Centre for International
Governance Innovation

CIGI Papers No. 255 — July 2021

Could Trade Agreements Help Address the Wicked Problem of Cross-Border Disinformation?

Susan Ariel Aaronson

Centre for International
Governance Innovation

CIGI Papers No. 255 — July 2021

Could Trade Agreements Help Address the Wicked Problem of Cross-Border Disinformation?

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.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director of Digital Economy Robert Fay
Program Manager Aya Al Kabarity
Publications Editor Susan Bubak
Publications Editor Lynn Schellenberg
Graphic Designer Sami Chouhdary

For publications enquiries, please contact publications@cigionline.org.

Printed in Canada on Forest Stewardship Council® certified paper containing 100% post-consumer fibre.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Author

Susan Ariel Aaronson is a CIGI senior fellow. She is an expert in international trade, digital trade, corruption and good governance, and human rights. She is currently writing an overview of data governance, including how to build trust with trade agreements, and working on the economics of data markets.

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 40 scholarly articles. Her work has been funded by major international foundations including the MacArthur, Hewlett, Ford 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.

Acronyms and Abbreviations

AI	artificial intelligence
COVID-19	coronavirus disease 2019
CUSMA	Canada-United States-Mexico Agreement
DARPA	Defense Advanced Research Projects Agency
DEPA	Digital Economy Partnership Agreement
FTAs	free trade agreements
G7	Group of Seven
GATS	General Agreement on Trade in Services
GATT	General Agreement on Tariffs and Trade
GDI	Global Disinformation Index
NetzDG	Network Enforcement Act
OECD	Organisation for Economic Co-operation and Development
SADEA	Singapore-Australia Digital Economy Agreement
SAFTA	Singapore-Australia Free Trade Agreement
UNCITRAL	United Nations Commission on International Trade Law
WHO	World Health Organization
WTO	World Trade Organization

Executive Summary

Disinformation is simultaneously a domestic and an international problem. It can be created and disseminated by domestic actors, or it can be created and transferred from individuals in one group or country to another. Moreover, because of its global and continuous nature, disinformation is a "wicked problem" that transcends nations and generations. Wicked problems cannot be "solved," but they can be mitigated.

Herein the author argues that trade agreements might help governments deal with cross-border disinformation (but they cannot address the problem of domestically created disinformation). Trade agreements cannot stop individuals, groups or governments from disseminating malicious or dangerous cross-border disinformation flows, but they can provide tools for mitigating such flows.

Policy makers should enhance trade agreement rules to govern disinformation and foster international cooperation by taking the following steps:

- Prod the United Nations Commission on International Trade Law (UNCITRAL)[1] to create a model law defining cross-border disinformation and delineating how to attribute such disinformation. Such a law should include provisions requiring platforms and media outlets to delineate how they protect users from disinformation. It should also include language banning private firms from producing and exporting disinformation as a service.
- Building on this model law, supplement trade agreement provisions on spam to include language covering cross-border disinformation and requiring signatories to enforce their own laws related to cross-border disinformation. Note that disinformation is often promoted by spambots across borders.
- Add language to trade agreements requiring signatories to develop national laws banning the use of spambots to disseminate disinformation across borders and requiring firms to ensure that users attempting to disseminate information across borders are human (through verification).
- Add language to trade agreements requiring nations to enforce their laws on the use of spambots and develop a transparent process to identify nations using spambots to disseminate disinformation.
- Clarify that nations can use the exceptions to justify breaching trade agreement rules and cross-border data flows to address disinformation. The language should provide guidance that trade agreement signatories can use trade or financial sanctions to punish entities and/or governments that disseminate disinformation across borders. However, nations must establish a transparent and public process of evidence gathering and attribution before they sanction.

Introduction

Disinformation is not like pornography; most of us do not know it when we see it.[2] While there is some disagreement on an exact definition, disinformation can be defined as information designed to mislead, deceive or polarize (Nemr and Gangware 2019). Moreover, unlike pornography, disinformation is dangerous to individuals, democracy and good governance.

An international network of users, firms and policy makers often perpetuates disinformation. Netizens around the world turn to Facebook, Google, WeChat and other sites, apps and browsers for information and increasingly for their news.[3] Many of these sites, apps and

1 UNCITRAL is the core legal body of the UN system in the field of international trade law. See https://uncitral.un.org/en/content/homepage.

2 In 1964, US Supreme Court Justice Potter Stewart tried to explain "hard-core" pornography: "I shall not today attempt further to define the kinds of material I understand to be embraced…[b]ut I know it when I see it." See https://corporate.findlaw.com/litigation-disputes/movie-day-at-the-supreme-court-or-i-know-it-when-i-see-it-a.html.

3 As an example, in 2018, some 40 percent of Facebook users got their news from the platform. See www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/.

browsers provide their services to netizens for free. Hence, these firms depend on ads for revenues and profits. After users provide personal data (such as their interests or search history), these firms aggregate it and use it to provide users with both tailored advertising and free content (Amnesty International 2019; Zuboff 2021).

Critics accuse many of these platforms of feeding their users divisive content to gain their attention and increase their time on the platform, which in turn encourages more advertisers (Ghosh et al. 2020). Meanwhile, these ads provide a global revenue stream that both incentivizes and sustains the spread of disinformation within countries and across borders. As an example, the Global Disinformation Index (GDI)[4] found that local ads for Bosch, the World Health Organization (WHO) and *The Wall Street Journal*, delivered by Google and Amazon, appeared on sites spreading anti-Semitic narratives and globalism conspiracy theories.[5] The GDI also found that ads promoting the American Cancer Society, the United Nations International Children's Emergency Fund and Doctors Without Borders appeared on sites with disinformation about the coronavirus disease 2019 (COVID-19).[6] *The Washington Post* (2021) argued in a February 2021 editorial, "Platforms have no excuse not to do something about the problem. They've already showed us they know how." But these companies are reluctant to change their business model because it is so profitable (Wakabayashi et al. 2020; Rossolillo 2021).

Individuals, organizations and governments have spread propaganda, fake news and conspiracy theories offline for centuries (Wardle and Derakhshan 2017). However, as life has moved online, so too has disinformation, flowing within and across borders (Vigneault 2021). As a result, the global internet has become both an information platform and a "battlefield" (Weaver 2013). According to scholar Shoshana Zuboff (2021), advertisers use this data to manipulate us to think, buy, believe, do or join something that we otherwise would not have done (Angwin 2021).

Disinformation is simultaneously a domestic and an international problem (Ewing 2020). It can be created and disseminated by domestic actors, or it can be created and transferred from individuals in one group or country to another. There are no reliable statistics, but one can see mounting qualitative evidence that disinformation increasingly crosses borders (Nemr and Gangware 2019; Office of the High Commissioner for Human Rights 2021).

Because of its global and continuous nature, disinformation is a "wicked problem" that transcends nations and generations. Wicked problems cannot be "solved," but they can be mitigated (Barclay 2018; Montgomery 2020). According to Brian Pierce (n.d.), former director of the Information Innovation Office at the Defense Advanced Research Projects Agency (DARPA), "wicked problems are typical of open, nonlinear systems that involve people and machines."[7] No one knows how best to counter disinformation at the local, national or international levels (Tucker et al. 2018).

Not surprisingly, people are worried about disinformation. A 2018 poll by BBC News in 18 countries found that 79 percent of respondents were worried about what was fake and what was real on the internet (Cellan-Jones 2017). The Centre for International Governance Innovation (CIGI) surveyed some 20,000 netizens around the world and, in 2019, found that social media companies were the leading source of user distrust in the internet — surpassed only by cybercriminals — with 75 percent of those surveyed citing Facebook, Twitter and other social media platforms as contributing to their lack of trust.[8] In a December 2020 study, the Oxford Internet Institute analyzed survey data from 154,195 participants living in 142 countries and found that more than half (53 percent) of regular internet users were concerned about disinformation (Knuutila, Neudert and Howard 2020). The researchers also found

4 The GDI is a non-profit organization that evaluates and rates websites' risk of spreading disinformation.

5 See https://disinformationindex.org/wp-content/uploads/2020/10/Oct-2nd-DisinfoAds-Brands-next-to-Anti-SemitismGlobalist-Conspiracy-theories.pdf.

6 See https://disinformationindex.org/wp-content/uploads/2020/12/Dec_4_2020-DisinfoAds-NGO-_-Charities-Disinformation-1.pdf.

7 Cognitive security is the application of artificial intelligence (AI) technologies patterned on human thought processes to detect threats and protect physical and digital systems.

8 See www.cigionline.org/cigi-ipsos-global-survey-internet-security-and-trust. The 2019 CIGI-Ipsos Global Survey on Internet Security and Trust was conducted between December 21, 2018, and February 10, 2019, and involved 25,229 internet users in Australia, Brazil, Canada, China, Egypt, France, Germany, Great Britain, Hong Kong (China), India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, Republic of Korea, Russia, South Africa, Sweden, Tunisia, Turkey and the United States.

that worries about the impact of disinformation were highest in North America and Europe and lowest in East and South Asia (ibid.).

Consequently, many nations have adopted a wide range of strategies to mitigate disinformation, including platform regulation, data regulation, competition policies, investment rules, technological fixes and citizen education strategies, among others. With so many different approaches, policy makers are able to achieve a clearer understanding of what works and what does not. However, this patchwork may not be effective in mitigating cross-border disinformation. Moreover, the lack of coherent approaches could also lead to trade distortions and spillover effects on internet openness and generativity (Organisation for Economic Co-operation and Development [OECD] 2016; World Economic Forum 2020). There is growing evidence that the data giants have acted at the national level to weaken and contest domestic regulations aimed at addressing disinformation. These firms may be trying to game the system (European Commission 2020; Petre, Duffy and Hund 2019).

Herein the author argues that trade agreements might help governments deal with cross-border disinformation (but they cannot address the problem of domestically created disinformation). Trade agreements cannot stop individuals, groups or governments from disseminating malicious or dangerous cross-border disinformation flows, but they can provide tools for mitigating such flows. When a netizen uses a dating app, searches for information on COVID-19 or watches a movie on Netflix, they are engaging in international trade. To provide the user with this data, firms often use servers located across different countries to improve access speed and reduce network traffic. Moreover, with the adoption of cloud computing (computing as a service), data may be stored and analyzed in many countries simultaneously. In recent years, trade diplomats have included rules to govern these cross-border data flows in a growing number of trade agreements.

However, trade agreements have their limitations in addressing cross-border disinformation. Policy makers cannot use trade agreements to directly regulate the business model that underpins the problem of disinformation. Meanwhile, trade liberalization and trade agreements such as those created by the World Trade Organization (WTO) are not well liked or well understood. Many people believe that these agreements are negotiated in an opaque process that is indirectly democratic, time consuming and out of sync with the digital economy (Kilic 2021; Epps 2008). As an example, members of the WTO for years have participated in a work program to delineate what they should negotiate to govern e-commerce goods and services delivered online through cross-border data flows. After talking about what they should talk about for years, in 2019, some 76 (now 84) nations agreed to actual negotiations. But members are divided by their understanding, capacity and willingness to set rules governing data. Many of the participating nations see the digital economy as deeply distorted because firms from two nations (China and the United States) dominate and are home to the main firms relying on this business model (Aaronson and Struett 2020; Aaronson 2019). Given this market dominance, many nations want to establish their own digital sectors and develop rules before they commit to negotiations (Aaronson and Struett 2020).

But this is where trade agreements may be helpful. Many recent trade agreements contain language designed to build trust online among users and the firms that provide information and infrastructure online. As an example, most trade agreements include provisions that require signatories to enforce domestic laws related to malicious data flows such as spam. Spam and disinformation have a lot in common. Both can be defined as unsolicited commercial electronic communications sent in bulk to recipients, often across borders.

