharing of information across and between the public and private sectors and a collective resolve to help each other make the world safer for all.[36]

Governments have turned to the UN system to develop norms for cybersecurity. In March 2021, the 193 members of the UN Open-Ended Working Group agreed to endorse a report that promotes responsible state behaviour in cyberspace. The report notes that data-driven technologies 'can be used for purposes that are inconsistent with the objectives of maintaining international peace, stability and security'. It also notes

> States concluded that threats may be experienced differently by States according to their levels of digitalization, capacity, ICT security and resilience, infrastructure and development. Threats may also have a different impact on different groups and entities, including on youth, the elderly, women and men, people who are vulnerable, particular professions, small and medium-sized enterprises, and others. In light of the increasingly concerning digital threat landscape and recognizing that no State is sheltered from these threats, States underscored the urgency of implementing and further developing cooperative measures to address such threats. (UN General Assembly, 2021)

But the document is vague as to what states should do about addressing these threats beyond creating norms for state actions.

[30] https://www.enisa.europa.eu/news/ransomware-publicly-reported-incidents-are-only-the-tip-of-the-iceberg.
[31] https://www.zdnet.com/article/reported-ransomware-attacks-are-just-the-tip-of-the-iceberg-thats-a-problem-for-everyone/.
[32] Senate Homeland Security and Government Affairs, 'Peters Announces Investigation Into Rise of Ransomware Attacks and How Cryptocurrencies Facilitate Cybercrimes', 20 July 2021, https://www.hsgac.senate.gov/media/majority-media/peters-announces-investigation-into-rise-of-ransomware-attacks-and-how-cryptocurrencies-facilitate-cybercrimes and https://www.hsgac.senate.gov/media/majority-media/peters-and-portman-landmark-provision-requiring-critical-infrastructure-to-report-cyber-attacks-signed-into-law-as-part-of-funding-bill-.
[33] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.
[34] WTO, TBT Committee, 'Members Debate Cyber Security and Chemicals at Technical Barriers to Trade Committee', 14–15 June 2017, https://www.wto.org/english/news_e/news17_e/tbt_20jun17_e.htm.
[35] https://www.wto.org/english/tratop_e/tbt_e/tbt_e.htm.
[36] Microsoft Security Team, 'Cybersignals: Defend Against the new Cyberspace Landscape', 22 August 2022, https://www.microsoft.com/security/blog/2022/08/22/cyber-signals-defend-against-the-new-ransomware-landscape/?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioscodebook&stream=top.

Bad actors use ransomware to take advantage of user and firm laziness—failure to: install patches on time; use updated infrastructure, hire the most effective cyber defenders. Government bodies are particularly vulnerable to ransomware, which can in turn kickstart a vicious cycle.

> Government agencies must provide public services and cannot afford to have data compromised to the point of governance paralysis. The cost of a police department unable to serve and protect the community or a school district unable to educate the community's children escalates quickly. (Subramanian *et al.*, 2020)

The cost is not just in funds, but in trust of government and trust online.

IV. Conclusion

In this paper, I have argued that policy-makers have made a choice to use trade agreements to govern the data that underpin the internet and flow across national boundaries. Trade agreements (including the WTO) are not the only or best venues, but they are where policy-makers seem to be working to build binding and disputable rules. Moreover, most digital trade agreements already addresses some barriers to cross-border data flows—it seems reasonable that policy-makers should develop provisions governing more of these barriers that also erode trust.

To some extent policy-makers have not yet addressed these concerns because they appear more sensitive to the purveyors and deployers of data-driven services than to the concerns of users. But if these policy-makers want to build trust, trade negotiators will need to rethink how they involve the broad public in digital trade policy making. The next section makes some recommendations.

(i) Some ideas to build trust among users, trade diplomats, and other market actors

If policy-makers truly want to build 'free flow with trust' into digital trade agreements, they must place trust (and user needs) at the heart of all trade agreements.

Policy-makers should expand the universe of who they listen to when they design digital trade policies (the feedback loop). Most democracies ask for public comment on their trade policies (Inter-American Development Bank, 2002; Aaronson and Zimmerman, 2007; Institute for Government, 2019). For example, the US government solicited public comment regarding whether the US should retaliate against governments imposing digital taxes.[37] Canada recently asked its citizens to comment as to whether it should join the Digital Economy Partnership,[38] while the government of Australia engaged its citizens to comment on the future of digital trade rules.[39]

But none of these countries provided evidence that the loop was complete—that they incorporated public comments into trade agreement provisions or trade policy practices. Thus, countries should:

- Create a portal and consistently ask for public comment. Incentivize public participation through town halls, in speeches, etc. Trade leaders in the legislative and executive branch should highlight the import of public comment and show how they changed public policies to meet public concerns. The International Association for Public Participation describes this process as moving from consultation and involvement to collaboration.[40]
- In their annual reports, trade-related agencies should delineate who provided public comment and how these comments were used.
- Policy-makers should also use new means (such as crowd-sourcing) to engage the public to discuss issues not yet addressed by trade agreements. For example, policy-makers could ask citizens to discuss whether banning apps is a form of censorship? If so, should we ban various apps because they threaten privacy or national security? Is there a different way to address this problem? Or should nations rely on the exceptions to protect their citizens from online harms? Are there other ways to include protective language in trade agreements?

