Listening to Users and Other Ideas for Building Trust in Digital Trade

Susan Ariel Aaronson
Listening to Users and Other Ideas for Building Trust in Digital Trade

Susan Ariel Aaronson
About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people’s lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

Credits

Managing Director of Digital Economy Robert Fay
Program Manager Aya Al Kabarity
Publications Editor Lynn Schellenberg
Senior Publications Editor Jennifer Goyder
Graphic Designer Sami Chouhdary
Table of Contents

vi    About the Author
vi    Acronyms and Abbreviations
1     Executive Summary
1     Introduction
3     What Do Trade Agreements Say and Why Are These Agreements Insufficient to Sustain Trust?
7     Case Studies
10    Some Ideas to Build Trust Among Users, Trade Diplomats and Other Market Actors
12    Works Cited
About the Author

Susan Ariel Aaronson is a CIGI senior fellow. She is an expert in international trade, digital trade, good governance and human rights. Aaronson is particularly interested in and writes on how the digital economy is changing governance and human rights. She is currently writing on comparative advantage in data, comparing how nations govern data, and how virtual reality will challenge our existing approach to governance.

Susan is also research professor of international affairs and cross-disciplinary fellow at George Washington University’s Elliott School of International Affairs, where she directs the Digital Trade and Data Governance Hub. The Hub educates policy makers and the public on domestic and international data governance. The Hub also maps the governance of personal, public and proprietary data around the world to illuminate the state of data governance.

Susan is the former Minerva Chair at the National War College. She is the author of six books and more than 50 scholarly articles. Her work has been funded by major international foundations including the MacArthur, Hewlett, Ford, Koch and Rockefeller Foundations; governments such as the Netherlands, the United States and Canada; international organizations such as the United Nations, International Labour Organization and the World Bank; and US corporations including Google, Ford Motor and Levi Strauss. She loves to do triathlons and study ballet.

Acronyms and Abbreviations

- **DDOS** distributed denial of service
- **DEPA** Digital Economy Partnership Agreement
- **G20** Group of Twenty
- **GATS** General Agreement on Trade in Services
- **GATT** General Agreement on Tariffs and Trade
- **ICT** information communication technology
- **OECD** Organisation for Economic Co-operation and Development
- **RCEP** Regional Comprehensive Economic Partnership
- **UNCITRAL** United Nations Commission on International Trade Law
- **UNGA** United Nations General Assembly
- **USITC** US International Trade Commission
- **USMCA** United States-Mexico-Canada Agreement
- **USTR** Office of the United States Trade Representative
- **WTO** World Trade Organization
Executive Summary

In 2019, then prime minister of Japan Shinzo Abe stated that if the world wanted to achieve the benefits of the data-driven economy, members of the World Trade Organization (WTO) should find common ground on what he called “Data Free Flow with Trust.” However, he never explained how trade policy makers could negotiate a trusted approach to the data flows that underpin both the internet and digital trade. Some two years later, policy makers have negotiated several agreements to facilitate digital trade (which the Organisation for Economic Co-operation and Development [OECD] defines as digitally enabled transactions of trade in goods and services that can either be digitally or physically delivered),1 but they have yet to delineate how such agreements can sustain public trust.

This paper argues that if trade policy makers truly want to achieve data free flow with trust, they must address user concerns beyond privacy. Survey data reveals that users are also anxious about online harassment, malware, censorship and disinformation. The paper focuses on three such problems, specifically, internet shutdowns, censorship and ransomware (a form of malware), each of which can distort trade and make users feel less secure online. Finally, the author concludes that trade policy makers will need to rethink how they involve the broad public in digital trade policy making if they want digital trade agreements to facilitate trust. Trade policy makers should work at the international level to:

→ train citizens in the developing world to recognize and thwart online harms;

→ convene an international conference to develop shared and internationally accepted strategies to protect personal data, thwart cross-border spam and malware, and protect consumer welfare; and

→ challenge internet shutdowns through a trade dispute and in so doing learn how to limit the international spillovers of such shutdowns.

At the national level, trade policy makers should:

→ incentivize public participation in digital trade policy making through multiple means such as town halls and online portals;

→ create an internet users’ advisory committee and regularly consult the committee, which should have access to, and the ability to inform, trade-negotiating documents and processes; and

→ show they are responsive and accountable by delineating how they heard and utilized public comments.