Moreover, trade agreements include useful language on competition policy, as well as provisions designed to ensure that national regulation does not lead to trade distortions. Policy makers include these provisions in the hopes of facilitating regulatory coordination and preventing a race to the bottom on regulation (Smeets 2021, 160, 168). In short, with some refinements, these agreements can help nations coordinate counterweights for cross-border disinformation flows, including data protection rules, content moderation and competition policies.

The paper proceeds as follows: First, the author defines disinformation and illuminates how technological change and market forces are facilitating its spread. Then, the author shows how the business model challenges regulators at the national level. Next, the author discusses what trade agreements say about data flows,

exceptions, competition policy, regulatory coherence and spam. Finally, the author presents suggestions for a broader approach to govern cross-border information that nations can use within trade agreements.[9]

Moreover, the author notes that disinformation is one of several negative spillovers of a global internet built on cross-border data flows shared by governments, firms, civil society and individuals. Policy makers should be anticipating such problems and working toward a twenty-first-century model to govern these spillover effects. One could describe such efforts as an updated approach to "embedded liberalism" (Ruggie 1982, 392; Yakovleva 2020).

What Is Disinformation and How Does It Affect the Global Economy?

Researchers traditionally defined disinformation as the purposeful dissemination of information designed to mislead, deceive, harm and/or polarize people within a country or among countries. It is not the same as misinformation, which is generally understood as the inadvertent sharing of false information that is not intended to cause harm (Derakhshan and Wardle 2018). Governments tend to have similar definitions. The European Union defines disinformation as "false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm" (European Commission 2020). The Government of Canada (2021b) describes it as information that is "false, misleading and inflammatory." In 2021, the Technology and Social Change Project at the Harvard Kennedy School defined disinformation as information that is "deliberately false or misleading, often spread for political gain or profit, or to discredit a target individual, group, movement, or political party."[10] It defined misinformation as "information whose inaccuracy is unintentional, and spread unknowingly."[11]

While there may not be a consensus on how to define it, many researchers agree that the data-driven economy and the rise of platforms have facilitated the spread of disinformation. In fact, some scholars call disinformation "computational propaganda" because, increasingly, disinformation is spread by individuals who rely on algorithms, automation and human curation.[12] As the Technology and Social Change Team (2021) noted, "opaque algorithms, policies, and enforcement mechanisms determine what information is available to whom....Social media, especially, brings with it mechanisms and tactics that allow for large-scale coordinated disinformation campaigns that are often hard to recognize and nearly impossible to mitigate once they have reached millions."

There is, however, a growing consensus among international human rights bodies and organizations that disinformation is dangerous to both human rights and democracy. Disinformation interferes with the public's ability to seek, receive and impart information and ideas regardless of frontiers. In addition, because individuals tend to congregate online in social bubbles with their friends and families, they may be less exposed to different voices. Yet to really understand an issue or problem, one needs to interact with people who hold different points of view or information that may challenge or nuance one's beliefs. Over time, these factors could exacerbate divisions and increase social and political polarization (Cedar Partners 2020; Infield 2020).

Consequently, with the spread of online disinformation, users may struggle to differentiate between authentic and false information online (Tucker et al. 2018; Technology and Social Change Team 2021). However, although disinformation has a corrosive effect on democracy, policy makers must ensure that any response does not undermine other human rights, such as freedom of expression or access to information (Office of the High Commissioner for Human Rights 2021). UN human rights bodies have made it clear that state actors should not make, sponsor, encourage or disseminate disinformation (Office of the High Commissioner for Human Rights 2017, 1, 3;

9 The Europen Union is calling for a shared approach. See https://ec.europa.eu/info/sites/info/files/joint-communication-eu-us-agenda_en.pdf.

10 See https://mediamanipulation.org/definitions; National Endowment for Democracy (2017).

11 See https://mediamanipulation.org/definitions.

12 See https://demtech.oii.ox.ac.uk/.

Methven O'Brien, Jørgensen and Hogan 2020; Amnesty International 2019). Researchers have found that disinformation efforts often include death and rape threats, accusations of treason or collusion with foreign intelligence agencies, and sexist and hyperpartisan insults. These efforts aim to intimidate and silence targeted individuals — most often journalists, activists, human rights defenders and vocal members of opposition coalitions (Riley, Etter and Bibhudatta 2018).

Disinformation can also affect the ability of individuals to shape their own destiny. Today, almost all our daily activities are data-collection opportunities, thanks to the mobile internet, the Internet of Things and other data-driven technologies (Nyst and Monaco 2018). According to one study, "personalized information builds a 'filter bubble' around us, a kind of digital prison for our thinking" (Helbing et al. 2017). In so doing, it could suppress creative and "out of the box" thinking, which in turn has spillover economic effects (ibid.).

Furthermore, disinformation is easily replicable. Anyone can share it online at no cost to them (Ryan et al. 2020). Not surprisingly, disinformation is also dangerous for economic stability: as it spreads, it can affect the reputations of firms and stock prices (Carvalho, Klagge and Moench 2011; Insikt Group 2019); alter economic decisions (Singh 2021); undermine public health and belief in science; and reduce trust in institutions (University of Baltimore and CHEQ 2019; Infield 2020). One study estimated that in 2018, disinformation cost the global economy some US$78 billion,[13] including $9 billion in unnecessary health-care costs and other expenditures; $17 billion in financial disinformation; $3 billion a year in platform efforts to combat disinformation and increase safety; and $9 billion a year in costs to repair damaged reputations due to fake news (University of Baltimore and CHEQ 2019).

If policy makers could develop a coordinated and effective international approach, they could possibly reduce these costs. 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). Policy makers have a long history of trying to develop a coordinated approach to other issues such as environmental protection and labour rights (Aaronson and Zimmerman 2007). Some have also tried to develop a coordinated approach to the governance of cyberspace and cyberthreats (Chernenko, Demidov and Lukyanov 2018; Lipton 2020; Talihärm, n.d.).

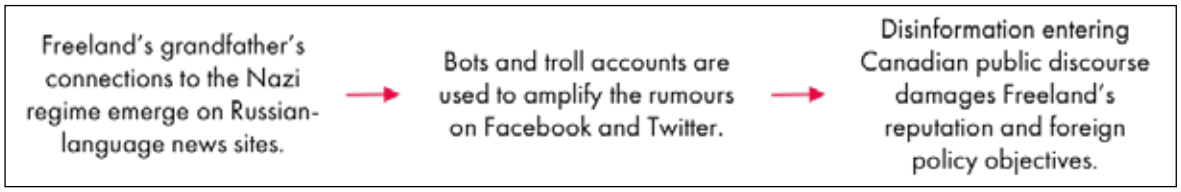
Figures 1, 2 and 3 outline recent examples of cross-border disinformation.

Figure 1: China's Disinformation about Alleged Australian Atrocities in Afghanistan

Sources: see Zhao (2020); Needham (2020); Hurst (2020).

13 All figures in US dollars unless otherwise noted.

Figure 2: Russian Disinformation about Canadian Deputy Prime Minister Chrystia Freeland



Sources: Carr (2017); Freeman (2017).

Figure 3: Russian Disinformation about French President Emmanuel Macron

Sources: Nugent (2018); Reuters (2017).

The Landscape for Disinformation and the Role of State Actors

State actors are both the perpetrators and the victims of disinformation. The Government of Canada's Communications Security Establishment (2019) reported that half of all advanced democracies holding national elections had their democratic processes targeted by cyberthreat activity, a three-fold increase since 2015. A 2021 study found that foreign actors were most active in disinformation campaigns against the United States, the United Kingdom and Egypt (Goldstein and Grossman 2021).

But it is difficult to attribute disinformation directly to a state. A government entity could be the creator and disseminator of disinformation, it could use bots or trolls, or it could hire a firm to do this dirty work. Government officials may be unable or unwilling to prove attribution because that could require government entities to release information about technical and physical intelligence capabilities and operations. As a result, even when intelligence agencies can attribute disinformation with a high degree of confidence, they face a second attribution problem in the court of public opinion (Newman 2016; Lindsay 2015).

Some governments actively spread disinformation, and firms are organizing to serve their needs. The US Department of Justice found that the Kremlin-backed Internet Research Agency initiated its efforts to interfere in US politics as early as 2014. This privately held Russian company, owned by a friend of President Vladimir Putin, spent $1.25 million per month on its combined domestic and global operations, which included 76 staffers fluent in English focused on the 2016 US presidential campaign.[14] In 2020, researchers at the Oxford Internet Institute estimated that some 65 firms deployed computational propaganda on behalf of a political actor in 48 countries. In addition, some "US $60 million was spent on hiring these firms since 2009" (Bradshaw, Bailey and Howard 2021, i). Apparently, there are few barriers to entry for such firms. In a 2017 study, Trend Micro found that $2,600 can buy a social media account with more than 300,000 followers; $55,000 is enough to fund a Twitter attack that successfully discredits a journalist; and $400,000 can influence policy changes on trade agreements,

14 *United States of America v Internet Research Agency LLC*, 18 USC §§ 2, 371, 1349, 1028A.

impact elections or change the course of a referendum (Gu, Kropotov and Yarochkin 2017).

What Role Do Platforms and Their Business Model Play in Fostering Dissemination across Borders?

The purveyors of disinformation rely on websites, apps, social networks and other means to disseminate information. Hence, they depend on the large companies that provide the tools for human connection in the internet age — the so-called platforms. Platforms can be defined as digital services that facilitate interactions between two or more distinct but interdependent sets of users (users can be firms, groups and/or individuals) who interact through the service via the internet (OECD 2019, 11).

Although every platform is distinct, and there are several business models used by various platforms, social networking platforms tend to rely on the "freemium" model, where users provide personal data in return for free digital services (Lynskey 2017). But these users are being "used" (United Nations Conference on Trade and Development 2019).[15] After collecting this data, the platforms aggregate users into groups divided by preferences, race, location, income and other features. Many data firms then make and sell predictions about users' interests, characteristics and, ultimately, behaviour to generate advertising revenue (Zuboff 2019; Amnesty International 2019; Snower and Twomey 2020). No one knows if the services that users receive for free are worth the direct and indirect costs of providing such data.

Netizens' understanding of the news is very much affected by who shares it and what their friends, family and colleagues say about it. In addition, the design of the platform's algorithm that provides users with content might convince them to stay on the site and focus their attention on a particular news item (Cave 2021; UK Information Commissioner's Office 2019). It is important to note that attention is a limited resource, and firms and individuals compete for users' attention (Ryan et al. 2020). Hence, platforms have incentives to design their algorithms to maintain their users' attention for as long as possible (CIGI 2019). In so doing, platforms can achieve economies of scale and scope from the content they provide as well as from the ads they tailor to users.[16] As an example, a search engine such as Bing or Chrome can include both results (content) and paid search ads (Evans 2020; GDI 2019).

Many researchers have shown that this business model incentivizes platforms to show sensationalistic or otherwise addictive content to keep people using and the ad money flowing. Platforms also gamify usage with "like" buttons, retweets and video view counters to keep people hooked. Hence, netizens are also incentivized to share and disseminate disinformation as well as information (Stoller 2021; Donovan 2021; Tworek 2021; Ryan et al. 2020).

Many of the large platforms are under extreme public pressure to moderate content and change their business model, but that is not necessarily what shareholders want. As AI expert Susan Etlinger (2019, 24) notes, "social media companies' mission statements focus on sharing, community and empowerment. But their business models are built on…their ability to grow, as measured in attention and engagement metrics: active users, time spent, content shared."