Finally, policy-makers should note that data-driven technologies have disrupted a wide range of human activity from dating to learning. Some day soon, technologies such as spatial computing and artificial intelligence may

[37] https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/march/ustr-announces-next-steps-section-301-digital-services-taxes-investigations;https://www.usitc.gov/section_337_building_record_public_interest.htm.

[38] All FTA consultations; https://www.international.gc.ca/trade-agreements-accords-commerciaux/consultations/fta-ale.aspx?lang=eng; and on DEPA, https://www.international.gc.ca/trade-commerce/consultations/depa-apen/index.aspx?lang=eng.

[39] https://www.dfat.gov.au/trade/services-and-digital-trade/Pages/the-future-of-digital-trade-rules-discussion-paper.

[40] The International Federation for Political Participation, https://www.iap2.org/page/resources.

disrupt how trade policy is negotiated. Negotiating such agreements in secret may build trust among negotiators, but can undermine trust among their constituents. Trade officials should be asking are there ways to be more transparent about the objectives and progress of trade negotiations related to data?

References

Aaronson, S. (2018*a*), 'Data is Different Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows', CIGI Paper No. 197, https://www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows

— (2018*b*) 'What Are We Talking About When We Discuss Digital Protectionism?', *World Trade Review*, Winter, https://www.cambridge.org/core/journals/world-trade-review/article/what-are-we-talking-about-when-we-talk-about-digital-protectionism/F0C763191DE948D484C489798863E77B

— (2022), 'A Future Build on Data: Data Strategies, Competitive Advantage and Trust', CIGI Paper No. 266, June.

— Zimmerman, J. M. (2007), *Trade Imbalance: The Struggle to Weigh Human Rights Concerns in Trade Policymaking*, Cambridge, Cambridge University Press.

Abe, S. (2019), 'Toward a New Era of "Hope-driven Economy"', 23 January, https://www.mofa.go.jp/ecm/ec/page4e_000973.html

Anderson, J., *et al*. (2021), 'Experts Say the "New Normal" in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges', Pew Research Center, 18 February, https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges/

Anomaly, J. (2017), 'Trust, Trade, and Moral Progress: How Market Exchange Promotes Trustworthiness', *Social Philosophy and Policy*, **34**(2), 89–107, https://doi.org/10.1017/S026505251700022X.

Auxier, B., *et al*. (2019), 'Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information', Pew Research Center, 15 November, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Box, S., and West, J. K. (2016), 'Economic and Social Benefits of Internet Openness', OECD Digital Economy Series No. 257, Paris, Organisation for Economic Co-operation and Development, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2800227.

CIGI-IPSOS (2019), *2019 CIGI-Ipsos Global Survey on Internet Security and Trust*, https://www.cigionline.org/internet-survey-2019

Deloitte (2016), 'The Economic Impact of Disruptions to Internet Connectivity: A Report for Facebook', London, Deloitte LLP, https://www.deloitte.com/global/en/Industries/tmt/perspectives/the-economic-impact-of-disruptions-to-internet-connectivity-report-for-facebook.html.

Fukuyama, F. (1996), *Trust: Social Virtues and the Creation of Prosperity*, New York, Simon and Schuster.

Google (2010), 'Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information', https://www.google.com/googleblogs/pdfs/trade_free_flow_of_information.pdf.

Institute for Government (2019), 'Taking Back Control of Trade Policy', https://www.instituteforgovernment.org.uk/sites/default/files/publications/IFGJ5448_Brexit_report_160517_WEB_v2.pdf

Inter-American Development Bank (2002), 'The Trade Policy-making Process: Level One of the Two Level Game: Country Studies in the Western Hemisphere', http://www.sice.oas.org/ctyindex/ARG/policymaking_e.pdf

Internet Society (2019*a*), 'Policy Brief: Internet Shutdowns', 18 December, https://www.internetsociety.org/policybriefs/internet-shutdowns/

— (2019*b*), 'The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things', 11 May, https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/

— (2020), 'Insights from Internet Society's 2020 Public Pulse Survey', 19 November, https://www.internetsociety.org/resources/doc/2020/insights-from-2020-public-pulse-survey/

Knutila, A., *et al*. (2020), 'Global Fears of Disinformation: Perceived Internet and Social Media Harms in 142 Countries', Oxford Internet Institute, 15 December, https://mediawell.ssrc.org/2020/12/15/global-fears-of-disinformation-perceived-internet-and-social-media-harms-in-142-countries-oxford-internet-institute/

Levush, R. (2019), Government Responses to Disinformation on Social Media Platforms: Argentina, Australia, Canada, China, Denmark, Egypt, European Union, France, Germany, India, Israel, Mexico, Russian Federation, Sweden, United Arab Emirates, United Kingdom, Law Library of Congress, Global Legal Research Directorate, September, https://digitalcommons.unl.edu/scholcom/178/.