Trade policy makers cannot say they care about trust but then remain oblivious to the concerns of users. There can be no free flow of data without trust.

Introduction

Trust is essential to the online economy. When we go online, download an app, buy a sweatshirt or peruse TikTok, we are taking a leap of faith. We trust that the firms delivering these services will not only provide us with goods and services but also protect our personal data and do their best to ensure we are not harmed by our online activities. As political theorist Francis Fukuyama (1996, 24) has written, “Trust is the expectation that arises within a community of regular, honest, and cooperative behavior, based on commonly shared norms, on the part of other members of that community.” 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. Trust is important for the success of a wide range of public policies that depend on behavioural responses from the public,” leading to broader compliance and faith in regulatory systems.2 In short, trust is essential to democratic capitalist functioning, both online and off.

However, the internet was not designed to sustain our trust. Today, users are troubled by a wide range of threats including hacks, cyber theft, ransomware, online harassment and other vulnerabilities. These threats are constant and

---

1 See www.oecd.org/trade/topics/digital-trade/.

bedevil even the most computer-savvy. As an example, in July 2021, newspapers around the world reported on how democracies and illiberal regimes alike used spyware to target “journalists, human rights defenders or political dissidents seeking safety abroad” (Amnesty International 2021; see also Willsher 2021). In the wake of these threats, the World Wide Web has become a network of insecurity (Timberg 2015; Emmitt 2020).

The online community is still trying to figure out how to sustain user trust given both these rapidly multiplying threats and data-driven change. According to researchers at the Pew Research Center, “the rise of the internet and social media has enabled entirely new kinds of relationships and communities in which 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 used by actors employing ever-proliferating strategies to capture users’ attention” (Rainie and Anderson 2017).

Our shared failure to sustain trust online is troubling because users are increasingly dependent on the internet and, in particular, on new data-driven services since the onset of the global pandemic. These services, such as Zoom and Netflix, allowed many of us — although not all — to connect, work, study and, essentially, prosper online (Internet Society 2020; Anderson, Rainie and Vogels 2021). Yet because many of these services are built on the collection, analysis and monetization of personal data, they also threaten our autonomy, individual rights and systems of governance (Aaronson 2018; United Nations General Assembly [UNGA] 2021b). The situation has gotten so bad that the United States’ National Intelligence Council warned that in the future “privacy and anonymity may effectively disappear by choice or government mandate, as all aspects of personal and professional lives are tracked by global networks. 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, 63).

In sum, the many benefits of the internet are counterbalanced by the plethora of risks that affect online trust. In 2019, researchers at the Pew Research Center found that many people fear that their data is being used without their consent and are concerned that firms might use their clients’ personal data to discriminate and manipulate them (Auxier et al. 2019).

In fact, the Centre for International Governance Innovation (CIGI) and Ipsos have conducted large international user surveys since 2014 and, in 2019, they found that 75 percent of 25,000 users polled cited Facebook, Twitter and other social media platforms as contributing to their lack of trust (CIGI and Ipsos 2019, 116). Among those surveyed, 78 percent were concerned about their online privacy, with more than half (53 percent) more concerned than they had been the previous year (ibid., 8, 10). Moreover, 40 percent reported taking greater care to secure their devices, and 39 percent said they were using the internet more selectively, among other precautions (ibid., 137).

Further, the Oxford Internet Institute analyzed 2019 World Risk Poll data from 154,195 participants living in 142 countries and found that among those active online, 53 percent were concerned about disinformation, and 71 percent were worried about a mixture of online threats, including disinformation, fraud, malware, spyware and harassment (Knuutila, Neudert and Howard 2020).

In 2019, then prime minister Abe proposed a framework that might address public insecurity about the online world. He wanted the Group of Twenty (G20) meeting in Japan “to be long remembered as the summit that started worldwide data governance…under the roof of the WTO” (Abe 2019). He noted that many internet services are built on data collected from individuals in one country and stored or analyzed in another. Hence, he proposed that the members of the WTO (the only global international organization dealing with the rules of trade between 164 nations3) find a common approach to what he called “Data Free Flow with Trust.” Abe suggested that countries should allow “medical, industrial, traffic and other most useful, non-personal, anonymous 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” (ibid.).