Not surprisingly, disinformation seems quite profitable (Ryan et al. 2020). In 2019, the GDI analyzed website traffic and audience information from 20,000 domains it suspected of disinformation and estimated the sites generated at least $235 million in ad revenue (Price 2019). Harvard University scholar Joan Donavan described disinformation as "a very lucrative business, especially if you're good at it" (Heim 2021).

In addition, this business model can create competition problems and, hence, problems for regulators. Data-driven platforms have found new ways of tying, bundling and self-preferencing that present new challenges. These strategies may lead to "winner-takes-all" markets and geographical concentration and may ultimately hinder innovation to the detriment of consumers.

15 Researchers at the Brown Institute for Media Innovation, a joint initiative between Columbia University and Stanford University, have shown that Amazon, Apple, Facebook and Google collect more than 450 different pieces of information about their users. See https://brown.columbia.edu/mapping-data-flows/.

16 A firm enjoys economies of scale when its long-run average costs decline as it expands output. A firm enjoys economies of scope when its total cost of producing two or more products and/or services is lower than the total cost when multiple firms produce the product lines separately (Baye and Prince 2020).

Much of what firms do, and supply, demand and pricing conditions are opaque to regulators (Crémer, de Montjoye and Schweitzer 2019).

Researchers struggle to show that consumers are hurt by the freemium model, but consumers have little market power. They cannot "punish" poor market performance in the form of higher prices or lower quality by switching to a rival company (Durocher 2019). Moreover, network externalities and scale economies lead to winner-takes-all market outcomes and, thus, a greater concentration of market power (WTO 2020, 157).

Platforms have and continue to receive significant revenue from this business model, which in turn gives them influence. Some of the biggest platforms have revenues that are significantly larger than many governments (Babic, Heemskerk and Fichtner 2018; Owens 2019). There is growing evidence that firms are using their market power to prevent governments from regulating or to shape such regulations so as not to reduce their dominant positions (Babic, Fichtner and Heemskerk 2017). As an example, in 2019, the British government reviewed the business practices of the digital behemoths and described their behaviour toward consumers and efforts to forestall regulation as "bullying" (BBC News 2019). In 2020, reports emerged that Facebook saw the short video app TikTok as an existential threat to Facebook's international ambitions. Several reporters found evidence that Facebook executives pressured the US government to act against the company. President Donald Trump's administration decided to ban the app and encouraged its sale to a US company (Arbel and O'Brien 2021). In 2021, both Google and Facebook threatened to leave Australia after the government proposed requiring major platforms to pay for news they link to.[17] While governments retain significant tools to act against these firms, a coordinated international approach might forestall such bullying of governments by the data giants.

The Role of Technology in Disinformation

Bots and AI

Technology has made it easier, cheaper and often more effective to automate disinformation (Bradshaw, Bailey and Howard 2021, 11, 23). Thanks to improvements in neural-based natural language generation and the availability of large pretrained models, companies find it increasingly easy to produce bots — another key innovation.

Bots are automated servants that can perform a wide variety of repetitive tasks such as generating reports, providing virtual assistance, creating and sending invoices, verifying documents or signatures, and even communicating with consumers. In so doing, they displace human workers (Nadel and Prescott 2019, 5; Howard 2014).[18]

Bots are not inherently bad. Some bots can do good things, such as search engine bots (web crawlers) that index content for online searches or customer service bots that help users. However, when bots are programmed to break into user accounts or perform other malicious activities, they can have "bad" direct and indirect effects on humans and society.[19] Moreover, some bots are designed to amplify the reach of disinformation and exploit the vulnerabilities that stem from our cognitive and social biases. In so doing, they create the illusion that individuals have independently agreed that information is correct (Wardle and Derakhshan 2017).

However, spam bots are clearly facilitating disinformation across borders. By automating "trolling" (i.e., the practice of criticizing or threatening certain speakers such as women and people of colour in response to their views), spambots can exacerbate highly problematic trends of online hate speech and abuse (Citron 2015). Using 2017 data, the Pew Research Center estimated that between nine and 15 percent of all Twitter accounts are automated, and 66 percent of all tweeted links to popular sites were disseminated by bot accounts (Wojcik et al. 2018). Bots, in general, are estimated to make up roughly 37.9 percent of all

17 For more on the Australian "bargaining code," see Frydenberg and Fletcher (2020); on Google leaving Australia, see https://about.google/google-in-australia/an-open-letter/; on Facebook threatening Australia, see Meade (2020); and for Australia's response, see Hywood (2021). It is interesting to note that Google is paying for news in France; see Browne (2021). The law is based on the EU Copyright Directive.

18 See www.cloudflare.com/en-ca/learning/bots/what-is-a-bot/.

19 Ibid.

internet traffic. In 2018, one in five website requests — 20.4 percent of traffic — was generated by bad bots alone (Osborne 2019). The United States is the source of many bad bots. In total, 53.4 percent of bad bot traffic came from the United States, followed by the Netherlands and China (ibid.).

Policy makers are starting to regulate spambots used to disseminate disinformation (they already regulate bots used for mass ticket purchasing/scalping purposes).[20] California became the first state to require bots to openly identify themselves as automated online accounts. The law makes it "unlawful for any person to use a bot to communicate or interact with another person in California online with the intent to mislead the other person about its artificial identity for the purpose of knowingly deceiving the person about the content of the communication in order to incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election."[21] Under the law, all such bots must conspicuously declare themselves. The owner or creator of the bot, not the platform, is responsible for designating the account as automated. Under the law, the state can challenge overinflated follower counts, fake likes, and engineered retweets and reposts, reducing the seeming newsworthiness and importance of certain posts and stories (DiResta 2019; Cohen 2019).[22] But the law is broad and vague (it includes chatbots on companies' websites) and provides no private right of action. In short, individuals cannot sue to challenge bots — only the state can (Nadel and Prescott 2019, 4). Senator Dianne Feinstein has introduced a similar bill in the Senate, but it has not moved past committee.[23] Meanwhile, the European Union has banned ticketing bots and is considering challenging spam- and chatbots that spread disinformation (Tech Observer 2020).

An Overview of Government Efforts to Tackle Disinformation beyond Competition Policy

Disinformation is a form of speech (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 United States sits on one side of a continuum, where law and culture dictate that there should be relatively few restrictions on speech and where government plays a limited role in regulating social networks. US policies are guided by section 230 of the 1996 Communications Decency Act, which states 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 but also a range of "interactive computer service providers," including basically any online service that publishes third-party content from sites such as Amazon, Target, Trip Advisor and Yelp.[24]

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

But most countries do not have sufficient leverage to influence the practices of the platforms, unless they are large and growing data markets such as India. Moreover, many netizens do not agree with the notion that companies should decide how and when to moderate content online when they profit from monetizing personal data. They want to put forward their own approaches (McCabe and Swanson 2019). As Canadian political scientist Blayne Haggart (2021) notes, "It may be time to question whether the very model of the global platform — and the outsourcing of ultimate authority to the United States — makes democratic sense. Domestic control of platforms (private or public), and not just domestic regulation, may be necessary to ensure that platforms are more

20 Pub. L. No. 114-274, S. 3183, commonly referred to as the Better Online Ticket Sales Act (BOTS Act), was signed into federal law on December 14, 2016.

21 *Ibid*.

22 To view the bill, see https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001.

23 A bill "to protect the right of the American public under the First Amendment to the Constitution of the United States to receive news and information from disparate sources by regulating the use of automated software programs intended to impersonate or replicate human activity on social media" (see www.govtrack.us/congress/bills/116/s2125).

24 See https://uscode.house.gov/view.xhtml?req=(title:47%20section:230%20edition:prelim); www.eff.org/issues/cda230. The Trump administration proposed several reforms (see www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996).

responsive to Canadians' needs. We need to stop thinking about the internet and platforms as undifferentiated spaces and start thinking about what a federated internet of interoperable democratic sovereign countries might look like."

Some countries have advanced domestic strategies to mitigate disinformation, although it is too early to evaluate whether these strategies are effective. For example, Germany created legislation to regulate hate speech, known as the Network Enforcement Act (NetzDG),[25] while the United Kingdom and Australia require firms to remove "online harms" (Hern 2020). The European Union just tabled new legislation to increase the accountability of online platforms and clarify the rules for taking down illegal content. Courts and laws will decide what is legal and when content should be blocked (Scott, Larger and Kayali 2020). Canada is working to enhance citizen preparedness to recognize disinformation, combat foreign interference, and increase the proactivity and accountability of social networks in protecting Canadian democracy.[26] However, policy makers are also finding it difficult to regulate disinformation domestically. As an example, Canada's disinformation law was struck down by Canada's high court and, thus far, NetzDG has not clearly led to a documentable reduction in hate speech.[27]

Around the world, policy makers[28] (and firms[29] to some degree [Chakravorti 2020]) are not only using content moderation regulations to address disinformation but they are also trying to develop technical fixes, regulate political advertising, train citizens to recognize disinformation, fund investigations and enforcement actions, and help other governments address disinformation. For example, DARPA spent $68 million trying to find a technological solution for spotting manipulated fake videos. It also funded the Enhanced Attribution program, which aims to provide greater visibility into "opaque malicious cyber adversary actions…by providing high-fidelity visibility…and to increase the government's ability to publicly reveal the actions of individual malicious cyber operators without damaging sources and methods."[30] Britain has spent £18 million on a "fake news fund" for Eastern Europe. The European Commission has put €$5.5 million into a rapid alert system to help EU member states recognize disinformation campaigns (University of Baltimore and CHEQ 2019). Meanwhile, researchers are analyzing the disinformation ecosystem and identifying disinformation campaigns, bot networks and troll factories, and foundations and governments are trying to bolster the free press and teach the public critical thinking skills (Canadian Security Intelligence Service 2018; Morrison, Barnet and Martin 2020; Cave 2021).[31]

Given this patchwork of approaches, policy makers (and executives) recognize the need for collective action. The members of the Group of Seven (G7) who met in Canada in June 2018 agreed to the Charlevoix Commitment on Defending Democracy from Foreign Threats. The G7 agreed to "establish a G7 Rapid Response Mechanism to strengthen our coordination to identify and respond to diverse and evolving threats to our democracies, including through sharing information" (Fried 2019). At the initiative of France, some 95 nations have banded together to discuss effective solutions to the problems of disinformation and cyber insecurity (Government of Canada 2021a).

However, these strategies can do little to mitigate cross-border disinformation flows or to prod firms to address some of the problems with their current business model. As with labour and the 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, especially at the regional and binational levels, increasingly contain rules that could lead to a more coordinated international approach to directly

25 See www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG_node.html.

26 See www.canada.ca/en/canadian-heritage/services/online-disinformation.html; www.loc.gov/law/help/social-media-disinformation/canada.php.

27 On Canada's election law, see www.cbc.ca/news/politics/elections-misinformation-court-free-speech-1.5948463; on the effects of NetzDG, see www.ceps.eu/ceps-projects/the-impact-of-the-german-netzdg-law/.

28 For a list of national laws regarding fake news, see www.reuters.com/article/us-singapore-politics-fakenews-factbox/factbox-fake-news-laws-around-the-world-idUSKCN1RE0XN.

29 As an example, Twitter is asking some of its users to point out disinformation (to crowdsource it) (see Fung 2021), while Facebook is trying to make its campaign advertising business more transparent and is making tweaks to its algorithms to support verified news and to curb political advertising during times of political volatility (see Fischer 2021).