Meltzer, J. P., and Kerry, C. F. (2019), 'Cybersecurity and Digital Trade: Getting it Right', 18 September, https://www.brookings.edu/research/cybersecurity-and-digital-trade-getting-it-right/

Morar, D., and Dos Santos, B. M. (2020), 'The Push for Content Moderation Legislation Around the World', 21 September, https://www.brookings.edu/blog/techtank/2020/09/21/the-push-for-content-moderation-legislation-around-the-world/.

National Intelligence Council (2021), 'Global Trends: A More Contested World', https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends2040.pdf

OECD (2016), 'Economic and Social Benefits of Internet Openness', OECD Digital Economy Papers No. 257, Paris, OECD Publishing, www.oecd-ilibrary.org/science-and-technology/economic-and-socialbenefits-of-internet-openness_5jlwqf2r97g5-en.

— (2021), 'Digital Trade Inventory, Pillar 1, Rules Standards and Principles', 14 April, AD/TC/WP(2020)14/FINAL, https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2020)14/FINAL&docLanguage=En

Office of the High Commissioner (2021), 'Freedom of Opinion and Expression—Annual Reports', Office of the High Commissioner for Human Rights, https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx
Rainie, L., and Anderson, J. (2017), 'The Fate of Online Trust in the Next Decade', 10 August, https://www.pewresearch.org/internet/2017/08/10/the-fate-of-online-trust-in-the-next-decade/
Ridley, M. (2011), *The Rational Optimist*, New York, Harper Perennial.
Rose, A. K. (2004). 'Do We Really Know that the WTO Increases Trade?', *American Economic Review*, **94**(1), 98–114.
Roy, D., Munasib, A., and Chen, X. (2014), 'Social Trust and International Trade: The Interplay between Social Trust and Formal Finance', *Review of World Economics*, **150**, 693–714. https://doi.org/10.1007/s10290-014-0197-2
Seabright, P. (2010), *The Company of Strangers: A Natural History of Economic Life*, Princeton, NJ, Princeton University Press.
Shandler, R. (2018), 'Measuring the Political and Social Consequences of Government-initiated Cyber Shutdowns', https://www.usenix.org/system/files/conference/foci18/foci18-paper-shandler.pdf
— Gross, M. L., and Canetti, D. (2019), 'Can You Engage in Political Activity Without Internet Access? The Social Effects of Internet Deprivation', *Political Studies Review*, **18**(4), https://doi.org/10.1177/1478929919877600
Solomon, F. (2020), 'Internet Shutdowns Become a Favorite Tool of Governments: "It's Like We Suddenly Went Blind"', *The Wall Street Journal*, 25 February, https://www.wsj.com/articles/internet-shutdowns-become-a-favorite-tool-of-governments-its-like-we-suddenly-went-blind-11582648765
Subramanian, S., *et al*. (2020), 'Ransoming Government: What State and Local Governments Can Do to Break Free from Ransomware Attacks', Deloitte, 11 March, https://www2.deloitte.com/content/dam/insights/us/articles/6421_Ransoming-government/DI_Ransoming-government.pdf
UN General Assembly (2021), 'Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security', United Nations, General Assembly, A/AC.290/2021/CRP.2, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
UN Human Rights Council (2016), 'The Promotion, Protection and Enjoyment of Human Rights on the Internet', United Nations, Human Rights Council, 27 June, A/HRC/32/L.20.
USITC (2022), 'Foreign Censorship, Part 1: Policies and Practices Affecting US Businesses', February, https://www.usitc.gov/publications/332/pub5244.pdf
Wagner, A. (2012), 'Is Internet Access a Human Right?', *The Guardian*, 11 January.
Weber, R. (2015), 'The Expansion of e-commerce in Asia-Pacific Trade Agreements', September, https://e15initiative.org/blogs/the-expansion-of-e-commerce-in-asia-pacific-trade-agreements/
West, D. M. (2016), *Internet Shutdowns Cost Countries $2.4 Billion Last Year*, Washington, DC, Brookings Institution, www.brookings.edu/research/internetshutdowns-cost-countries-2-4-billion-last-year/.
World Economic Forum (2011), 'Personal Data, the Emergence of a New Asset Class', https://www.weforum.org/reports/personal-data-emergence-new-asset-class/