Although Abe argued that certain types of data needed special rules to facilitate trust, he never explained what these rules should look like or how nations might find an internationally accepted approach to developing them. Nonetheless,

---

3 See www.wto.org/english/thewto_e/whatis_e/whatis_e.htm.
in the years that followed, other international organizations have reiterated his call for “free flow with trust,” including the Digital Economy Task Force of the G20, representing the world’s 20 largest economies (OECD 2020); the OECD (2021b); the World Economic Forum (2021); and, most recently, the Group of Seven, representing the world’s seven largest so-called advanced economies. But their pretty words have not led to real change. Although policy makers have negotiated several agreements that discuss cross-border data flows, and some mention trust, they do not really address concerns that may undermine trust.

Policy makers have long paid close attention to the needs of importers and exporters, but if they want to build trust in digital trade they must also pay closer attention to users’ concerns. After all, as the OECD notes, “government’s competence — its responsiveness and reliability in delivering public services and anticipating new needs — are crucial for boosting trust in institutions.” Hence, how policy makers respond — their approach to being responsive, responsible and accountable — is as important as what they put forward during the process of negotiating internationally accepted rules to govern data.

This paper will focus on three concerns identified by users that impede trust online — internet shutdowns, censorship, and ransomware (a form of malware or malicious data flows). The author chose these concerns for three reasons. First, internet shutdowns, censorship and ransomware seem to be increasing in visibility and frequency. As an example, Google’s Jigsaw project teamed up with the digital rights non-profit Access Now and the censorship measurement company Censored Planet to study internet shutdowns, and found that they are growing “exponentially.” They noted that of nearly 850 shutdowns documented over the last 10 years, some 90 percent (768) have occurred since 2016 (Ryan-Mosely 2021). Second, the public is concerned about these issues: the Internet Society surveyed 20,000 internet users in the United States and the United Kingdom, and found that more than 65 percent identified accessibility and reliability as the most important aspects of the internet (Internet Society 2020). Censorship, internet shutdowns and ransomware forestall access and impede reliability. Third, all three affect market access for users and producers of data-driven services. Hence, they are not only issues impeding trust, but also “trade issues” (Huang, Madnick and Johnson 2019; Meltzer and Kerry 2019). However, the trade regime may not be the only or the best venue to address them.

This paper proceeds as follows: first, the author looks at what trade agreements say about trust and why current strategies cannot meet the goal of building trust. She then uses the case studies to describe how censorship, internet shutdowns and ransomware affect both trade and trust. The paper concludes with some ideas on how to actually achieve the goal of “Data Free Flow with Trust.”

What Do Trade Agreements Say and Why Are These Agreements Insufficient 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 (Ridley 2011; Seabright 2010). Researchers believe that the concept of trust emerged in society when individuals began to believe that other people would follow the rules or else experience shame and other forms of societal punishment (Anomaly 2017).

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 (ibid.). 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
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce domestic laws regarding privacy?</td>
<td>Yes (Article 14.8: Personal Information Protection)</td>
<td>Yes (Article 15: Personal Information Protection)</td>
<td>Yes (Article 19.8: Personal Information Protection)</td>
<td>Yes (Article 4.2: Personal Information Protection)</td>
<td>Yes (Article 17: Personal Information Protection)</td>
<td>Yes (Article DIGIT.7: Protection of personal data and privacy)</td>
<td>No. Adopt or maintain laws. (Article 9: Online Personal Data Protection)</td>
</tr>
<tr>
<td>Include regulations banning divulgence of encryption?</td>
<td>No</td>
<td>Yes (Article 2: Information and Communication Technology Goods that Use Cryptology)</td>
<td>No</td>
<td>Yes (Article 3.4: Information and Communication Technology Products that Use Cryptography)</td>
<td>Yes (Article 7: Information and Communication Technology Products that Use Cryptography)</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Source: Andrew Kraskewicz with Susan Ariel Aaronson.

supposed to create a virtuous circle between trust and trade (Roy, Munasib and Chen 2014; Rose 2004).