30 See www.darpa.mil/program/enhanced-attribution.

31 The Carnegie Endowment for International Peace (see Smith 2020), *The Washington Post* (see Heim 2021) and *The Guardian* (see Wong 2021) recently published descriptions of innovative ideas to address disinformation. CIGI (2019) published a whole essay series on the topic.

tackle cross-border disinformation. The next section delineates what trade agreements currently say and how they may provide building blocks for language to govern cross-border disinformation flows.

The State of Digital Trade Agreements and the Governance of Malicious Cross-Border Data Flows

In its *World Trade Report 2020*, the WTO Secretariat noted a Catch-22 in the global economy. On the one hand, "the increasing importance of data as an input in production and of the fluidity of data is leading to increasing demands for new international rules on data transfers, data localization and privacy....At the same time, the winner-takes-all characteristics of certain digital industries could lead to policy responses that raise tensions between countries and introduce unnecessarily high market barriers" (WTO 2020, 11–12).

This section delineates what trade agreements say about regulating cross-border data flows, competition policies, spam and the use of trade tools to target entities that disseminate disinformation across borders. The author notes that, for the purposes of this writing, e-commerce and digital trade agreements are used interchangeably.

Much of the language in trade agreements is built on and highly influenced by the US approach to governing the internet, the companies that provide its infrastructure and the data that underpins that network of networks. For this reason, the author argues, the free flow of data, with certain exceptions, became the default for almost every trade agreement until recently. The United States was and is home to many of the world's largest digital firms, and it drafted the original principles designed to govern e-commerce and cross-border data flows (Aaronson 2015).

America began that effort in 1997 when then President Bill Clinton announced a Framework for Global Electronic Commerce. This framework articulated what the regulatory environment "should" look like if nations wanted to encourage national and global e-commerce. The framework focused on private sector leadership, a limited role for government intervention, and principles to reassure consumers that their data would be protected and secure.[32]

But, to some extent, the effort to build trust in e-commerce by ensuring users that they and their data would be safe took a back seat to the notion of free flow of data across borders. US policy makers recognized that rules encouraging the free flow of data would help America's data giants both expand their access to data and grow ever bigger. The Clinton administration made it clear that "the US government supports the broadest possible free flow of information across international borders."[33] This framework very much influenced the OECD Action Plan for Electronic Commerce, which in turn influenced the bilateral and regional agreements on e-commerce described below (Aaronson 2015; 2018; Burri 2013).

Unfortunately, almost every trade agreement does not acknowledge the Catch-22 underpinning cross-border data flows. Much of the data flowing across borders is aggregated and allegedly anonymized personal data. While users may benefit from services built on data, the people who are the source of that data do not control it. It is their asset, yet they cannot manage, control, exchange or account for it (World Economic Forum 2011, 11). Individuals' data can essentially be weaponized to create malicious cross-border data flows, whether through disinformation, malware, spam or other means.

Provisions to Encourage Cross-Border Data Flows

In the absence of consensus on how to govern data at the WTO, many countries including Australia, Canada, Chile, EU member states, Japan, Singapore, the United Kingdom and the United States have placed language governing cross-border data flows in the e-commerce chapters of recent free trade agreements (FTAs). Some 52 percent (182 of 345) of recent (2000–

32 See Framework for Global Electronic Commerce at https://clintonwhitehouse4.archives.gov/WH/New/Commerce/.

33 Ibid.; see presidential directive at https://fas.org/irp/offdocs/pdd-nec-ec.htm.

2019) trade agreements have e-commerce or digital trade provisions, and such language is increasingly binding (Burri and Polanco 2020).

Some of these agreements, such as the United Kingdom's withdrawal agreement from the European Union (Brexit), the Canada-United States-Mexico Agreement (CUSMA), and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, cover a wide range of sectors. However, some nations, including Chile, Japan, New Zealand, Singapore and the United States, have established sector-specific stand-alone digital trade agreements. The Digital Economy Partnership Agreement (DEPA), the Singapore-Australia Digital Economy Agreement (SADEA) and the US-Japan digital FTAs have much in common (Wu 2017; Monteiro and Teh 2017; Asian Trade Centre 2019). As noted above, these agreements are built on principles first enunciated by the United States in 1997, in the Framework for Global Electronic Commerce. Trade negotiators focus on rules to govern cross-border data flows and generally rely on nations to enforce their own laws to protect consumers and citizens from harmful or malicious cross-border data flows.

Almost every recent agreement has binding language that makes the free flow of data a default. They contain language such as "Neither Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means, if this activity is for the conduct of the business of a covered person."[34] Such language makes no distinction between data flows that underpin a press release from the WHO or disinformation from Russia's Internet Research Agency, a Russian troll farm famous for sending disinformation (Chen 2015). But policy makers also acknowledge that nations have other important policy objectives, such as preserving public order, privacy, consumer welfare or public morals. Hence, by using the exception as justification, a nation can restrict cross-border data flows.[35] These agreements generally incorporate both the General Agreement on Tariffs and Trade (GATT) (articles XX and XXI) and the General Agreement on Trade in Services (GATS) exceptions (article XIV).[36] All of these trade agreements also include a national security exception, in which nations can breach the rules to protect against what their policy makers see as a national security threat. Nations using these exceptions do not have to justify their reasons to other nations.[37] However, when nations use the exceptions, they must be for necessary purposes and be designed to be as least trade restrictive as possible.[38]

Nations are supposed to turn to these exceptions only in extraordinary circumstances. However, there are few shared norms and definitions regarding how nations should behave when rules governing data flows conflict with the achievement of other important policy objectives (Aaronson 2018). Consequently, there is a patchwork of strategies to build consumer and user trust at the national level, but less of a focus on shared and/or interoperable strategies. However, exceptions risk becoming the rule without the further development of mechanisms to bridge regulatory differences between countries. For example, the

34 See *Agreement between the United States of America and Japan Concerning Digital Trade*, 7 October 2019, art 11 (entered into force 1 January 2020) [*US-Japan Digital Trade Agreement*], online: <https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf>; *Digital Economy Partnership Agreement*, 12 June 2020, art 4.2 at 4-1–4-2 (entered into force 7 January 2021) [*DEPA*], online: <www.mfat.govt.nz/assets/Uploads/DEPA-Signing-Text-11-June-2020-GMT.pdf>.

35 See *General Agreement on Trade in Services*, 15 April 1994, 1869 UNTS 183, 33 ILM 1167 (1994) art XIV (entered into force 1 January 1995) [*GATS*]: the exceptions include "measures (a) necessary to protect public morals or to maintain public order; (b) necessary to protect human, animal or plant life or health; (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this agreement including those relating to: (i) the prevention of deceptive and fraudulent practices or to deal with the effects or a default on services contracts; (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; [and] (iii) safety." See also www.international.gc.ca/trade-commerce/assets/pdfs/agreements-accords/cusma-aceum/cusma-19.pdf.

36 See e.g. *GATS*, *supra* note 35, art XIV bis: "Nothing in this Agreement shall be construed: (a) to require any Member to furnish any information, the disclosure of which it considers contrary to its essential security interests; or (b) to prevent any Member from taking any action which it considers necessary for the protection of its essential security interests."

37 See *DEPA*, *supra* note 34, art 15.2: "Nothing in this Agreement shall be construed to: (a) require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or (b) preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests."

38 They use language such as "such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between the Parties where like conditions prevail." See *Canada-European Union Comprehensive Economic and Trade Agreement*, 30 October 2016, art 28.3 (provisionally entered into force 21 September 2017), online: <www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/ceta-aecg/text-texte/28.aspx?lang=eng>.

United States used the exceptions to protect public morals in an internet gambling case (the United States refused foreign suppliers of gambling on the basis of public morals) and considered using the exceptions in response to Chinese censorship (the "Great Firewall of China") because it impeded market access for US digital firms (Aaronson 2018).

Moreover, the exceptions were not built for the digital age. Economist Dan Ciuriak (2019) argues that the socially harmful use of data such as "fake news" and disinformation for personally targeted advertising and/or messaging (for example, the exploitation of psychological vulnerabilities for marketing purposes or for political manipulation) should be considered a legitimate exception.

Protecting privacy and personal data is a widely accepted "exception" to the free flow of data. Canadian, New Zealand and US FTAs generally state that the parties agree that because consumer and personal data protection are important, signatories should enforce their own laws, which in turn should be built on international principles such as the Asia-Pacific Economic Cooperation Privacy Framework and OECD Guidelines.[39] The parties also recognize the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented. In contrast, signatories to EU digital trade agreements must first be deemed adequate for personal data to flow freely among nations. As of this writing, only 14 nations are deemed "adequate."[40]

The 2020 SADEA seems to be the first agreement calling for interoperability of data protection regimes. Interoperability would make data protection more effective, as national approaches would be more coherent. It notes that "each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks."[41] In short, the signatories are calling mutual recognition an appropriate approach to foster interoperability.

Intermediary Liability and Content Moderation

As noted above, countries have different ideas on how content should be regulated and what entities — whether business, government or a combination of the two — should do such regulating. US rules have protected online platforms from lawsuits related to user content and legal challenges stemming from how they moderate content. Not surprisingly, in recent years, the United States tried to include its approach to content moderation in some trade agreements. The United States demanded language on intermediary liability in the US-Japan Digital Trade Agreement and CUSMA. Interestingly, the provisions do not apply to Mexico until the agreement has been in effect for three years.[42] In 2019, Australia passed the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act, which makes it illegal for social media platforms to fail to promptly remove such user material shared on their services. The author could not find language adding this policy to the recent SADEA, although the agreement states that online safety is a shared responsibility for all online actors.[43] In addition, the author could find no other nations with intermediary liability language in their trade agreements.[44]

39 These principles include limitations on collection, choice, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation and accountability.

40 The adoption of an adequacy decision involves a proposal from the European Commission, an opinion of the European Data Protection Board, approval from EU countries and adoption of the decision by the European Commission. The European Commission has, so far, recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection. See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en; and https://trade.ec.europa.eu/access-to-markets/en/content/digital-trade-eu-trade-agreements-0.

41 See *Singapore-Australia Digital Economy Agreement*, 6 August 2020, art 17(7) (entered into force 8 December 2020) [*SADEA*], online: <www.mti.gov.sg/-/media/MTI/Microsites/DEAs/Singapore-Australia-Digital-Economy-Agreement/Singapore-Australia-Digital-Economy-Agreement.pdf>.

42 See *US-Japan Digital Trade Agreement*, *supra* note 34, art 18 at paras 3, 4; *Canada-United States-Mexico Agreement*, 30 November 2018, c 19, art 19.17(2) (entered into force 1 July 2020) [*CUSMA*], online: <www.international.gc.ca/trade-commerce/assets/pdfs/agreements-accords/cusma-aceum/cusma-19.pdf> ("[N]o Party shall adopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by the service, except to the extent the supplier or user has, in whole or in part, created or developed the information.")

43 See *SADEA*, *supra* note 41.

44 See *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill 2019* (Austl), 2019/45, online: <www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1201>.

The United States is unlikely to push to include language regarding content moderation rules built on section 230 in other trade agreements. President Joe Biden's administration wants to see reform of section 230 and recognizes that other nations are not enthusiastic about including such language in future trade agreements (McCabe and Swanson 2019; Laslo 2019; Lerman 2021).

Provisions to Encourage Competition

The WTO has limited competence on competition/antitrust policies, which could be used by states collectively to tackle the business model. As an example, GATT and GATS contain rules on monopolies and exclusive service suppliers. The principles have been elaborated considerably in the rules and commitments on telecommunications. The agreements on intellectual property and services both recognize governments' rights to act against anti-competitive practices and their rights to work together to limit these practices (Anderson et al. 2018).

Specifically, GATS generally prohibits WTO members from adopting regulations that discriminate among foreign service suppliers ("most-favoured-nation treatment") (GATS article 2.1). GATS, moreover, requires WTO members to regulate reasonably, objectively and impartially and provide foreign service providers with a possibility to express concerns and have a regulation reviewed (GATS article 6). GATS also requires WTO members to be transparent about regulations that may affect services trade (GATS article 3). These regulations can include labour laws and competition policies (Basedow and Kauffmann 2016).

But policy makers have greater freedom to export their competition policy strategies in their bilateral and regional FTAs. In its FTAs, the European Union requires regional trade agreement parties to prohibit specific anti-competitive practices to the extent that they affect trade; these agreements include obligations to establish or maintain competition laws and to create an institution to enforce them. The United States and Canada require signatories to establish and enforce their own laws (Anderson et al. 2018).[45] The United States and Canada have also added accountability provisions with requirements relating to non-discrimination, transparency and/or procedural fairness (WTO 2020, 147).

In a 2020 report, the OECD (2020, 3) suggested that "competition authorities seeking to address abuses of dominance in digital markets would benefit from deeper international co-operation, given the international scope of many digital firms." Recent FTAs seem to be moving in that direction with cooperation language. In its most recent trade agreement, Australia and Singapore agreed to a more thorough approach to cooperation on enforcement, noting that the parties "shall endeavour to cooperate, where practicable and in accordance with their respective laws and regulations, on issues of competition law enforcement in digital markets, including through notification, consultation and the exchange of information."[46]

DEPA includes similar non-binding language to encourage cooperation on completion. Signatories are supposed to exchange information and experiences on development of competition policies in the digital markets, share best practices and provide advice or training. "The Parties shall cooperate…including through notification, consultation and the exchange of information," but "in a manner compatible with their respective laws, regulations and… within their reasonably available resources."[47]

Taken in sum, given different national objectives and approaches to competition policies, trade agreements have yet to effectively encourage cooperation across borders to tackle the negative spillovers of this new data-driven economy.

Provisions to Promote Regulatory Coherence and Prevent a Race to the Bottom

Policy makers understand that nations have different norms and strategies for regulation, but a patchwork of regulation could cause problems for both producers and consumers of goods and services. In recent years, trade diplomats have drafted provisions in trade agreements to encourage greater coherence.

45 See e.g. *CUSMA*, *supra* note 42.

46 See *SADEA*, *supra* note 41, art 16(2).

47 See *DEPA*, *supra* note 34, art 8.4(2–3).

There are many strategies to achieve coherence, from measures to prod cooperation to mutual recognition and harmonization of regulations. Regulatory coherence includes competition policies, yet these most up-to-date FTAs do not have specific language facilitating such competition cooperation. DEPA, for example, calls for signatories to "pursue the development of mechanisms to promote compatibility and interoperability between their different regimes for protecting personal information."[48] Such strategies can include mutual recognition, regulatory sandboxes (where regulators can experiment) or shared international frameworks.[49] CUSMA, a broader trade agreement, has a regulatory chapter, which states that "each Party should encourage its regulatory authorities to engage in mutually beneficial regulatory cooperation activities with relevant counterparts of one or more of the other Parties in appropriate circumstances to achieve these objectives."[50] EU trade agreements have a section on regulatory cooperation, which notes, "Recognising the global nature of digital trade, the parties shall cooperate on regulatory issues and best practices through the existing sectoral dialogues."[51] The Brexit agreement simply states, "The Parties shall exchange information on regulatory matters in the context of digital trade."[52]

The Singapore-Australia Free Trade Agreement (SAFTA) goes further on how nations should cooperate. It calls for the parties to endeavour to support data innovation through data-sharing collaboration and regulatory sandboxes.[53] But here, too, the current approach is unlikely to encourage a shared approach to regulation that can serve as a multilateral counterweight to the power of the big firms. Moreover, such strategies cannot prevent a race to the bottom, as many countries have no digital regulations or are just learning how to regulate digital firms. For example, many developing countries in Africa have to trade with Europe, which increasingly means they must adopt European standards for data protection. They do not have the time or policy space to develop their own standards (Pisa, Dixon and Ndulu 2021). Moreover, data governance is expensive and requires good policy governance skills. Data governance will be essential to development, and donor nations have a responsibility to work with developing countries to improve their data governance. Yet trade policy makers have yet to effectively link digital trade governance and data governance capacity building (Aaronson 2019).

Provisions to Reduce Spam

Many, but not all, countries have laws that ban spam.[54] In 2006, members of the OECD issued recommendations on cooperation to address spam. They acknowledged that spam undermined trust and consumer confidence, "which is a prerequisite for the information society and for the success of e-commerce," and that it led to "economic and social costs."[55] They also recognized that "spam poses unique challenges for law enforcement in that senders can easily hide their identity, forge the electronic path of their email messages, and send their messages from anywhere in the world to anyone in the world, thus making spam a uniquely international problem that can only be efficiently addressed through international co-operation."[56] The signatories agreed that they must cooperate to investigate and enforce cross-border spam problems (OECD 2006).

The OECD Recommendations have influenced e-commerce and digital trade language. Almost every trade agreement that covers e-commerce or digital trade includes language to govern spam (Asian Trade Centre 2019). Many FTAs have taken steps to regulate unsolicited commercial electronic communications. Such measures include obtaining

48 *Ibid.*, art 4.2(6).

49 *Ibid.*

50 See *CUSMA*, *supra* note 42, c 28, art 28.17(1), online: <www.international.gc.ca/trade-commerce/assets/pdfs/agreements-accords/cusma-aceum/cusma-28.pdf>.

51 See *Modernisation of the Trade part of the EU-Mexico Global Agreement*, not yet signed, art 11(1), online: <https://trade.ec.europa.eu/doclib/docs/2018/april/tradoc_156811.pdf>.

52 See *Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part*, 30 December 2020, OJ L 149, tit III, art 16(1) (entered into force 1 May 2021) [*EU-UK Trade and Cooperation Agreement*], online: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948119/EU-UK_Trade_and_Cooperation_Agreement_24.12.2020.pdf>.

53 See *Singapore-Australia Free Trade Agreement*, 17 February 2003, art 2(2) (entered into force 28 July 2003) [*SAFTA*], online: <www.dfat.gov.au/trade/agreements/in-force/safta/official-documents/Pages/default>.

54 See https://en.wikipedia.org/wiki/Email_spam_legislation_by_country.

55 See https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0344.

56 Ibid.

personal consent of the consumers to receive such messages, their right to opt out from receiving unwanted messages and appropriate recourse if suppliers do not respect such regulations.[57] As an example, the Digital EU UK Agreement states, "Each Party shall ensure that users are effectively protected against unsolicited direct marketing communications,"[58] but it does not delineate how. It also states that spam is not illegal, but "each Party shall ensure that direct marketing communications are clearly identifiable as such, clearly disclose on whose behalf they are made and contain the necessary information to enable users to request cessation free of charge and at any moment."[59] Finally, users must have a form of redress.[60] SAFTA goes further, noting that "each Party shall provide recourse against a supplier of unsolicited commercial electronic messages" and the parties should cooperate in issues regarding spam.[61]

However, telling countries they should enforce their own laws is based on a presumption that countries have the funds and expertise to do so. In the time of COVID-19, when all budgets are challenged by increased expenditures for public health and unemployment, that approach seems unworkable.

Bans on Certain Practices

Trade agreements create rules to ensure that certain practices do not discriminate among domestic and foreign providers of services or create unfair advantages for domestic companies. Some practices are regulated and other, more egregious, practices are banned.

Almost every digital trade agreement or chapter bans two practices — performance requirements and data localization — because these practices can discriminate against foreign providers of data services (and, in so doing, impede market access). The EU-UK Trade and Cooperation Agreement states that cross-border data flows shall not be restricted by data localization strategies and "a Party shall not require the transfer of, or access to, the source code of software owned by a natural or legal person of the other Party."[62] Recent US and Canadian trade agreements ban "performance requirements" for source code. As an example, the US-Japan Digital Trade Agreement states that "neither Party shall require the transfer of, or access to, source code of software owned by a person of the other Party, or the transfer of, or access to, an algorithm expressed in that source code, as a condition for the import, distribution, sale, or use of that software, or of products containing that software, in its territory."[63] It then allows an exception for a "specific investigation,... enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure."[64] EU agreements have similar language.[65]

Trade diplomats have not yet banned other practices. Yet disinformation such as malware and distributed denial-of-service attacks can undermine market access and raise costs for firms that must hire researchers to ascertain who is responsible for these attacks while simultaneously correcting disinformation. Moreover, disinformation may have hidden costs, including reducing internet generativity and perceptions that the internet is a safe and stable place to be.

Retaliatory Measures

The United States has used sanctions to deal with "malicious cyber-enabled activities originating from, or directed by persons located, in whole or in

57 See e.g. *US-Japan Digital Trade Agreement, supra* note 34, art 16: "Each Party shall adopt or maintain measures regarding unsolicited commercial electronic messages that: (a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; or (b) require the consent, as specified in its laws and regulations, of recipients to receive commercial electronic messages. 2. Each Party shall provide recourse against suppliers of unsolicited commercial electronic messages." See also *CUSMA, supra* note 42, c 19, art 19.13: "1. Each Party shall adopt or maintain measures providing for the limitation of unsolicited commercial electronic communications. 2. Each Party shall adopt or maintain measures regarding unsolicited commercial electronic communications sent to an electronic mail address that messages that (a) require suppliers of unsolicited commercial electronic messages to facilitate the ability of recipients to prevent ongoing reception of those messages; or (b) require the consent, as specified in the laws and regulations of each Party, of recipients to receive commercial electronic messages."

58 See *Digital EU UK Agreement* (part of *EU-UK Trade and Cooperation Agreement, supra* note 52), c 1, art 14(1), online: <http://brexitlegalguide.co.uk/digital-eu-uk-agreeement/>.

59 *Ibid.*, art 14(4).

60 See *EU-UK Trade and Cooperation Agreement, supra* note 52.

61 See *SAFTA, supra* note 53, c 14, art 19(3–4).

62 See *EU-UK Trade and Cooperation Agreement, supra* note 52, tit III, art 12(1).

63 See *US-Japan Digital Trade Agreement, supra* note 34, art 17(1).

64 *Ibid.*, art 17(2).

65 See *EU-Indonesia Free Trade Agreement*, not yet signed, tit XX, art X.9(1): "No Party may require the transfer of, or access to, source code of software owned by a juridical or natural person of the other Party."

substantial part, outside the United States."[66] Since 2016, US law has authorized sanctions related to interfering with or undermining election processes or institutions (US Department of the Treasury 2017, 3). In this regard, the United States has sanctioned Russian and Iranian entities. The US process requires an investigation, attribution and then development of a strategy to target the responsible entities.[67] The United States justifies its actions as legitimate under the national security exceptions.

Although the United States seems to be the only nation that has retaliated, the European Union did a poll in 2019, which found that 74 percent of respondents to the public consultation were in favour of imposing costs on states that conduct organized disinformation campaigns. Although many democracies such as the United States overuse sanctions, they could threaten trade sanctions against countries that launch disinformation campaigns designed to undermine democracy or trust in government actors. Such a strategy could be effective because it raises the cost of foreign influence operations (European Commission 2020).