However, policy makers have not thought creatively about how to build trust in digital trade agreements. Table 1 considers seven recent trade agreements and some of their similarities and differences. Six of these agreements are in effect; one, the Regional Comprehensive Economic Partnership (RCEP), an agreement among 15 Indo-Pacific nations, will likely come into effect by the end of the year. Of the seven agreements, only four briefly mention trust. But none of these agreements clearly delineate how the signatories will use trade policies to address the concerns of users about the free flow of data across borders and, in so doing, build trust.

Several agreements, including the United States-Mexico-Canada Agreement (USMCA), the Digital Economy Partnership Agreement (DEPA) between Singapore, Chile and New Zealand, and the Digital Economy Agreement between Australia and Singapore, say most types of data should flow freely across borders. Moreover, these provisions are binding and disputable. Signatories can initiate a trade dispute to challenge barriers to the free flow of data, even when another signatory tries to justify such barriers as necessary to achieve legitimate domestic public policy objectives such as protecting national security, social stability, public health or privacy (the exceptions under the General Agreement on Tariffs and Trade [GATT] and the General Agreement on Trade in Services [GATS]). However, under 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, because these provisions are not subject to dispute settlement. Instead, RCEP recommends that they solve these differences through good faith efforts and consultation.9

The EU model is different. EU agreements such as the European Union-United Kingdom 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 those few nations that the European Union deems to be adequate or that have adopted what the European Union deems an acceptable data protection regime.10

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 toward 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.”11 Taken in sum, these provisions suggest to users and trade diplomats that the trade regime is not the right place to foster interoperability or regulatory coherence.

Finally, these agreements generally ban only two practices that may undermine trust among online market actors (see Table 2). All seven prohibit requirements that data be stored in local servers. RCEP states that “the Parties recognise 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.12 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. Yet there are few shared

---

8 See www.dfat.gov.au/trade/agreements/not-yet-in-force/rccep and Zhang (2021). The signatories include the members of the Association of Southeast Asian Nations — Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam — and trading partners Australia, China, Japan, Korea and New Zealand.


11 Ibid., art. 4, Cooperation, Electronic Commerce Chapter, pp. 2–3.

12 Ibid., art. 15, 16.
Table 2: Overview of Recent Digital Trade Agreements

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Language explicitly encouraging cross-border data?</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes, but self-judging and subject to disputes (Articles 16.3 and 17.3)</td>
</tr>
<tr>
<td>GATT/GATS exceptions?</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Bans on performance requirements, e.g., sharing source code and/or algorithms?</td>
<td>Yes, source code only (Article 14.17: Source Code)</td>
<td>Yes (Article 17: Source Code)</td>
<td>Yes (Article 19.16: Source Code)</td>
<td>Yes (Article 3.4: Information and Communication Technology Products that Use Cryptography)</td>
<td>Yes (Article 28: Source Code; Article 28.4: Algorithms)</td>
<td>Yes, source code only (Article DIGIT.12: Transfer of or access to source code)</td>
<td>No</td>
</tr>
<tr>
<td>Regulations banning divulgence of encryption?</td>
<td>No</td>
<td>Yes (Article 21: Information and Communication Technology Goods that Use Cryptography)</td>
<td>No</td>
<td>Yes (Article 3.4: Information and Communication Technology Products that Use Cryptography)</td>
<td>Yes (Article 7: Information and Communication Technology Products that Use Cryptography)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Language encouraging development of cybersecurity abilities?</td>
<td>Yes (Article 14.16: Cooperation on Cybersecurity Matters)</td>
<td>Yes (Article 19: Cybersecurity)</td>
<td>Yes (Article 19.15: Cybersecurity)</td>
<td>Yes (Article 5.1: Cybersecurity Cooperation)</td>
<td>Yes (Article 34: Cybersecurity)</td>
<td>Yes (Articles CYB.1–CYB.5)</td>
<td>Yes, use existing mechanisms (Article 14)</td>
</tr>
</tbody>
</table>

Source: Andrew Kraskewicz with Susan Ariel Aaronson.
Notes: See Table 1 notes for full names of agreements and URLs.
norms, and trade disputes are just beginning to provide insights into how nations should behave when rules governing data flows conflict with the achievement of domestic policy objectives. Without such guidance, nations will continue to rely on the exceptions, and they risk becoming the rule.

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 online.

Third, most trade agreements include vague aspirational language on cybersecurity. According to the OECD, which has done an inventory of such provisions, these provisions are aspirational and 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 cybersecurity (without specifying what these mechanisms might be) (OECD 2021a, 21). The USMCA (art. 19.15.2) 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.

Finally, the agreements ban practices that many executives from big tech firms see as trade-distorting. However, these agreements do not address other issues such as censorship, internet shutdowns, or ransomware or distributed denial of service (DDOS) attacks that can make both users and executives from such firms feel less secure online. The next section describes how these issues could undermine both trade and trust.

---

**Case Studies**

**Internet Shutdowns and Censorship**

Internet shutdowns have become a frequent online occurrence. Many countries routinely restrict the internet (China and Iran, for example) while others use protests, elections, national exams or other events to justify shutting off the internet (Belarus, Cuba, Ethiopia, India and so forth). While most countries doing blanket shutdowns are authoritarian states, leaders in some democratic states, including the United States, India (Phartiyal 2021) and Brazil (Conger 2016), 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.

The digital rights group Access Now defines internet shutdowns as an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information. According to a 2020 analysis by The Wall Street Journal, firms such as AT&T, Telenor and Vodafone that provide internet access often must get government approval through contracts to provide such services (Solomon 2020). These contracts forbid executives from such firms from delineating when or why such shutdowns occurred. 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 (ibid.).

Full and even partial internet shutdowns directly affect users. They undermine access to information and, because so many activities are now solely online, make it almost impossible for users to express their opinions or participate politically (OECD 2016; Aaronson 2018). As a result of these

---

13 See [https://netblocks.org/reports](https://netblocks.org/reports).

14 The Trump administration tried to ban two Chinese-owned apps for alleged national security reasons (Clayton 2020), but the courts did not uphold the bans and President Joe Biden’s administration has abandoned this plan (Ferguson 2021).

shutdowns, some 268 million people in 2020 were unable to access the internet at various times; some 42 percent of shutdowns in 2020 were associated with additional human rights abuses: among these, 29 percent were associated with restrictions on freedom of assembly, 15 percent were associated with election interference and 12 percent were associated with infringements on freedom of the press. Not surprisingly, these shutdowns can undermine trust in government as well as in providers of internet services (Shandler 2018; Shandler, Gross and Canetti 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). But internet shutdowns also have larger spillovers. When national officials place limitations on which firms can participate in the network, they reduce its overall size and generativity. Moreover, such shutdowns increase costs to local businesses, affect global value chains and reduce technology diffusion, thereby undermining development and trade (Box 2016, 2).

While internet shutdowns appear to raise costs to companies and users, these costs are hard to quantify. In 2016, Darrell West of Brookings estimated that internet shutdowns cost the global economy US$2.4 billion (West 2016). In 2019, researchers found some 21 countries shut down the internet within their boundaries and these shutdowns cost their economies US$8.05 billion. However, another group estimated that such shutdowns cost US$4 billion in lost revenue in 2020 (Woodhams and Migliano 2021).

When utilizing such shutdowns, 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.Shutdowns may also reduce internet stability and diminish the predictability of data flows (Box 2016; OECD 2016).

Essentially, shutdowns export these negative effects to other markets (Aaronson 2018).

In addition, internet shutdowns are a form of censorship, directly affecting a wide range of users and providers online. Yet internet shutdowns are different from censorship, because shutdowns do not discriminate regarding content; instead, they block all content. Internet shutdowns also encompass all forms of digital communication, from email to social networks. They typically also directly affect mobile phone services. Finally, internet shutdowns are not aimed at one piece of content but rather on the act of communication (Wagner 2018, 3920–21).

In studying internet shutdowns and censorship, researchers can directly see the plethora of effects on users both within a country and beyond its borders (Wagner 2018; Hsu 2020). These actions are not rare. The Open Observatory of Network Interference has compiled a complete data set of these actions at the country level. In examining these shutdowns, the Internet Society stressed that intentional physical damage to infrastructure, such as cutting fibre-optic cables, is probably the most extreme method of implementing an internet shutdown. But internet shutdowns can also affect the Domain Name System servers. Finally, if internet shutdowns are used as a blunt-force means of blocking access locally to a specific service or application, access to other unrelated services may also be impacted as collateral damage (Internet Society 2019).