Recommendations

Trade agreements cannot stop cross-border disinformation flows, but they can provide tools for mitigating such flows. In addition, trade agreements cannot address the business model underlying disinformation, although they can help policy makers collaborate to challenge platform practices that fuel disinformation. These agreements may also help ensure that policy makers do not avoid regulating for fear of tech-firm bullying. Moreover, they could provide an impetus to return to a focus on establishing trust and security among market actors — the users that provide the data, as well as the companies that control and monetize the data. One can see the beginnings of this approach in SADEA and DEPA.

In this section, the author presents ideas on how nations might cooperate to build greater transparency regarding the frequency of disinformation; develop appropriate responses to disinformation; examine the business model underpinning disinformation; and work together effectively to address it.

Objective: Enhance trade agreement rules to govern disinformation and foster international cooperation. Policy makers should:

- Encourage UNCITRAL to create an additional model law defining cross-border disinformation and delineating how to attribute such disinformation. Such a law should include provisions requiring platforms and media outlets to delineate how they protect users from disinformation. It should also include language banning private firms from producing and exporting disinformation as a service. Since 1996, UN bodies have encouraged nations to adopt a variant of the Model Law on Electronic Commerce.[68] The law serves as a building block for national legislation as well as a foundation for international trade agreements.[69]
- Supplement trade agreement provisions on spam to include language covering cross-border disinformation and requiring signatories to enforce their own laws related to cross-border disinformation. Note that disinformation is often promoted by spambots across borders.
- Add language to trade agreements requiring signatories to develop national laws banning the use of spambots to disseminate disinformation across borders and require firms to ensure that users attempting to disseminate information across borders are human (through verification).
- Add language to trade agreements requiring nations to enforce their laws on the use of spambots. This language should encourage nations to attempt to attribute the use

66 See www.whitehouse.gov/briefing-room/presidential-actions/2021/03/29/notice-on-the-continuation-of-the-national-emergency-with-respect-to-significant-malicious-cyber-enabled-activities/.

67 For more on sanctions against Russian entities, see https://home.treasury.gov/news/press-releases/sm1118; on sanctions against Iranian entities, see https://home.treasury.gov/news/press-releases/sm1158; and on the executive order imposing sanctions against foreign interference in US elections, see https://home.treasury.gov/system/files/126/election_executive_order_13848.pdf.

68 See https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce. Drafters designed the model law to encourage a more universal approach to governing e-commerce.

69 See *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998*, online: <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf>.

of spambots and collaborate with other nations to identify those countries that use spambots to disseminate disinformation.

- Clarify that nations can use the exceptions to justify breaching trade agreement rules and cross-border data flows to address disinformation. The language should provide guidance that trade agreement signatories can use trade or financial sanctions to punish entities and/or governments that disseminate disinformation across borders. However, nations must establish a transparent and public process of evidence gathering and attribution before they sanction.

- Add language to trade agreements that bans disinformation as an internationally traded service. Private firms should not be allowed to work for foreign governments that create or disseminate disinformation across borders.

Objective: Individuals and economic actors can be harmed collectively by disinformation when their data is aggregated under the current business model. This problem can be addressed by enhancing personal data protection to mitigate collective harms. Policy makers should:

- Add language stating that signatories shall not use the personal information of natural persons obtained from enterprises within their jurisdiction in a manner that constitutes targeted discrimination based on attributes such as race, colour, sex, sexual orientation, gender, language, religion, political or other opinion, national origin, property, medical or birth (or other status); genetic identity, age, ethnicity or disability.[70]

- Add language in the provisions on personal data protection that allows natural persons to pursue remedies for violations of personal data protection across borders. Such language would also allow groups at the national and international levels to pursue such remedies against platforms and other entities in cases of cross-border disinformation when groups of individuals are targeted.

Objective: Bolster competition policies, encourage international cooperation on competition, restrict data-giant bullying and prevent a race to the bottom regarding regulating digital firms. Policy makers should:

- Add language to the competition chapters/language in trade agreements that encourages signatories to cooperate on investigations and accept competition analysis and data from other signatories (mutual recognition) (Dutch Data Protection Authority 2013). Encourage nations to collaborate on regulatory action and remedies in more than one jurisdiction. Provide capacity building to developing country competition authorities for such shared investigations and remediation.

Objective: Bolster international understanding and cooperation on regulating disinformation. Policy makers should:

- Build a culture of transparency regarding malicious cross-border data flows. In trade policy reviews, where member states review each other's commitments to the rules, states should be transparent about their experience with disinformation and other malicious cross-border data flows and how they are regulating such flows. Greater transparency about what states are doing may reduce the incentives to spread disinformation across borders and increase incentives to punish such activities.

Conclusion

The World Economic Forum ranks the spread of disinformation and fake news as among the world's top global risks (Edmond 2020). Under current legal frameworks and economic conditions, many of the giant platforms are unwilling to address the business model that both finances and perpetuates disinformation. Hence, disinformation is both a global and a national problem that nations must cooperate with each other to mitigate.

Rather than constraining governments, international cooperation may help many developing countries that are also subject to disinformation address this shared problem. Moreover, a shared approach could build trust among users.

70 This language builds on the WTO *Electronic Commerce Negotiations – Consolidated negotiating text – December 2020* (dated December 14, 2020), paragraph 14, which contains language in the draft text released online without the permission of the WTO Secretariat or WTO members.

Works Cited

Aaronson, Susan. 2015. "Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security." *World Trade Review* 14 (4): 671–700.

———. 2018. "What Are We Talking about When We Talk about Digital Protectionism?" *World Trade Review* 18 (4): 1–37.

———. 2019. *Data Is a Development Issue*. CIGI Paper No. 223. Waterloo, ON: CIGI. www.cigionline.org/publications/data-development-issue/.

Aaronson, Susan Ariel and Thomas Struett. 2020. *Data Is Divisive: A History of Public Communications on E-commerce, 1998–2020*. CIGI Paper No. 247. Waterloo, ON: CIGI. www.cigionline.org/publications/data-divisive-history-public-communications-e-commerce-1998-2020/.

Aaronson, Susan Ariel and Jamie M. Zimmerman. 2007. *Trade Imbalance: The Struggle to Weigh Human Rights Concerns in Trade Policymaking*. New York, NY: Cambridge University Press.

Amnesty International. 2019. *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*. London, UK: Amnesty International, Ltd. www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF.

Anderson, Robert D., William E. Kovacic, Anna Caroline Müller and Nadezhda Sporysheva. 2018. "Competition Policy, Trade and the Global Economy: Existing WTO Elements, Commitments in Regional Trade Agreements, Current Challenges and Issues for Reflection." WTO Staff Working Paper ERSD-2018-12.

Angwin, Julia. 2021. "Understanding the Threat of 'Surveillance Capitalism.'" The Markup, February 13. www.getrevue.co/profile/themarkup/issues/understanding-the-threat-of-surveillance-capitalism-350921.

Arbel, Tali and Matt O'Brien. 2021. "Biden backs off on TikTok ban in review of Trump China moves." PBS News Hour, February 10. www.pbs.org/newshour/politics/biden-backs-off-on-tiktok-ban-in-review-of-trump-china-moves.

Asian Trade Centre. 2019. "Comparing Digital Rules in Trade Agreements." Asian Trade Centre, July 24. http://asiantradecentre.org/talkingtrade/comparing-digital-rules-in-trade-agreements.

Babic, Milan, Jan Fichtner and Eelke M. Heemskerk. 2017. "States versus Corporations: Rethinking the Power of Business in International Politics." *The International Spectator, Italian Journal of International Affairs* 52 (4): 20–43. doi:10.1080/03932729.2017.1389151.

Babic, Milan, Eelke M. Heemskerk and Jan Fichtner. 2018. "Who is more powerful — states or corporations?" The Conversation, July 10. https://theconversation.com/who-is-more-powerful-states-or-corporations-99616.

Barclay, Donald A. 2018. "Confronting the Wicked Problem of Fake News: A Role for Education?" Cicero Foundation Great Debate Paper No. 18/03. www.cicerofoundation.org/wp-content/uploads/Donald_Barclay_Confronting_Fake_News.pdf.

Basedow, Robert and Céline Kauffmann. 2016. "International Trade and Good Regulatory Practices: Assessing The Trade Impacts of Regulation." OECD Regulatory Policy Working Papers No. 4. doi:10.1787/5jlv59hdgtf5-en.

Baye, Michael Roy and Jeffrey Prince. 2020. "The Economics of Digital Platforms: A Guide for Regulators." The Global Antitrust Institute Report on the Digital Economy 34. doi:10.2139/ssrn.3733754.

BBC News. 2019. "Tackle tech giants' 'bullying tactics' review urges." BBC News, March 13. www.bbc.com/news/business-47543107.

Bradshaw, Samantha, Hannah Bailey and Philip N. Howard. *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation*. Oxford, UK: The Computational Propaganda Project at the Oxford Internet Institute, University of Oxford. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/02/CyberTroop-Report20-Draft9.pdf.

Browne, Ryan. 2021. "Google agrees to pay French publishers for news." CNBC, January 21. www.cnbc.com/2021/01/21/google-agrees-to-pay-french-publishers-for-news.html?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioslogin&stream=top.

Burri, Mira. 2013. "Should There Be New Multilateral Rules for Digital Trade?" E15 Expert Group on Trade and Innovation Think Piece. Geneva, Switzerland: International Centre for Trade and Sustainable Development. https://e15initiative.org/publications/should-there-be-new-multilateral-rules-for-digital-trade/.

Burri, Mira and Rodrigo Polanco. 2020. "Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset." *Journal of International Economic Law* 23 (1): 187–220. doi:10.1093/jiel/jgz044.

Canadian Security Intelligence Service. 2018. *Who Said What? The Security Challenges of Modern Disinformation*. World Watch: Expert Notes Series Publication No. 2016-12-05. www.canada.ca/content/dam/csis-scrs/documents/publications/disinformation_post-report_eng.pdf.

Carr, Hope. 2017. "Waging Information Warfare in the 21st Century." *The Three Swords Magazine*, July 17. www.jwc.nato.int/images/stories/_news_items_/2017/InformationWarfare_JWCThreeSwordsJuly17.pdf.

Carvalho, Carlos, Nicholas Klagge and Emanuel Moench. 2011. "The Persistent Effects of a False News Shock." Federal Reserve Bank of New York Staff Reports No. 374.

Cave, Damien. 2021. "An Australia With No Google? The Bitter Fight Behind a Drastic Threat." *The New York Times*, January 23. www.nytimes.com/2021/01/22/business/australia-google-facebook-news-media.html.

Cedar Partners. 2020. *Platform Accountability: Global Challenges & Opportunities*. https://drive.google.com/file/d/1S4MBS8VmKCiqqBXLdANiF4ijaqfvq-mY/view.

Cellan-Jones, Rory. 2017. "Fake news worries 'are growing' suggests BBC poll." BBC News, September 22. www.bbc.com/news/technology-41319683.

Chakravorti, Bhaskar. 2020. "Social media companies are taking steps to tamp down coronavirus misinformation — but they can do more." The Conversation, March 30. https://theconversation.com/social-media-companies-are-taking-steps-to-tamp-down-coronavirus-misinformation-but-they-can-do-more-133335.

Chen, Adrian. 2015. "The Agency." *The New York Times Magazine*, June 7. www.nytimes.com/2015/06/07/magazine/the-agency.html.

Chen, Yongmin, Xinyu Hua and Keith E. Maskus. 2020. "International Protection of Consumer Data." EUI Working Papers RSCAS 2020/42. https://cadmus.eui.eu/bitstream/handle/1814/67583/RSCAS%20 2020_42.pdf?sequence=1&isAllowed=y.