The Internet Society noted internet shutdowns “undermine users’ trust in the Internet, setting in motion a whole range of consequences for the local economy, the reliability of critical online government services, and even for the reputation of the country itself” (ibid., 2).

According to the Internet Society, governments must apply their national legislation to cross-border platform firms: “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” (ibid., 6). In short, the failure to address this problem globally could lead governments to more drastic solutions.

---

16 Samuel Woodhams and Simon Migliano (2021) used NetBlocks Cost of Shutdown Tool (https://netblocks.org/projects/cost) to estimate these costs.


18 See https://explorer.ooni.org/.
Despite these systemic effects on the internet as a whole, no trade agreement says anything about internet shutdowns. Moreover, trade diplomats have never challenged shutdowns or censorship in a trade dispute. The United States (and, for a time, the European Union) has flirted with the idea of examining censorship as a trade barrier (Aaronson 2017).

However, in 2020, the US Senate Finance Committee requested that the US International Trade Commission (USITC) examine whether censorship is a barrier to trade, thereby making the United States the first nation to seek both qualitative and quantitative evidence of such costs. The requestors defined censorship broadly as “the prohibition or suppression of speech or other forms of communication” (cited in Barton 2021, 2) 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. The USITC’s study is designed to identify and describe various foreign censorship practices, in particular those that impede trade or investment in key foreign markets (Barton 2021). As paraphrased, the description of these practices should include the evolution of censorship policies and practices over the past five years in key foreign markets; any elements that entail extraterritorial censorship; and the roles of governmental and non-governmental actors in implementation and enforcement of censorship (ibid.).

By rooting out the direct trade implications, the USITC study could inspire other nations to similarly examine, and work to find common ground on, the barriers ranging from censorship to DDoS attacks that impede both market access and human rights.

A Most Dangerous Form of Malware: Ransomware

It is a vicious world online. In 2020, the White House noted that America’s personal data remained at risk because there were 30,819 information security incidents across the federal government — an eight percent increase from 2019 (US Senate Committee on Homeland Security and Governmental Affairs 2021b, ii–iii). Statistics Canada (2020) reported that in 2019 one-fifth (21 percent) of Canadian businesses had been impacted by cybersecurity incidents, which was the same proportion as in 2017. The United Kingdom experienced a 31 percent increase in cybercrime from May to June 2020, a trend replicated globally (Security Magazine 2020).

According to the consulting firm Accenture’s Cyber Investigations, Forensics & Response mid-year update, the volume of cyber intrusion activity increased 125 percent in the first half of 2021 compared with the same period in 2020 (cited in Shein 2021). The company blamed the increase on web shell activity, which is the use of small pieces of malicious code to gain remote access and control, targeted ransomware and extortion operations and supply chain intrusions (ibid.).

Ransomware has become one of the most dangerous online threats. Bad actors can use ransomware to steal data and credentials or even to wipe data (Runnegar 2017). According to SonicWall, 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 percent year-to-date increase (Help Net Security 2021). The cybersecurity firm Emsisoft estimated that Canada had experienced more than 4,000 ransomware incidents in 2020 — with a minimum ransom cost estimate of US$164,772,274 and a maximum estimate of US$659,246,267. When factoring in the added cost of downtime due to ransomware attacks, those numbers jump to a minimum downtime and ransom cost estimate of US$1,011,008,551 and a maximum estimate of US$4,044,034,203 (Emsisoft Malware Lab 2021). Members of the US Senate Committee on Homeland Security and Governmental Affairs (2021a) are so concerned about this threat that they plan to investigate the rise in ransomware.

Ransomware is just one of many different types of malware. Malware is widely available for sale on the dark web, and can infect almost any type of internet device (Mikalauskas 2020). Firms can purchase malware to test their cyber defences, but much of the malware produced appears to be for malign purposes as outlined above (OECD 2009, 5).

In the wake of the rise in numbers of malware attacks and other online threats, most countries have adopted cybersecurity strategies. These strategies serve to define threats and illuminate how government is responding. The International Telecommunication Union found that more than
100 countries have cybersecurity strategies, not including those with strategies in draft.19

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. China provides a good example. During a routine discussion about trade barriers at the WTO, the European Union, the United States, Japan, Canada and Australia asked China to define the scope of its cybersecurity regulations and clarify the definitions of key terms such as “secure and controllable services and products” that are covered by the draft law. While members acknowledged the importance of safeguarding against “network intrusions” and “cyber-attacks,” as well as of protecting users’ personal information and sensitive data, they urged China to implement relevant measures in a non-discriminatory manner and in line with the Technical Barriers to Trade Agreement.20

Malware is not just a trade problem; like internet shutdowns, it can affect internet openness and generativity (OECD 2016). 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” (UNGA 2021a, para. 5). It also notes that “States concluded that threats may be experienced differently by States according to their levels of digitalization, capacity, ICT [information communication technology] 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” (ibid., paras 21–22). But the document is vague as to what states should do about addressing these threats beyond creating norms for state actions.

Bad actors use ransomware to take advantage of user and firm laziness — their failures to install patches on time, use updated infrastructure or hire the most effective cyber defenders. Government bodies are particularly vulnerable to ransomware, which can kick-start a vicious cycle. According to a report from the Deloitte Center for Government Insights, 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, 3). The cost is not just in funds but in trust of government and trust online.

Some Ideas to Build Trust Among Users, Trade Diplomats and Other Market Actors

Taken in sum, our shared failure to secure both the internet and the data that underpins it has put individuals,21 groups, firms, democracy and even national security at risk (Aaronson 2020). Hence, trade policy makers cannot argue that they are enabling free flows of data with trust without addressing these types of concerns. Moreover, if policy makers could develop a coordinated and effective international approach, they might diminish the economic and human costs of these problems. A recent study found that unilateral data regulations can either raise or reduce global welfare, but a coordinated approach would yield substantial gains (Chen, Hua and Maskus 2020, 4).

---

19 See www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.
Here are some ideas that policy makers could adopt to place trust (and user needs) at the heart of all trade agreements:

→ **Incentivize cybersecurity through societal understanding.** Public and private development donors should incentivize cybersecurity by requiring their development recipients to educate users on how to work safely online. Nations have developed free tools that can be helpful, such as Europe’s No More Ransom tool.22

→ **Address the concerns of users and foster international cooperation.** An international conference should be convened to develop internationally accepted strategies to protect personal data, thwart cross-border spam and malware, and protect consumer welfare. WTO members should encourage the United Nations Commission on International Trade Law (UNCITRAL) to create model laws finding such common ground.23

→ **Challenge internet shutdowns as a barrier to trade.** Nations can use the exceptions to justify such shutdowns, but democracies should challenge the use of blanket shutdowns as a barrier to trade in a trade dispute. Such a dispute could provide guidance as to whether such shutdowns are overly broad and how nations could limit their effects on other market actors.

In addition, at both the national and the international level, policy makers should expand the universe of who they listen to when they make digital trade policies (the feedback loop).

Most democracies ask for public comment on their trade policies (Aaronson and Zimmerman 2007; Inter-American Development Bank 2002; Ilott, Stelk and Rutter 2017). For example, the Office of the United States Trade Representative (USTR) solicited public comment regarding whether the United States should retaliate against governments imposing digital taxes.24 Canada recently asked its citizens to comment as to whether it should join the Digital Economy Partnership.25 Australia created a discussion paper and asked citizens to comment on the future of digital trade rules.26 Clearly, government officials understand that trust in government officials (political efficacy) is positively correlated with public engagement and participation.27

However, none of these countries provided evidence that they heard their citizens’ concerns and made changes in response to these concerns. Thus, countries should:

→ Create a portal and consistently ask for public comment. Incentivize stakeholder involvement through town halls, in speeches, and so forth. Trade leaders in the legislative and executive branch should highlight the importance of public comment.

→ Create an internet users’ advisory committee comprised of academics, internet civil society groups, internet activists and local government officials to discuss how digital trade rules may affect users and the internet as a whole. Trade policy makers should regularly consult the committee, which should have access to, and the ability to inform, trade-negotiating documents and processes.

→ In their annual report, trade-related agencies should delineate who provided public comment and how these comments were utilized.

Trade policy makers cannot say they care about trust but remain oblivious to the concerns of users. There can be no free flow of data without such user trust.

---


23 Established in 1966, UNCITRAL works toward the progressive harmonization and modernization of the law of international trade by preparing and promoting the use and adoption of legislative and non-legislative instruments in a number of key areas of commercial law.


Works Cited