Chernenko, Elena, Oleg Demidov and Fyodor Lukyanov. 2018. "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms." Council on Foreign Relations, February 23. www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

CIGI. 2019. *Models for Platform Governance*. Waterloo, ON: CIGI. www.cigionline.org/models-platform-governance/.

Citron, Danielle Keats. 2015. "Hate Crimes in Cyberspace – Introduction." University of Maryland Legal Studies Research Paper No. 2015-11. https://ssrn.com/abstract=2616790.

Ciuriak, Dan. 2019. *World Trade Organization 2.0: Reforming Multilateral Trade Rules for the Digital Age*. CIGI Policy Brief No. 152. Waterloo, ON: CIGI. www.cigionline.org/publications/world-trade-organization-20-reforming-multilateral-trade-rules-digital-age/.

Cohen, Noam. 2019. "Will California's New Bot Law Strengthen Democracy?" *The New Yorker*, July 2. www.newyorker.com/tech/annals-of-technology/will-californias-new-bot-law-strengthen-democracy.

Communications Security Establishment. 2019. *2019 Update: Cyber Threats to Canada's Democratic Processes*. Ottawa, ON: Government of Canada. https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report_e.pdf.

Crémer, Jacques, Yves-Alexandre de Montjoye and Heike Schweitzer. 2019. *Competition policy for the digital era*. Brussels, Belgium: European Commission. https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

Derakhshan, Hossein and Claire Wardle. 2018. "Information Disorder: Definitions." In *Understanding and Addressing the Disinformation Ecosystem*, 5–12. Philadelphia, PA: Annenberg School for Communication. https://firstdraftnews.org/wp-content/uploads/2018/03/The-Disinformation-Ecosystem-20180207-v4.pdf?x86275.

DiResta, Renée. 2019. "A New Law Makes Bots Identify Themselves — That's the Problem." *Wired*, July 24. www.wired.com/story/law-makes-bots-identify-themselves/.

Donovan, Joan. 2021. "How Social Media's Obsession with Scale Supercharged Disinformation." *Harvard Business Review*, January 13. https://hbr.org/2021/01/how-social-medias-obsession-with-scale-supercharged-disinformation?registration=success.

Durocher, Anthony. 2019. "Competition in the Age of the Digital Giant." Remarks by Anthony Durocher, Deputy Commissioner, Monopolistic Practices, Competition Bureau, Big Data Toronto 2019, June 13. www.canada.ca/en/competition-bureau/news/2019/06/competition-in-the-age-of-the-digital-giant.html.

Dutch Data Protection Authority. 2013. "Canadian and Dutch data privacy guardians release findings from investigation of popular mobile app." News message, January 28. https://cbpweb.nl/en/news/canadian-and-dutch-data-privacy-guardians-release-findings-investigation-popular-mobile-app.

Edmond, Charlotte. 2020. "These are the top risks facing the world in 2020." World Economic Forum, January 15. www.weforum.org/agenda/2020/01/top-global-risks-report-climate-change-cyberattacks-economic-political.

Epps, Tracey. 2008. "Reconciling public opinion and WTO rules under the SPS Agreement." *World Trade Review* 7 (2): 359–92.

Etlinger, Susan. 2019. "What's So Difficult about Social Media Platform Governance?" In *Models for Platform Governance*, 20–25. Waterloo, ON: CIGI.

European Commission. 2020. "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European democracy action plan." COM(2020) 790 final, December 3. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790&from=EN.

Evans, David S. 2020. "The Economics of Attention Markets." SSRN. doi:10.2139/ssrn.3044858.

Ewing, Philip. 2020. "Report: Russian Election Trolling Becoming Subtler, Tougher To Detect." NPR, March 5. www.npr.org/2020/03/05/812497423/report-russian-election-trolling-becoming-subtler-tougher-to-detect.

Fischer, Sara. 2021. "Facebook to downplay politics on its platform." Axios, January 27. www.axios.com/facebook-to-downplay-politics-on-its-platform-78364717-3f52-4cd2-b8e7-8efe6d8f4960.html.

Freeman, Alan. 2017. "Russia should stop calling my grandfather a Nazi, says Canada's foreign minister." *The Washington Post*, March 9. www.washingtonpost.com/news/worldviews/wp/2017/03/09/canadas-foreign-minister-says-russia-is-spreading-disinformation-about-her-grandfather/.

Fried, Daniel. 2019. "Democratic defense against disinformation 2.0." Atlantic Council, June 13. www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation-2-0/.

Frydenberg, Josh and Paul Fletcher. 2020. "News Media and Digital Platforms Mandatory Bargaining Code." Media release, December 8.

Fung, Brian. 2021. "Twitter bets on crowdsourcing to help combat misinformation." CNN Business, January 25. www.cnn.com/2021/01/25/tech/twitter-birdwatch/index.html.

Ghosh, Dipayan, Lindsay Gorman, Bret Schafer and Clara Tsao. 2020. "The Weaponized Web: Tech Policy Through the Lens of National Security." Alliance for Securing Democracy. https://securingdemocracy.gmfus.org/wp-content/uploads/2020/12/The-Weaponized-Web.pdf.

Goldstein, Josh A. and Grossman, Shelby. 2021. "How disinformation evolved in 2020." Brookings TechStream, January 4. www.brookings.edu/techstream/how-disinformation-evolved-in-2020/.

Government of Canada. 2021a. "Paris Call for Trust and Security in Cyberspace." www.canada.ca/en/democratic-institutions/services/paris-call-trust-security-cyberspace.html.

———. 2021b. "Online disinformation." www.canada.ca/en/canadian-heritage/services/online-disinformation.html.

Gu, Lion, Vladimir Kropotov and Fyodor Yarochkin. 2017. "Fake News and Cyber Propaganda: The Use and Abuse of Social Media." Trend Micro, June 13. www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media.

Haggart, Blayne. 2021. "Platform Regulation Is Too Important to Be Left to Americans Alone." Opinion, Centre for International Governance Innovation, January 18. www.cigionline.org/articles/platform-regulation-too-important-be-left-americans-alone/.

Heim, Joe. 2021. "'Disinformation can be a very lucrative business, especially if you're good at it,' media scholar says." *The Washington Post*, January 21. www.washingtonpost.com/lifestyle/magazine/disinformation-can-be-a-very-lucrative-business-especially-if-youre-good-at-it-media-scholar-says/2021/01/19/4c842f06-4a04-11eb-a9d9-1e3ec4a928b9_story.html.

Helbing, Dirk, Bruno S. Frey, Gerd Gigerenzer, Ernst Hafen, Michael Hagner, Yvonne Hofstetter, Jeroen van den Hoven, Roberto V. Zicari and Andrej Zwitter. 2017. "Will Democracy Survive Big Data and Artificial Intelligence?" *Scientific American*, February 25. www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/.

Hern, Alex. 2020. "Online harms bill: firms may face multibillion-pound fines for illegal content." *The Guardian*, December 15. www.theguardian.com/technology/2020/dec/15/online-harms-bill-firms-may-face-multibillion-pound-fines-for-content.

Howard, Philip. 2014. "EAGER: Computational Propaganda and the Production and Detection of Bots." National Science Foundation Grant Proposal, August 1. http://blogs.oii.ox.ac.uk/comprop/wp-content/uploads/sites/93/2015/01/Project-Description.pdf.

Hurst, Daniel. 2020. "Kevin Rudd says Scott Morrison's 'public relations eggbeater' is harming relationship with Beijing." *The Guardian*, December 4. www.theguardian.com/australia-news/2020/dec/05/kevin-rudd-says-scott-morrisons-public-relations-eggbeater-is-harming-relationship-with-beijing.

Hywood, Greg. 2021. "Shrill threats: Google risks losing media fight." *The Sydney Morning Herald*, February 1. www.smh.com.au/business/consumer-affairs/shrill-threats-google-risks-losing-media-fight-20210131-p56y6e.html.

Infield, Tom. 2020. "Americans Who Get News Mainly on Social Media Are Less Knowledgeable and Less Engaged." Pew Charitable Trusts, November 16. www.pewtrusts.org/en/trust/archive/fall-2020/americans-who-get-news-mainly-on-social-media-are-less-knowledgeable-and-less-engaged.

Insikt Group. 2019. *The Price of Influence: Disinformation in the Private Sector*. Recorded Future, September 30. https://go.recordedfuture.com/hubfs/reports/cta-2019-0930.pdf.

Kilic, Burcu. 2021. "Shaping the Future of Multilateralism. Digital trade rules: Big Tech's end run around domestic regulations." Brussels, Belgium: Heinrich-Böll-Stiftung European Union. https://eu.boell.org/index.php/en/2021/05/19/shaping-future-multilateralism-digital-trade-rules-big-techs-end-run-around-domestic.

Knuutila, Aleksi, Lisa-Maria Neudert and Philip N. Howard. 2020. "Global Fears of Disinformation: Perceived Internet and Social Media Harms in 142 Countries." Computational Propaganda Project Data Memo 2020.8. https://demtech.oii.ox.ac.uk/research/posts/global-fears-of-disinformation-perceived-internet-and-social-media-harms-in-142-countries/.

Laslo, Matt. 2019. "The Fight Over Section 230 — and the Internet as We Know It." *Wired*, August 13. www.wired.com/story/fight-over-section-230-internet-as-we-know-it/.

Lerman, Rachel. 2021. "Social media liability law is likely to be reviewed under Biden." *The Washington Post*, January 18. www.washingtonpost.com/politics/2021/01/18/biden-section-230/.

Levush, Ruth. 2019. "Government Responses to Disinformation on Social Media Platforms: Comparative Summary." Library of Congress Law, September. www.loc.gov/law/help/social-media-disinformation/compsum.php.

Lindsay, Jon R. 2015. "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack." *Journal of Cybersecurity* 1 (1): 53–67.

Lipton, David. 2020. "Cybersecurity Threats Call for a Global Response." *IMFBlog* (blog), January 13. https://blogs.imf.org/2020/01/13/cybersecurity-threats-call-for-a-global-response/.

Lynskey, Orla. 2017. "Regulating 'Platform Power.'" LSE Legal Studies Working Paper No. 1/2017. doi:10.2139/ssrn.2921021.

McCabe, David and Ana Swanson. 2019. "U.S. Using Trade Deals to Shield Tech Giants from Foreign Regulators." *The New York Times*, October 7. www.nytimes.com/2019/10/07/business/tech-shield-trade-deals.html.

Meade, Amanda. 2020. "Facebook threatens to block Australians from sharing news in battle over landmark media law." *The Guardian*, September 1. www.theguardian.com/media/2020/sep/01/facebook-instagram-threatens-block-australians-sharing-news-landmark-accc-media-law?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioslogin&stream=top.

Methven O'Brien, Claire, Rikke Frank Jørgensen and Benn Finlay Hogan. 2020. "Tech Giants: Human Rights Risks and Frameworks." SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3768813.

Monteiro, José-Antonio and Robert Teh. 2017. "Provisions on Electronic Commerce in Regional Trade Agreements." WTO Working Paper ERSD-2017-11. www.wto.org/english/res_e/reser_e/ersd201711_e.pdf.

Montgomery, Molly. 2020. "Disinformation as a Wicked Problem: Why We Need Co-Regulatory Frameworks." Brookings Institution, August. www.brookings.edu/wp-content/uploads/2020/08/Montgomery_Disinformation-Regulation_PDF.pdf.

Morar, David and Bruna Martins dos Santos. 2020. "The push for content moderation legislation around the world." Brookings Techtank, September 21. www.brookings.edu/blog/techtank/2020/09/21/the-push-for-content-moderation-legislation-around-the-world/.

Morrison, Sarah, Belinda Barnet and James Martin. 2020. "China's disinformation threat is real. We need better defences against state-based cyber campaigns." The Conversation, June 23. https://theconversation.com/chinas-disinformation-threat-is-real-we-need-better-defences-against-state-based-cyber-campaigns-141044.

Nadel, Evan and Natalie Prescott. 2019. "Legal Implications of Using AI, Biometrics, or Bots in the Workplace." The Bureau of National Affairs, Inc., December 3. www.mintz.com/sites/default/files/media/documents/2019-12-03/LegalImplicationsofUsingAI-ECO29364.pdf.

National Endowment for Democracy. 2017. "Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and 'Fake News.'" National Endowment for Democracy, October 17. www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news/.

Needham, Kirsty. 2020. "China tweet that enraged Australia propelled by 'unusual' accounts, say experts." Reuters, December 5. www.reuters.com/article/us-australia-china-tweet/china-tweet-that-enraged-australia-propelled-by-unusual-accounts-say-experts-idUSKBN28E0YI.

Nemr, Christina and William Gangware. 2019. *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age*. Park Advisors. www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf.

Newman, Lily Hay. 2016. "Hacker Lexicon: What Is the Attribution Problem?" *Wired*, December 24. www.wired.com/2016/12/hacker-lexicon-attribution-problem/?.

Nugent, Clara. 2018. "France Is Voting on a Law Banning Fake News. Here's How it Could Work." *Time*, June 7. https://time.com/5304611/france-fake-news-law-macron/.

Nyst, Carly and Nick Monaco. 2018. *State-Sponsored Trolling: How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns*. Palo Alto, CA: Institute for the Future. www.iftf.org/fileadmin/user_upload/images/DigIntel/IFTF_State_sponsored_trolling_report.pdf.

OECD. 2006. "OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam." 1133rd sess. April 13. www.oecd.org/sti/ieconomy/oecdrecommendationoncross-borderco-operationintheenforcementoflawsagainstspam.htm.

———. 2016. "Economic and Social Benefits of Internet Openness." OECD Digital Economy Papers No. 257. Paris, France: OECD Publishing. doi:10.1787/5jlwqf2r97g5-en.

———. 2019. *An Introduction to Online Platforms and Their Role in the Digital Transformation*. Paris, France: OECD Publishing. www.oecd.org/innovation/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation-53e5f593-en.html.

———. 2020. *Abuse of Dominance in Digital Markets*. Paris, France: OECD. www.oecd.org/daf/competition/abuse-of-dominance-in-digital-markets-2020.pdf.

Office of the High Commissioner for Human Rights. 2017. "Joint Declaration on Freedom of Expression and 'Fake News,' Disinformation and Propaganda." www.ohchr.org/Documents/Issues/Expression/JointDeclaration3March2017.doc.

———. 2021. *Disinformation and freedom of opinion and expression: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan*. 47th sess. A/HRC/47/25. https://undocs.org/A/HRC/47/25.

Osborne, Charlie. 2019. "Bad bots now make up 20 percent of web traffic." ZDNet, April 17. www.zdnet.com/article/bad-bots-focus-on-financial-targets-make-up-20-percent-of-web-traffic/.

Owens, James. 2019. "The tech giants dominated the decade. But there's still time to rein them in." *The Guardian*, December 25. www.theguardian.com/commentisfree/2019/dec/25/2010s-tech-giants-google-amazon-facebook-regulators.

Petre, Caitlin, Brooke Erin Duffy and Emily Hund. 2019. "'Gaming the System': Platform Paternalism and the Politics of Algorithmic Visibility." *Social Media and Society* 5 (4). doi:10.1177/2056305119879995.

Pierce, Brian. n.d. "A Wicked Problem About Thinking: Cognitive Security." Media at Stanford University. https://mediax.stanford.edu/program/thinking-tools-for-wicked-problems/a-wicked-problem-about-thinking-cognitive-security/.

Pisa, Michael, Pam Dixon and Benno Ndulu. 2021. "Addressing Cross-Border Spillovers in Data Policy: The Need for a Global Approach." *Center for Global Development* (blog), February 3. www.cgdev.org/blog/addressing-cross-border-spillovers-data-policy-need-global-approach.

Price, Rande. 2019. "Disinformation is profitable. That needs to change." *Digital Content Next* (blog), August 21. https://digitalcontentnext.org/blog/2019/08/21/disinformation-is-profitable-that-needs-to-change/.

Reuters. 2017. "French election contender Macron is Russian 'fake news' target: party chief." Reuters, February 13. www.reuters.com/article/us-france-election-cyber/french-election-contender-macron-is-russian-fake-news-target-party-chief-idUSKBN15S192.

Riley, Michael, Lauren Etter and Pradhan Bibhudatta. 2018. "A Global Guide to State-Sponsored Trolling." Bloomberg, July 19. www.bloomberg.com/features/2018-government-sponsored-cyber-militia-cookbook/.

Rossolillo, Nicholas. 2021. "Better Buy: Facebook vs. Google." The Motley Fool, January 25. www.fool.com/investing/2021/01/25/better-buy-facebook-vs-google/.

Ruggie, John Gerard. 1982. "International Regimes, Transactions, and Change: Embedded Liberalism in the Postwar Economic Order." *International Organization* 36 (2): 379–415.

Ryan, Camille D., Andrew J. Schaul, Ryan Butner and John T. Swarthout. 2020. "Monetizing disinformation in the attention economy: The case of genetically modified organisms (GMOs)." *European Management Journal* 38 (1): 7–18. doi:10.1016/j.emj.2019.11.002.

Scott, Mark, Thibault Larger and Laura Kayali. 2020. "Europe rewrites rulebook for digital age." *Politico*, December 15. www.politico.eu/article/europe-digital-markets-act-services-act-tech-competition-rules-margrethe-vestager-thierry-breton/.

Singh, Preeti. 2021. "Inside the Pro-Huawei Influence Campaign." *The New York Times*, January 29. www.nytimes.com/2021/01/29/technology/commercial-disinformation-huawei-belgium.html.

Smeets, Maarten, ed. 2021. *Adapting to the digital trade era: challenges and opportunities*. Geneva, Switzerland: WTO Publications. www.wto.org/english/res_e/booksp_e/adtera_e.pdf.

Smith, Victoria. 2020. "Mapping Worldwide Initiatives to Counter Influence Operations." Carnegie Endowment for International Peace, December 14. https://carnegieendowment.org/2020/12/14/mapping-worldwide-initiatives-to-counter-influence-operations-pub-83435.

Snower, Dennis and Paul Twomey. 2020. "Humanistic Digital Governance." Social Macroeconomics Working Paper. www.bsg.ox.ac.uk/research/publications/humanistic-digital-governance.

Stoller, Matt. 2021. "Take the Profit Out of Political Violence." Big by Matt Stoller, January 19. https://mattstoller.substack.com/p/take-the-profit-out-of-political.

Talihärm, Anna-Maria. n.d. "Towards Cyberpeace: Managing Cyberwar Through International Cooperation." UN Chronicle. www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation.

Tech Observer. 2020. "After GDPR, EU now goes after bots and data harvesters." Tech Observer, January 8. https://techobserver.in/2020/01/08/after-gdpr-eu-now-goes-after-bots-and-data-harvesters/.

Technology and Social Change Team. 2021. "Disinformation at Scale Threatens Freedom of Expression Worldwide." Comment to Irene Khan, Special Rapporteur on the promotion and protection of the right to freedom of expression. https://mediamanipulation.org/sites/default/files/2021-02/Donovan-et-al-TaSC-Comment.pdf.

The Washington Post. 2021. "Opinion: Facebook and Twitter can do something about deceptive news. So why don't they?" *The Washington Post*, February 1. www.washingtonpost.com/opinions/facebook-and-twitter-can-do-something-about-deceptive-news-so-why-dont-they/2021/02/01/da702e0e-626a-11eb-afbe-9a11a127d146_story.html.

Tucker, Joshua A., Andrew Guess, Pablo Barbera, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal and Brendan Nyhan. 2018. "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature." SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144139.

Tworek, Heidi. 2021. "The Dangerous Inconsistencies of Digital Platform Policies." Opinion, Centre for International Governance Innovation, January 13. www.cigionline.org/articles/dangerous-inconsistencies-digital-platform-policies.

UK Information Commissioner's Office. 2019. "Adtech Phase 2: Key Findings." https://ico.org.uk/media/about-the-ico/documents/2616754/fff2-info-gathering-201912.pdf.

United Nations Conference on Trade and Development. 2019. "Global efforts needed to spread digital economy benefits, UN report says." United Nations Conference on Trade and Development, September 4. https://unctad.org/news/global-efforts-needed-spread-digital-economy-benefits-un-report-says.

University of Baltimore and CHEQ. 2019. *The Economic Cost of Bad Actors on the Internet*. https://s3.amazonaws.com/media.mediapost.com/uploads/EconomicCostOfFakeNews.pdf.

US Department of the Treasury. 2017. "Cyber-Related Sanctions Program." Office of Foreign Assets Control, July 3. https://home.treasury.gov/system/files/126/cyber.pdf.

Vigneault, David. 2021. "Remarks by Director David Vigneault to the Centre for International Governance Innovation." Canadian Security Intelligence Service speech, February 9. www.canada.ca/en/security-intelligence-service/news/2021/02/remarks-by-director-david-vigneault-to-the-centre-for-international-governance-innovation.html.

Wakabayashi, Daisuke, Karen Weise, Jack Nicas and Mike Isaak. 2020. "The economy is in record decline, but not for the tech giants." *The New York Times*, July 30. www.nytimes.com/2020/07/30/technology/tech-company-earnings-amazon-apple-facebook-google.html.

Wardle, Claire and Hossein Derakhshan. 2017. *Information Disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe Report DGI(2017)09. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c.

Weaver, Nicholas. 2013. "Our Government Has Weaponized the Internet. Here's How They Did It." *Wired*, November 13. www.wired.com/2013/11/this-is-how-the-internet-backbone-has-been-turned-into-a-weapon/.

Wojcik, Stefan, Solomon Messing, Aaron Smith, Lee Rainie and Paul Hitlin. 2018. "Bots in the Twittersphere." Pew Research Center. www.pewresearch.org/internet/2018/04/09/bots-in-the-twittersphere/.

Wong, Julia Carrie. 2021. "Banning Trump won't fix social media: 10 ideas to rebuild our broken internet — by experts." *The Guardian*, January 16. www.theguardian.com/media/2021/jan/16/how-to-fix-social-media-trump-ban-free-speech.

World Economic Forum. 2011. *Personal Data: The Emergence of a New Asset Class*. Geneva, Switzerland: World Economic Forum. January. www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

———. 2020. "A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy." White Paper. Geneva, Switzerland: World Economic Forum. www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf.

WTO. 2020. *World Trade Report 2020: Government policies to promote innovation in the digital age*. Geneva, Switzerland: WTO Publications. www.wto.org/english/res_e/booksp_e/wtr20_e/wtr20_e.pdf.

Wu, Mark. 2017. *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System*. Geneva, Switzerland: International Centre for Trade and Sustainable Development.

Yakovleva, Svetlana. 2020. "Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy." *University of Miami Law Review* 74 (2): 416–519.

Zhao, Lijian. 2020. "Shocked by murder of Afghan civilians & prisoners by Australian soldiers. We strongly condemn such acts, &call for holding them accountable" (Twitter thread). Twitter, November 29, 8:02 p.m. https://twitter.com/zlj517/status/1333214766806888448.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY: PublicAffairs.

———. 2021. "The Coup We Are Not Talking About." *The New York Times*, January 29. www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline