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

Can Trade Agreements Solve the Wicked Problem of Disinformation

IIEP-WP-2021-12

Susan Aaronson
George Washington University

April 2021

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

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

Draft for CIGI, February 3, 2021

Susan Ariel Aaronson[1]

Introduction

Disinformation is not like pornography; most of us don't 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 (Park Advisors: 2019). Moreover, unlike pornography, disinformation is dangerous to individuals, democracy, and good governance.

An international network of users, firms, and policymakers maintains and disseminates 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 browsers provide their services to netizens for free. Hence these firms depend on ads for revenues and profits.[4] After users provide personal data (their interests or search history), these firms aggregate it and use that aggregated information to provide users with both tailored advertising and free content (Amnesty: 2019, Zuboff: 2021).

Critics accuse many 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: 2021). Meanwhile, the ads provide the firms with a global revenue stream that both incentives and sustains the spread of disinformation. As example, the Global Disinformation Index found that local ads for Bosch, the World Health Organization and the Wall Street Journal, delivered by Google and Amazon, appeared on sites spreading anti-Semitic narratives and conspiracy theories.[5] The Global Disinformation Index also found ads promoting the American Cancer Society,

[1] I am grateful to Andrew Kraskewicz, a master's student at GWU, for his help with this project. Stephanie Honey, Patrick Leblond, Ian Wheeler, Josh Melzer and Mark Froese read early drafts and made helpful suggestions. Participants in a seminar at European University Institute also made helpful suggestions.

[2] In 1964, US Supreme Court Justice Potter Stewart tried to explain "hard-core" pornography, by saying, "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 ..." https://corporate.findlaw.com/litigation-disputes/movie-day-at-the-supreme-court-or-i-know-it-when-i-see-it-a.html

[3] As example, in 2018 some 40% of Facebook users get their news from the platform. https://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/ https://www.accc.gov.au/media-release/lack-of-competition-in-ad-tech-affecting-publishers-advertisers-and-consumers

[4] Digital advertising is, in essence, how consumers' attention and data are monetized.

[5] Global Disinformation Index, https://disinformationindex.org/wp-content/uploads/2020/10/Oct-2nd-DisinfoAds-Brands-next-to-Anti-SemitismGlobalist-Conspiracy-theories.pdf

UNICEF, and Doctors without Borders appeared on sites with disinformation about COVID 19.[6] The Washington Post argued in a recent editorial, "Platforms have no excuse not to do something about the problem. They've already showed us they know how."[7] But these companies are reluctant to change their business model because it is so profitable.[8]

Disinformation is not a new phenomenon. Individuals, organizations, and governments have spread propaganda, fake news, and conspiracy theories offline for centuries (Wardle and Derakshan: 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."[9] According to Shoshana Zuboff, advertisers use that data to manipulate us to think, buy, believe, do, or join something that we otherwise would not have done.[10]

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 we can see mounting qualitative evidence that disinformation increasingly crosses borders (Park Advisors: 2019; Office of the High Commissioner for Human Rights: 2020).

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 David Pierce, the 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."[11] No one knows how best to counter disinformation at the local, national, or international levels (Tucker et al 2018)

---

[6] Global Disinformation Inex, https://disinformationindex.org/wp-content/uploads/2020/12/Dec_4_2020-DisinfoAds-NGO-_-Charities-Disinformation-1.pdf

[7] Editorial Board, Opinion: Facebook and Twitter can do something about deceptive news. So why don't they? Washington Post, February 1, 2022, https://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

[8] https://www.nytimes.com/2020/07/30/technology/tech-company-earnings-amazon-apple-facebook-google.html; https://www.fool.com/investing/2021/01/25/better-buy-facebook-vs-google/

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

[10] Shoshana Zuboff, The Coup we Are Not Discussing, New York Times, January 29, 2021, https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html; and Hello World, Dispatches from Editor-in-Chief Julia Angwin, Hello World, This Week Understanding the Threat of "Surveillance Capitalism" e-mail newsletter, February 13, 2021.

[11] David Pierce, "A Wicked Problem About Thinking: Cognitive Security," ND, https://mediax.stanford.edu/program/thinking-tools-for-wicked-problems/a-wicked-problem-about-thinking-

Not surprisingly, people are worried about disinformation. A 2018 poll from BBC News in 18 countries found 79% of respondents said they worried about what was fake and what was real on the internet.[12] CIGI surveyed some 20,000 netizens around the world and in 2019, found social media companies are the leading source of user distrust in the internet – surpassed only by cybercriminals – with 75% of those surveyed citing Facebook, Twitter, and other social media platforms as contributing to their lack of trust.[13] In a December 2020 study, the Oxford Internet Institute analyzed survey data of 154,195 participants living in 142 countries found that more than half (53%) of regular internet users are concerned about disinformation. The researchers also found that worries about the impact of disinformation is highest in North America and Europe and lowest in East and South Asia (Knuutila, Neudert and Howard: 2020).

Consequently, many nations have adopted a wide range of strategies to mitigate disinformation, including platform regulation, personal data protection rules, competition policies, investment rules, technological fixes, and citizen education strategies. With so many different approaches, policymakers 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 upon internet openness and generativity (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. Firms may be trying to game the system (European Commission: 2021).

Herein we argue that trade agreements might provide a means to address cross-border disinformation flows and the nexus between domestic and international data governance. The internet is built on data flows that often cross-borders. When a netizen uses a dating app, searches for information on COVIDi-19 or watches a movie on Netflix, he or she is engaging in international trade. To provide the user with that 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 (Gonzalez: 2019). In recent years, trade diplomats have included

cognitive-security/ Cognitive security is the application of AI technologies patterned on human thought processes to detect threats and protect physical and digital systems.

[12] Rory Cellan-Jones, Fake news worries 'are growing' suggests BBC poll, BBC News, September 27, 2017, http://www.bbc.com/news/technology-41319683

[13] CIGI, 2019 CIGI-Ipsos Global Survey on Internet Security and Trust, June 2019, https://www.cigionline.org/internet-survey-2019. The survey 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, Russia, South Africa, Republic of Korea, Sweden, Tunisia, Turkey and the United States.

rules to govern these cross-border data flows in a growing number of trade agreements.

However, trade agreements have their limitations. They can't be used to directly regulate the business model that underpins the problem of disinformation, but they could facilitate greater coordination of national strategies to counter it. Moreover, many people have deep concerns about the role of trade agreements in the global economy. They note that trade agreements are negotiated in an opaque process that is indirectly democratic, time consuming, and out of sync with the digital economy. As example, the members of the WTO for years have participated in a work programme 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 US) dominate and are home to the main firms relying on this business model (Aaronson and Struett: 2020; Aaronson: 2019). Given that market dominance, many nations want to establish their own digital sectors and establish rules before they commit to negotiations (Aaronson and Struett: 2020).

But here's where trade agreements might 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 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. Policymakers could build on that language.

Moreover, trade agreements include useful language on competition policy, as well provisions designed to ensure that national regulation does not lead to trade distortions. Policymakers include these provisions in the hopes of facilitating regulatory coordination and preventing a race to the bottom on regulation (WTO: 2021a, 160,168).

The article proceeds as follows: We first define disinformation and illuminate how technological change and market forces are facilitating its spread. We show how the business model that underpins many digital firms challenges regulators at the national level. We then discuss what trade agreements say about data flows, exceptions, competition policy, regulatory coherence, and spam. Finally, we present

suggestions on a broader approach to govern cross-border information that nations can use within trade agreements.[14]

Moreover, we note that disinformation is one of several negative spillovers of a shared internet. Policymakers should be anticipating such problems and working towards strategies to address these spillover effects, just as they invented embedded liberalism as a means of addressing the national spillovers of globalization (Ruggie: 1982; Yakoleva: 2019).

What is Disinformation and what how does it affect the global economy?

Disinformation can be defined as 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.[15] *Disinformation* is widely defined as the purposeful dissemination of false information *intended* to mislead or harm.[16] Some call disinformation computational propaganda because increasingly disinformation is deliberately spread by individuals who rely on algorithms, automation, and human curation to deliberately spread false information .[17] Although states have similar definitions of disinformation they have different views on how best to address it.[18]

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

[14] Europe is calling for a shared approach. https://ec.europa.eu/info/sites/info/files/joint-communication-eu-us-agenda_en.pdf

[15] Hossein Derakhshan and Clair Wardle, "Information Disorder: Definitions" in Understanding and Addressing the Disinformation Ecosystem, Annenberg School for Communications workshop, 15-16 December 2017, pp. 5-12, https://firstdraftnews.org/wp-content/uploads/2018/03/The-Disinformation-Ecosystem-20180207-v2.pd

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

[17] https://comprop.oii.ox.ac.uk/

[18] As example, the EU 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 2020b, p. 13. Canada describes it as "false, misleading and inflammatory." https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html

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). However, although disinformation has a corrosive effect on democracy, policymakers 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: 2020) UN Human Rights bodies have made it clear that state actors should not make, sponsor, encourage or disseminate disinformation (Office of the High Commissioner: 2017. pp. 1, 3; O'Brien et al: 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 hyper partisan insults. These efforts aim to intimidate and silence targeted individuals—most often journalists, activists, human rights defenders, and vocal members of opposition coalitions. (Riley et al. 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 IoT (internet of things), and other data driven technologies (NIST, 2018). According to one study, "personalized information builds a "filter bubble" around us, a kind of digital prison for our thinking." In so doing, it could suppress creative and "out of the box" thinking which in turn have spillover economic affects (Heibing et al: 2017).

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 et al; 2010; Insikt Group: 2019), alter economic decisions;[19] 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 78 billion USD, including $9 billion in unnecessary healthcare 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 trying to repair damaged reputations due to fake news (University of Baltimore and Cheq: 2019).

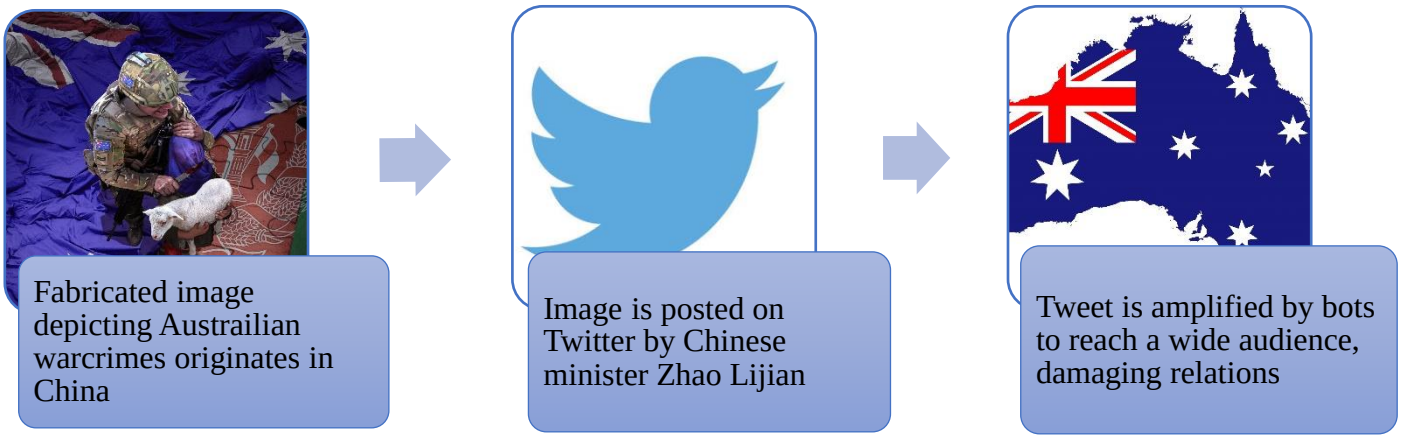
If policymakers could develop a coordinated and effective international approach, they could possibly reduce these costs. A recent study found that unilateral data regulations can either raise or reduce global welfare, but a coordinated approach would yield substantial gains (Chen, Hua, and Maskus: 2020, 4). Policymakers have a

[19] https://www.nytimes.com/2021/01/29/technology/commercial-disinformation-huawei-belgium.html

long history of trying to develop a coordinated approach on other issues such as environmental protection and labor rights (Aaronson and Zimmerman: 2007). Some have also tried to develop a coordinated approach to the governance of cyberspace and cyber threats.[20]

Recent Examples of Cross-border Disinformation

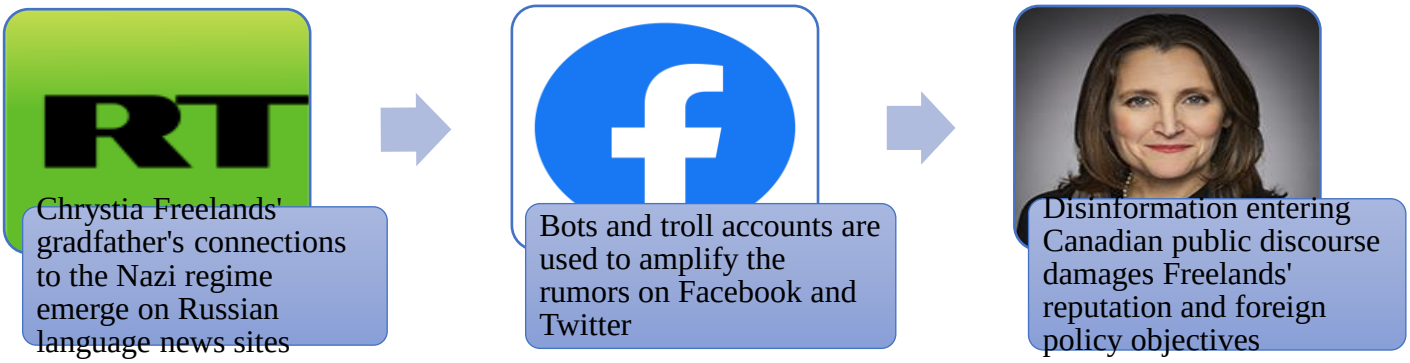
a. China's Disinformation about Australian alleged Atrocities in Afghanistan



Source: https://twitter.com/zlj517/status/1333214766806888448; Kirsty Needham, "Chinese official's 'repugnant' tweet of Australia soldier likely amplified by fake accounts, experts say," Reuters, December 5; https://www.reuters.com/article/us-australia-china-tweet/china-tweet-that-enraged-australia-propelled-by-unusual-accounts-say-experts-idUSKBN28E0YI ; Daniel Hurst, Kevin Rudd says Scott Morrison's 'public relations eggbeater' is harming relationship with Beijing, The Guardian, December 4,https://www.theguardian.com/australia-news/2020/dec/05/kevin-rudd-says-scott-morrisons-public-relations-eggbeater-is-harming-relationship-with-beijing

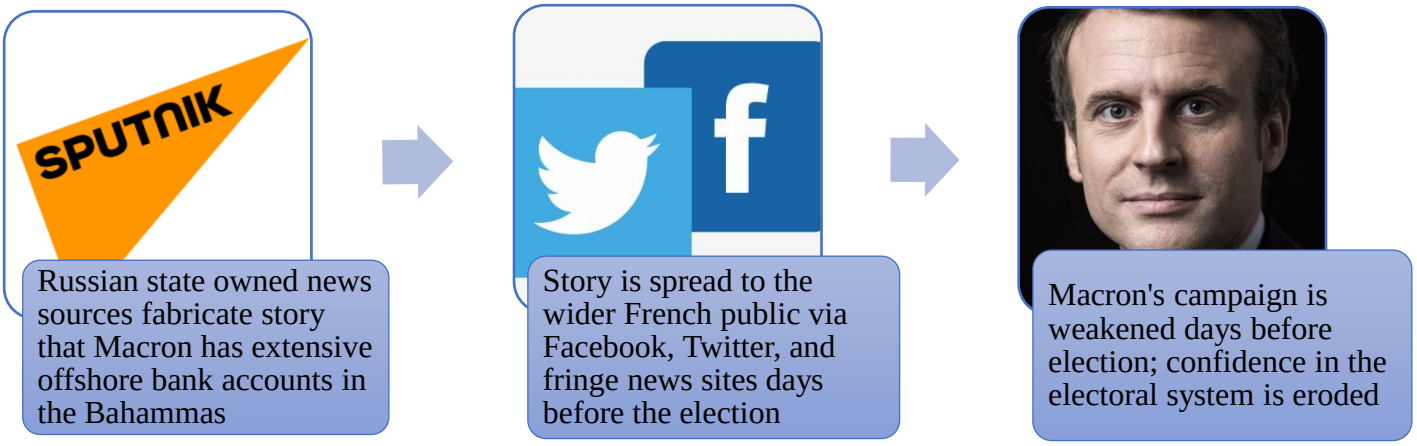
b. Russian Disinformation about former Canadian Prime Minister Freeland

[20] https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms; https://blogs.imf.org/2020/01/13/cybersecurity-threats-call-for-a-global-response/; andhttps://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation



Sources: Hope Carr, "Waging Information Warfare in the 21st Century", The Three Swords Magazine, 2017, pp 36-37; https://www.jwc.nato.int/images/stories/_news_items_/2017/InformationWarfare_JWCThreeSwordsJuly17.pdf; Alan Freeman, "Russia Should Stop Calling My Grandfather a Nazi, Says Canadas Foreign Minister", The Washington Post, march 9, 2017; https://www.washingtonpost.com/news/worldviews/wp/2017/03/09/canadas-foreign-minister-says-russia-is-spreading-disinformation-about-her-grandfather/

c. Russian Disinformation about French President Macron



Sources: Ciara Nugent, "France is Voting on a Law Banning Fake News. Here's How it Could Work", Time, June 7, 2018; https://time.com/5304611/france-fake-news-law-macron/ and Reuters, "French election contender Macron is Russian 'fake news' target: party chief", February 13, 2017, https://www.reuters.com/article/us-france-election-cyber/french-election-contender-macron-is-russian-fake-news-target-party-chief-idUSKBN15S192

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 reported half of all advanced democracies holding national elections had their democratic process targeted by cyber threat activity, a three-fold increase since 2015 (Canada: 2020a). 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 or it could use bots or trolls. Alternatively, 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; Lindsey: 2016).

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 (IRA) initiated its efforts to interfere in US politics as early as 2014. This privately held Russian company owned by a friend of 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 (US Department of Justice: 2018). In 2020, researchers at 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, p.1). 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 to influence policy changes on trade agreements, impact elections, or change the course of a referendum.[21]

What role do platforms and their business model play in fostering dissemination across borders?

The purveyors of disinformation rely on websites, apps, and social networks etc. 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

[21] ion Gu, Vladimir Kropotov & Fyodor Yarochkin, Fake News and Cyber Propaganda: The Use And Abuse of Social Media, TREND MICRO (June 13, 2017), https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media

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 (Lynsky: 2017). But these users are being 'used.'[22] After collecting this data, the platforms aggregate users into groups divided by preferences, race, location, income etc.. Many data firms then make and sell predictions about users' interests, characteristics, and ultimately behavior to generate advertising revenue (Zuboff: 2019; Amnesty: 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 this news. It is also affected by the design of the platform's algorithm that provide users with content that might convince them to stay on the site and focus their attention (Cave: 2021; UK Information Commissioner's Office: 2019, and Bannon and Singh: 2021) It is important to note that attention is a limited resource and firms, and individuals compete for users' attention (Ryan et al: 2019). Hence platforms have incentives to design their algorithms to maintain their users' attention for as long as possible (CIGI: 2019). In so doing they can achieve economies of scale and scope from the content they provide s well as the ads they tailor to users.[23] As example, a search engine like Bing or Chrome can include both results (content) and paid search ads (Evans: 2020: Global Disinformation Index; 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. They also gamify it, putting 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 and Ryan et al. 2019).

Many of the large platforms are under extreme public pressure to moderate content and change their business model. But that's not necessarily what shareholders want. As CIGI Senior Fellow Susan Etlinger notes, "social media companies' mission

[22]https://unctad.org/news/global-efforts-needed-spread-digital-economy-benefits-un-report-saysrchers at the Brown Institute of Columbia University have shown that, Amazon, Apple, Facebook, and Google collect over 450 different items of information about their users. See https://brown.columbia.edu/mapping-data-flows/

[23] 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)

statements focus on sharing, community and empowerment. But their business models and stock prices are built on their ability to grow, as measured in attention and engagement metrics: active users, time spent, content shared" (Ettlinger: 2019, 24).

Not surprisingly, disinformation seems quite profitable (Ryan et al: 2020). In 2019, the Global Disinformation Institute 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. [24] Harvard scholar Joan Donavan described disinformation as "a lucrative business especially if you are good at it" (Heim: 2021).

In addition, this business model can create competition problems and hence problems for regulators. As the European Commission noted, 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. Much of what firms do and supply, demand and pricing conditions are opaque to regulators (European Commission: 2021, 3-4).

Meanwhile, researchers struggle to show that consumers are hurt by the freemium model. But consumers have little market power. They can't "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: 2019, 157)

Platforms have and continue to receive significant revenue from this business model, which in turn gives them influence.. Some of the largest platforms have revenues significantly larger than many governments.[25] 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 et al. 2017). As example, in 2019, the British government reviewed the business practices of the digital behemoths and described their behavior towards consumers and to forestall regulation as "bullying."[26] As example, in 2020, reports emerged that Facebook saw

[24] The Global Disinformation Institute is a nonprofit that evaluates and rates websites' risk of spreading disinformation. Rande Price, "Disinformation is profitable, that needs to change," August 21, https://digitalcontentnext.org/blog/2019/08/21/disinformation-is-profitable-that-needs-to-change/ .

[25] https://theconversation.com/who-is-more-powerful-states-or-corporations-99616; https://www.theguardian.com/commentisfree/2019/dec/25/2010s-tech-giants-google-amazon-facebook-regulators

[26] BBC, Tackle tech giants' 'bullying tactics' review urges, March 13, 2019, https://www.bbc.com/news/business-47543107

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, The Trump Administration decided to ban the app and encourage its sale to a US company .[27] In 2021, both Google and Facebook's threatened to leave Australia after the government proposed requiring major platforms to pay for news they link to.[28] 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 pre-trained 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; Cloudflare: 2020; Howard"2-14).

Bots are not inherently bad. Some bots can do good things, such as search engine bots (web crawlers) that index content for search 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 upon humans and society (Cloudflare: 2020). Moreover, some bots are designed to amplify the reach of disinformation and exploit the vulnerabilities that stem from our

[27] https://www.pbs.org/newshour/politics/biden-backs-off-on-tiktok-ban-in-review-of-trump-china-moves

[28] Here is the Australian "bargaining code: https://ministers.treasury.gov.au/ministers/josh-frydenberg-2018/media-releases/news-media-and-digital-platforms-mandatory-bargaining?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioslogin&stream=top On Google leaving Australia, see https://about.google/google-in-australia/an-open-letter/; Facebook, https://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 and response https://www.smh.com.au/business/consumer-affairs/shrill-threats-google-risks-losing-media-fight-20210131-p56y6e.html. ILt is interesting to note that Google is paying for news in France. https://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 The law is based on the EU copyright directive.

cognitive and social biases. In so doing, they create the illusion that individuals have independently agreed that information is correct (Wardle and Derakhstan: 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 color in response to their views, spam-bots can exacerbate highly problematic trends of online hate speech and abuse (Citron: 2015). Using 2017 data, the Pew Research Center estimated that between 9 percent 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 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 US, followed by the Netherlands and China (Osborne: 2019).

Policymakers are starting to regulate spam- bots used to disseminate disinformation (they already regulate bots used for mass ticket/scalping purposes.)[29] California became the first state to require bots to openly identify 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 to make a purchase or sale of goods or services or to influence a vote in an election. Under the law, all such bots must conspicuously declare themselves. The owner or creator of the bot and 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.[30] But the law is broad and vague includes chat bots on companies' websites, and provides no private right of action. In short individuals can't sue to challenge bots, only the state can (Nadel and Prescott: 2019, 4). Senator Feinstein has introduced a similar bill in the Senate, but it has not moved pass committee.[31]

---

[29] (Pub.L. 114-274, S.3183, commonly referred to as the BOTS Act) was signed into federal law on December 14, 2016

[30] The bill is at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001 https://www.wired.com/story/law-makes-bots-identify-themselves/; and https://www.newyorker.com/tech/annals-of-technology/will-californias-new-bot-law-strengthen-democracy

[31] 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.
"S. 2125 — 116th Congress: Bot Disclosure and Accountability Act of 2019." www.GovTrack.us. 2019. February 6, 2021 <https://www.govtrack.us/congress/bills/116/s2125>

Meanwhile, the EU has banned ticketing bots, and is considering challenging spam and chatbots that spread disinformation.[32]

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 US sits on one side of a continuum, where law and culture dictate that there should be relatively few restrictions on speech and government plays a limited role in regulating social networks. US policies are guided by Section 230 of the 1996 Communications and Decency Act which says that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. The protected intermediaries include not only regular Internet Service Providers (ISPs), but also a range of "interactive computer service providers," including basically any online service that publishes third-party content from Target, Yelp, or Amazon to Trip Advisor. [33]

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

But most countries don't have sufficient leverage to influence the practices of the platforms, unless they are large and growing data markets such as India. Moreover, many netizens don't 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.[34] As Canadian scholar Blayne Haggart 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 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." (Haggart: 2021).

[32] https://techobserver.in/2020/01/08/after-gdpr-eu-now-goes-after-bots-and-data-harvesters/
[33] https://uscode.house.gov/view.xhtml?req=(title:47%20section:230%20edition:prelim)
And https://www.eff.org/issues/cda230. The Trump Administration proposed several reforms.
https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996
[34] https://www.nytimes.com/2019/10/07/business/tech-shield-trade-deals.html

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, the Network Enforcement Act (NetzDG).[35] while the UK and Australia require firms to remove "online harms." [36] The EU just tabled new legislation to increase the accountability of online platforms and clarify the rules for taking down illegal content. Courts and laws rather than individual firms will decide what is legal and when content should be blocked. [37] 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.[38]

Around the world, policymakers[39] (and firms[40]) 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, the US Department of Defense Advanced Research Projects Agency (DARPA) spent $68 million trying to find a technological solution for spotting manipulated fake videos. It also funded the Enhanced Attribution program 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[41]. 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,

[35] https://www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG_node.html

[36] https://www.theguardian.com/technology/2020/dec/15/online-harms-bill-firms-may-face-multibillion-pound-fines-for-content

[37] https://www.politico.eu/article/europe-digital-markets-act-services-act-tech-competition-rules-margrethe-vestager-thierry-breton/

[38] https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html: Library of Congress, Government Responses to Disinformation on Social Media Platforms: Canada, 2019, https://www.loc.gov/law/help/social-media-disinformation/canada.php

[39] Here is a listing of national laws regarding fake news https://www.reuters.com/article/us-singapore-politics-fakenews-factbox/factbox-fake-news-laws-around-the-world-idUSKCN1RE0XN

[40] As example, Twitter is asking some of its users to point out disinformation (to crowdsource it). https://www.cnn.com/2021/01/25/tech/twitter-birdwatch/index.html?bt_ee=fzNssD67tONL%2B6XKocxD6pIR7KzJ7ZRyaSpXYdK4Tt0D6a8MLR2%2FaoG25sc1hGD9&bt_ts=1611634136462; while Facebook is trying to make its campaign advertising business more transparent and making tweaks to its algorithms to support verified news and to curb political advertising during times of political volatility. https://www.axios.com/facebook-to-downplay-politics-on-its-platform-78364717-3f52-4cd2-b8e7-8efe6d8f4960.html?stream=technology&utm_source=alert&utm_medium=email&utm_campaign=alerts_technology. Also see Bhaskar Chakravorti, "Social media companies are taking steps to tamp down coronavirus misinformation — but they can do more," The Conversation, March 30, 2020, https://theconversation.com/social-media-companies-are-taking-steps-to-tamp-down-coronavirus-misinformation-but-they-can-do-more-133335.

[41] https://www.darpa.mil/program/enhanced-attribution

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 et al. 2020, and Cave: 2021).[42]

Given this patchwork of approaches, policymakers (and executives) recognize the need for collective action. The members of the G7 who met in Canada in June 2018 agreed to the "Charlevoix Commitment on Defending Democracy from Threats." The G7 agreed to "Establish a G7 Rapid Response Mechanism [RRM] to strengthen our coordination to identify and respond to diverse and evolving threats to our democracies, including through sharing information…"[43] At the initiative of France, some 95 nations have banded together to discuss effective solutions to the problems of disinformation and cyber-insecurity (Canada 2020b)

However, these strategies can do little to mitigate cross-border disinformation flows or prod firms to address some of the problems with their current business model. As with labor and environment, uncoordinated national strategies to address the problem could lead to a race to the bottom among some nations to encourage firms to locate in their countries. Trade agreements, especially at the regional and binational level increasingly contain rules that could lead to a more coordinated international approach to directly tackle cross-border disinformation. The next section delineates what trade agreements currently say and how that might 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 2020 World Trade Report, the WTO Secretariat noted a catch 22 in the global economy. On 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: 2021b, 11-12).

[42] The Carnegie Endowment for International Peace, the Washington Post and The Guardian recently published descriptions of innovative ideas to address disinformation. This think tank, CIGI, published a whole book on it https://carnegieendowment.org/2020/12/14/mapping-worldwide-initiatives-to-counter-influence-operations-pub-83435; https://www.theguardian.com/media/2021/jan/16/how-to-fix-social-media-trump-ban-free-speech?CMP=Share_iOSApp_Other&__twitter_impression=true&s=03; 'Joe Heim, "Disinformation can be a very lucrative business, especially if you're good at it,' media scholar says," Washington Post, January 19, 2021, and CIGI, https://www.cigionline.org/sites/default/files/documents/Platform-gov-WEB_VERSION.pdf

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

The Latest Digital Trade Agreements and Provisions Relevant to Disinformation

Provision:	USMCA	EU-UK TCA	CPTPP	DEPA	AU/Sing Digital Economy Agreement	US-Japan DTA	WTO draft text
Language explicitly encouraging cross-border data flows with GATT/GATS exceptions	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intermediary liability and content moderation	Yes	No	No	No	Yes[44]	Yes	Yes[45]
Language to encourage competition and policy coherence (cooperation)	Yes	No	No	Yes	Yes	No	Yes
Promote Regulatory Coherence through mutual recognition and other strategies	Yes	No	No	Yes	No	No	Cooperative language throughout, but no specific coherence strategies
Enforce domestic laws regarding privacy	Yes	Yes	Yes	Yes	Yes	Yes	No consensus yet[46]
Enforce domestic law regarding consumer protection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enforce domestic laws regarding spam	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Language on cooperation regarding disinformation	No	No	No	No	No	No	No

[44] The Parties shall create and promote a safe online environment where users are protected from harmful content, including terrorist and violent extremist content. No direction on how they shall.
[45] The Parties shall create and promote a safe online environment where users are protected from harmful content, including terrorist and violent extremist content. No direction on how.
[46] See p. 27-28

Table by Andrew Kraskewicz with S. Aaronson

This section delineates what trade agreements say about regulating cross-border data flows, competition policies, spam, and the use of trade tools to targets entities that disseminate disinformation across borders. We note for the purposes of this writing, we use e-commerce and digital trade agreements simultaneously.

Much of the language in digital trade agreements are 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 that reason, we argue, the free flow of data became the default for almost every trade agreement, along with recognition of the need for exceptions to such open data flows. The US 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 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.[47]

But to some extent the effort to build trust in e-commerce by ensuring netizens that they and their data would be safe took a back seat to the notion of free flow of data across borders. Free flow of data would allow US companies to expand their access to data and grow ever bigger. The Administration made clear that "the US government supports the broadest possible free flow of information across international borders."[48] 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; Aaronson: 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 they may benefit from services built on data, the people who are the source of that data don't control it. It is their asset, yet they cannot manage, control, exchange and account for it (World

[47] The Framework for Global Electronic Commerce, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/
[48] The Framework for Global Electronic Commerce, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/ and Presidential Directive, https://fas.org/irp/offdocs/pdd-nec-ec.htm; http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=SG/EC(98)9/FINAL&docLanguage=En

Economic forum: 2011,11). Individuals' data can essentially be weaponized to create malicious cross-border data flows, whether through disinformation, malware, spam, etc.

A. 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, the EU, Japan, Singapore, the US, and the UK, have placed language governing cross-border data flows in the e-commerce chapters of recent FTAs. Some 52% (182 of 345) of recent (2000-2019) 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 Brexit. CUSMA (Canada, US, Mexico Free Trade Agreement), and the Comprehensive Trans Pacific Partnership (CP TPP) cover a wide range of sectors. However, some nations, including the US, Japan, Chile, New Zealand, and Singapore, have established sector specific stand- alone digital trade agreements. The Digital Economy Partnership Agreement (DEPA), Australia-Singapore Digital Economy Agreement, US/Japan digital free trade agreements have much in common (Wu: 2017; Monteiro and The: 2017; Asian Trade Center: 2019). As noted above they are built on principles first enunciated by the United States in 1997, in the Global Framework. Trade negotiators focus on rules to govern cross-border data flows and generally rely on nations to enforce their own laws to protect consumers/citizens from harmful or malicious cross-border data flows.

Almost every recent agreement has binding language that make the free flow of data a default. They contain language like "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."[49] Such language makes no distinction between data flows that underpin a press release from the World Health Organization or disinformation from Russia's Internet Research Agency, a Russian troll farm famous for sending disinformation.[50] But policymakers 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. [51] These

[49] Article 11, US Japan, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf and ARticle 4.2 DEPA, pp. 4.2-4.3. https://www.mfat.govt.nz/assets/Uploads/DEPA-Signing-Text-11-June-2020-GMT.pdf

[50] https://www.niemanlab.org/reading/inside-the-internet-research-agency-a-russian-troll-farm/

[51] The exceptions include measure necessary to protect public morals or to maintain public order; 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:) the prevention of deceptive and fraudulent practices or to deal with the effects of a default on services contracts; (i) the protection

agreements generally incorporate both the GATT (Articles XX and XXI) and GATS exceptions (Articles XIV).[52] All of these trade agreements also include a national security exception, in which nations can breach the rules to protect against what its policymakers see as a national security threat. Nations using these exceptions do not have to justify their use to other nations.[53] However, when nations use the exceptions, they must be necessary, and be designed to be as least trade restrictive as possible.[54]

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, we see 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 (WEF: 2019). For example, the US used the exceptions to protect public morals in an internet gambling case (the US refused foreign suppliers of gambling based on 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 Daniel Ciuriak argues that socially harmful use of data such as "fake news" and disinformation for personally targeted advertising and/or messaging–e.g., for exploitation of psychological vulnerabilities for marketing purposes or for political manipulation should be considered a legitimate exception (Ciuriak: 2019).

Protecting privacy and personal data are a widely accepted "exception" to the free flow of data. US, New Zealand, and Canadian FTAs generally state that the parties

---

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 safety.
https://www.international.gc.ca/trade-commerce/assets/pdfs/agreements-accords/cusma-aceum/cusma-19.pdf

[52] As example, "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,:

[53] 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. See Article 15.2, DEPA, https://www.mfat.govt.nz/assets/Uploads/DEPA-Signing-Text-11-June-2020-GMT.pdf

[54] They use language like 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.

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 APEC Privacy Framework and OECD Guidelines.[55] 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."[56]

The 2020 Australia-Singapore Digital Economy Agreement 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 internationally. The agreement states that "each Party shall 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."[57]

B. 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 US tried to include its approach to content moderation in some trade agreements. The US demanded language on intermediary liability in the US Japan Digital Trade Agreement and CUSMA. While Japan and Canada must adhere to these rules when the agreement went into effect, Mexico was granted three years to develop appropriate national legislation.[58] In 2019, Australia

[55] These principles include limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability.

[56] 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, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection. 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

[57] Downloadable text at https://www.dfat.gov.au/trade/agreements/in-force/safta/Pages/singapore-australia-fta. See Article 18, #7.

[58] Neither 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

passed the Criminal Code Amendment (sharing of abhorrent violent material) Bill which makes it illegal for social media platforms to fail to promptly remove abhorrent violent user material shared on their services. We could not find language adding this policy to the recent Singapore Australia Digital Economy Agreement although the agreement states that that online safety is a shared responsibility for all online actors.[59] We could find no other nations with intermediary liability language in their trade agreements.[60]

The US is unlikely to push for including language regarding content moderation rules built on Section 230 in other trade agreements. The Biden Administration and many members of Congress want to see Section 230 reform and it recognizes that other nations are not enthusiastic about such language in future trade agreements.[61]

C. Provisions to Encourage Competition

Most trade agreements say little about competition policies. As 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, the General Agreement on Services Trade (GATS) generally prohibits WTO members from adopting regulations which discriminate among foreign service suppliers ('Most favored nation treatment') (GATS Art. 2.1). The 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 Art. 6). The GATS also requires WTO members to be transparent about regulations that may affect services trade (GATS Art. 3). These regulations can include labor regulations and competition policies (Basedow and Kaufman: 2016).

---

or in part, created or developed the information. Article 18, paragraph 3 and 4 US Japan, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf and Article 19.17 CUSMA, https://www.international.gc.ca/trade-commerce/assets/pdfs/agreements-accords/cusma-aceum/cusma-19.pdf

[59] https://www.dfat.gov.au/trade/services-and-digital-trade/Pages/australia-and-singapore-digital-economy-agreement

[60] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1201

[61] https://www.nytimes.com/2019/10/07/business/tech-shield-trade-deals.html; https://www.wired.com/story/fight-over-section-230-internet-as-we-know-it/; https://www.nytimes.com/2021/03/09/technology/section-230-congress.html and https://www.washingtonpost.com/politics/2021/01/18/biden-section-230/

But policymakers have greater freedom to export their competition policy strategies in their bilateral and regional free trade agreements. In its FTAs, the EU requires RTA 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 US and Canada require signatories to establish and enforce their own laws (Anderson et al: 2018)[62]. The US and Canada have also added accountability provisions with requirements relating to non-discrimination, transparency and/or procedural fairness (World Trade Report: .2021, 147).

in a 2020 report, the OECD 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. "[63] 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 endeavor 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."[64]

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."[65]

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.

D. Provisions to promote Regulatory coherence and Prevent a Race to the Bottom

Policymakers understand that nations have different norms and strategies for regulation, but a patchwork of regulation could cause problems for both producers

[62] See as example, CUSMA.
[63] https://oecdonthelevel.com/2020/10/14/how-can-competition-law-tackle-misconduct-in-digital-markets/, p. 62.
[64] https://www.dfat.gov.au/trade/agreements/in-force/safta/Pages/singapore-australia-fta, Article 16, # 2.
[65] DEPA Article 8.4, p. 8.2, https://www.mfat.govt.nz/assets/Uploads/DEPA-Signing-Text-11-June-2020-GMT.pdf

and consumers of goods and services. In recent years, trade diplomats have drafted provisions in trade agreements to encourage greater coherence.

There are many strategies to achieve coherence, from measures to prod cooperation to mutual recognition, to 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 as example, calls for signatories to "pursue the development of mechanisms to promote compatibility and interoperability between their different regimes for protecting personal information. Such strategies can include mutual recognition, regulatory sandboxes (where regulators can experiment) or shared international frameworks."[66] 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"[67] EU trade agreements have a section on regulatory cooperation which notes, "Recognizing the global nature of digital trade, the parties shall cooperate on regulatory issues and best practices through the existing sectoral dialogues ."[68] The Brexit agreement simply says The Parties shall exchange information on regulatory matters in the context of digital trade,[69]

The Digital Economy Agreement of Australia-Singapore goes further on how nations should cooperate. It calls for the parties to endeavor to support data innovation through data-sharing collaboration and regulatory sandboxes[70]. 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, developing countries 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 et al: 2021). Moreover, data governance is expensive and requires good policy governance skills. Data governance will be essential to development, and that donor nations have a responsibility to work with developing countries to improve their data governance. Yet trade policymakers have

[66] https://www.mfat.govt.nz/assets/Uploads/DEPA-Signing-Text-11-June-2020-GMT.pdf
[67] Chapter 28, Good Regulatory Practices, https://usmca.com/good-regulatory-practices-usmca-chapter-28/
[68] Article 11, Modernization of the Trade part of the EU-Mexico Global Agreement Digital Trade, https://trade.ec.europa.eu/doclib/docs/2018/april/tradoc_156811.pdf
[69] Article 16, Title III, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948119/EU-UK_Trade_and_Cooperation_Agreement_24.12.2020.pdf
[70] Article 2, # 2 Australia, Singapore, [70] https://www.dfat.gov.au/trade/agreements/in-force/safta/Pages/singapore-australia-fta

yet to effectively link digital trade governance and data governance capacity building (Aaronson: 2019).

E. Provisions to Reduce Spam

Many but not all countries have laws that ban spam, reflecting the important role of email and the challenge that spam posed in the early days of the web. [71] in 2006, the 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." 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." 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: 2020. Many FTAs have taken steps to regulate unsolicited commercial electronic communications. Such measures include obtaining a 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. [72] As example, Brexit says "Each Party shall ensure that users are effectively protected against unsolicited direct marketing communications," but it does not delineate how. It also says 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." Finally, users must have a form of redress (European Commission: 2020a). Australia-Singapore goes further, noting that Each Party shall provide recourse against a

[71] https://en.wikipedia.org/wiki/Email_spam_legislation_by_country

[72] As example, US Japan says, E ach 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 electron. See Article 16, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf CUSMA states "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 do not comply with the measures adopted or maintained pursuant to paragraph 1". Article 19.13 https://www.international.gc.ca/trade-commerce/assets/pdfs/agreements-accords/cusma-aceum/cusma-19.pdf

supplier of unsolicited commercial electronic message and the parties should cooperate in issues regarding spam.[73]

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.

F. 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 Agreement says 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.[74] Recent US and Canadian trade agreements ban "performance requirements," for source code. As example, US Japan 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." It then allows an exception for a specific investigation, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure.[75] EU agreements have similar language.[76]

Trade diplomats have not yet banned other practices. Yet disinformation, like malware and DDOS attacks, can undermine market access and raise costs for firms who must hire researchers to ascertain who is responsible for these attacks while simultaneously correcting disinformation. Moreover, disinformation may have hidden

[73] Australia/Singapore, Article 19.
[74] Title III, Digital Trade p. 116, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948119/EU-UK_Trade_and_Cooperation_Agreement_24.12.2020.pdf
[75] As example, US Japan, Article 17, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf
[76] 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.

costs—including reducing internet generativity and perceptions that the internet is a safe and stable place to be.

G. Retaliatory Measures

The US has used sanctions to deal with "malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States" Since 2016, the US law authorized sanctions related to interfering with or undermining election processes or institutions. (US Department of the Treasury: 2017, 3). In this regard, the US has sanctioned Russian and Iranian entities. The US process requires an investigation, attribution, and then development of a strategy to target the responsible entities.[77] The US justifies its actions as legitimate under the national security exceptions.

Although the US seems to be the only nation that has retaliated, the EU did a poll in 2019 which found that 74% of respondents to the public consultation were in favor of imposing costs on states that conduct organized disinformation campaigns. Although many democracies such as the US overuse sanctions, they could threaten trade sanctions again 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: 2020b).

Recommendations

While we don't know if disinformation is truly on the rise, we do know that individuals, entities and governments continue to disseminate disinformation across borders. Trade agreements can't stop cross-border disinformation flows, but they can provide tools for mitigating such flows. In addition, trade agreements can't address the business model, although they can help policymakers collaborate to challenge platform practices that fuel disinformation. They may also help ensure that policymakers don't avoid regulating in response to bullying from the data giants. Trade agreements might help a rebalancing of government actions away from the priority of ensuring the free flow of data towards simultaneously trying to establish 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 the Australia/Singapore Digital Economy Agreement and DEPA.

[77] Sanctions on Russian Entities; https://home.treasury.gov/news/press-releases/sm1118; Iran, https://home.treasury.gov/news/press-releases/sm1158; on the law; https://home.treasury.gov/system/files/126/election_executive_order_13848.pdf

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

Objective: Enhance trade agreement rules to govern disinformation and foster international cooperation

Strategy:

1.Since 1996 UN bodies have encouraged nations to adopt a variant of the Model Law on Electronic Commerce (MLEC),[78] Drafters designed the law to encourage a more *universal approach to governing e-commerce. Consequently, the law serves as a building block for national legislation as well as a foundation for international trade agreements[79] In this regard, UNICTRAL, the United Nations Commission on International Trade Law, should create a model law defining cross-border disinformation and delineating how to attribute such disinformation.[80] 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.*

2. 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.

3.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 (verification).

4. Add language to trade agreements requiring nations to enforce their laws on the use of spambots and allow members to a. attribute the use of spambots and b. develop a transparent process to identify nations using such spambots to disseminate disinformation.

5.Clarify that nations can use the exceptions to justify breaching trade agreements rules and cross-border data flows to address disinformation. The language should provide guidance that trade agreement signatories can use trade or financial

[78] https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce
[79] https://uncitral.un.org/en/content/homepage; https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf
[80] he United Nations Commission on International Trade Law is the core legal body of the United Nations system in the field of international trade law.

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.

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

Objective: Individuals and economic actors can be harmed collectively by disinformation when their data is aggregated under the current business model. Address the business model facilitating disinformation by enhancing personal data protection to address collective harms.

7.Strategy: Add language stating that signatories shall not use the personal information of natural persons obtained from enterprises within their jurisdiction in a manner which constitutes targeted discrimination based on attributes such as race, color, sex, sexual orientation, gender, language, religion, political or other opinion, national origin, property, medical, birth or other status, genetic identity, age, ethnicity, or disability.[81]

8. Add language in the provisions on personal data protection that allow natural persons to pursue remedies for violations of personal data protection across borders. Such language would also allow groups at the national and international level 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, prevent data giant bullying, and prevent a race to the bottom regarding regulating digital firms.

9. Strategy: Add language to the competition chapters/language in trade agreements that encourage signatories to cooperate on investigations and accept competition analysis and data from other signatories (mutual recognition).[82] *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.*

[81] This language builds on WTO, "WTO Electronic Commerce Negotiations, Consolidated Negotiating Text-December 2020, 14 December, 2020, Paragraph 14, p.47 language in the draft text released online without the permission of the Secretariat or members.

[82] Dutch Data Protection Authority. 2013. Canadian and Dutch Data Privacy Guardians Release Findings From Investigation of Popular Mobile App. January 28. https://cbpweb.nl/en/news/canadian-and-dutch-data-privacy-guardians-release-findings-investigation-popular-mobile-app

Objective: Bolster international understanding and cooperation on regulating disinformation.

10. Strategy: 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 might 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.[83] 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 it is both a global and a national problem that nations must cooperate to mitigate.

Rather than constraining governments, international cooperation may help the bulk of nations, many of which lack digital prowess to defend against disinformation. Trade agreement language on disinformation could build trust and in so doing expand markets for data, particularly in the developing world.

Bibliography:

Aaronson, Susan, 2018, What Are We Talking about When We Talk about Digital Protectionism? World Trade Review (2018), 0: 0, 1–37.

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.

Aaronson, Susan, 2019. Data is a Development Issue, CIGI,

Aaronson, Susan. 2020 Why the World Needs a Wicked Problems Agency, The Hill, July, 13, https://thehill.com/opinion/technology/506695-why-we-need-a-wicked-problems-agency

Aaronson, Susan and Patrick LeBlond, 2020. Your personal data is being used to fight COVID-19, but the data market needs transparency, The Hill, April 4, https://thehill.com/opinion/cybersecurity/493628-your-personal-data-used-to-fight-covid-19-data-market-transparency

[83] https://www.weforum.org/agenda/2020/01/top-global-risks-report-climate-change-cyberattacks-economic-political/

Aaronson, Susan and Thomas Struett, 2020, Data is Divisive; A History of Public Communications on E-commerce, 1998-2020, CIGI Paper No. 247-December 2020.

AMNESTYINTERNATIONAL.2019."SurveillanceGiants:HowthebusinessmodelofGoogleandFacebookthreatenshumanrights".Availableat:https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF.

Anderson, Robert D. , William E. Kovacic, Anna Caroline Müller and Nadezhda Sporysheet, 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, 31 October

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

Milan Babic, Jan Fichtner & Eelke M. Heemskerk (2017) States versus Corporations: Rethinking the Power of Business in International Politics, The International Spectator, 52:4, 20-43, DOI: 10.1080/03932729.2017.1389151

Ball, Joshua, 2019. What is Hybrid Warfare?, Global Security Review, https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/

Barclay, Donald A. 2018, CONFRONTING THE WICKED PROBLEM OF FAKE NEWS: A ROLE FOR EDUCATION? Cicero Foundation Great Debate Paper, No. 18/3, https://www.cicerofoundation.org/wp-content/uploads/Donald_Barclay_Confronting_Fake_News.pdf

Basedow, R. and C. Kauffmann (2016), "International Trade and Good Regulatory Practices: Assessing The Trade Impacts of Regulation", OECD Regulatory Policy Working Papers, No. 4, OECD Publishing, Paris, https://doi.org/10.1787/5jlv59hdgtf5-en.

Baye, Michael Roy and Prince, Jeffrey, The Economics of Digital Platforms: A Guide for Regulators (November 11, 2020). The Global Antitrust Institute Report on the Digital Economy 34, Available at SSRN: https://ssrn.com/abstract=3733754 or http://dx.doi.org/10.2139/ssrn.3733754

Beall, Chris and Bob Fay,. 2020. In the Age of Connection, Disconnected Digital Governance Isn't Working, December 28,

Bildt, C. (2012), 'A Victory for the Internet', New York Times, 5 July, www.nytimes.com/2012/07/06/opinion/carl-bildt-a-victory-for-the-Internet.html.

Box, S. (2016), 'Internet Openness and Fragmentation: Toward Measuring the Economic Effects', Centre for International Governance Innovation, May.

Boyd, Danah, Google and Facebook Can't Just Make Fake News Disappear, Wired, March 27, https://www.wired.com/2017/03/google-and-facebook-cant-just-make-fake-news-disappear/

Bradshaw, Samantha, Hannah Bailey and Philip N. Howard, 2021. Industrialized Disinformation2020 Global Inventory of Organized Social Media Manipulation, Computational Propaganda Project, Oxford Internet Institute, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/CyberTroop-Report-2020-v.2.pdf

Samantha Bradshaw and Philip N. Howard, 2018. "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation," Oxford Internet Institute's Computational Propaganda Research Project, July 2018, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf.

BT, 2020. How China's trade restrictions are affecting the Australian economy, November 26, https://www.bt.com.au/insights/perspectives/2020/australia-china-relations.html

Burri, Mira and Rodrigo Polanco, 2020. Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset, Journal of International Economic Law, 23: 1 , 1-34. Doi: 10.1093/jiel/jgz044.

Burri, M. (2013), Should There be New Multilateral Rules for Digital Trade? Think Piece for the E15 Expert Group on Trade and Innovation, Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum, December, http://e15initiative.org/wpcontent/uploads/2015/09/E15-Innovation-Burri-FINAL.pdf.

Canada, 2020a. 2019 Update: Cyber threats to Canada's Democratic Processes, https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report_e.pdf

Canada 2020b Paris Call for Trust and Security in Cyberspace, https://www.canada.ca/en/democratic-institutions/services/paris-call-trust-security-cyberspace.html

Canadian Security Intelligence Service: 2018. Who Said What? The Security Challenges of Modern Disinformation: Academic Outreach, February, https://www.canada.ca/content/dam/csis-scrs/documents/publications/disinformation_post-report_eng.pdf

Carvalho, Carlos, Nicholas Klagge, and Emanuel Moench The Persistent Effects of a False News Shock, Federal Reserve Bank of New York Staff Reports, no. 374May 2009; revised March 2010

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

Cedar Partners, 2020. Platform Accountability November, https://drive.google.com/file/d/1S4MBS8VmKCiqqBXLdANiF4ijaqfvq-mY/view

Centre for International Governance Innovation, 2020. Models for Platform Governance. https://www.cigionline.org/sites/default/files/documents/Platform-gov-WEB_VERSION.pdf

Chen, Yongmin Chen, Xinyu Hua, and Keith E. Maskus: 2020. International Protection of Consumer Data, RSCAS 2020/42 Robert Schuman Centre for Advanced Studies Global Governance Programme- https://cadmus.eui.eu/bitstream/handle/1814/67583/RSCAS%202020_42.pdf?sequence=1&isAllowed=y

Citron, Danielle Keats, Hate Crimes in Cyberspace - Introduction (2014). Hate Crimes in Cyberspace, Harvard University Press (2014), U of Maryland Legal Studies Research Paper No. 2015-11, Available at SSRN: https://ssrn.com/abstract=2616790

Ciuriak, Dan, 2019. World Trade Organization 2.0: Reforming Multilateral Trade Rules for the Digital Age (July 6, 2019). CIGI Policy Brief No. 152, Centre for International Governance Innovation, Available at SSRN: https://ssrn.com/abstract=3415973

Cloudflare, 2020, What is a bot? https://www.cloudflare.com/learning/bots/what-is-robots.txt/

Congressional Executive Commission on China, 2011. China's Censorship of the Internet: The Human Toll and Trade Impact, HEARING before the CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA, ONE HUNDRED TWELFTH CONGRESS, November 17, https://www.govinfo.gov/content/pkg/CHRG-112hhrg72895/html/CHRG-112hhrg72895.htm

Cory, Nigel, 2020 Censorship as a Non-tariff Barrier to Trade, http://www2.itif.org/2020-censorship-non-tariff-barrier-trade.pdf

Clark, J., R. Faris, R. Morrison-Westphal, H. Noman, C. Tilton, and J. Zittrain (2017), 'The Shifting Landscape of Global Internet Censorship', Berkman Klein Center for

Internet & Society Research Publication, June, http://nrs.harvard.edu/urn-3:HUL.InstRepos:33084425.

Cory, N. (2017), 'Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost? Information Technology and Innovation Foundation', May, https://itif.org/publications/2017/05/01/crossborder-data-flows-where-are-barriers-and-what-do-they-cost.

Lt. Col. Geoffrey B. Demarest,1996. Espionage in International Law, 24 Denver. Journal of International Law and Policy, 321.

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

Donavan, Joan: 2020, Thank you for posting: Smoking's lessons for regulating social media, October 5, https://www.technologyreview.com/2020/10/05/1009231/social-media-facebook-tobacco-secondhand-smoke/

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

Efrat, Asif, 2010. "Toward Internationally Regulated Goods: Controlling the Trade in Small Arms and Light Weapons" (2010).Cornell Law Faculty Publications. Paper 34.http://scholarship.law.cornell.edu/facpub/34

Elgan, Mike, 2017. **Disinformation as a service? DaaS not good!** , Computerworld, September 17, https://www.computerworld.com/article/3222680/disinformation-as-a-service-daas-not-good.html

Ettlinger, Susan, 2019. What's So Difficult about Social Media Platform Governance?, October 28, https://www.cigionline.org/articles/whats-so-difficult-about-social-media-platform-governance

European Commission, 2018. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Tackling online disinformation: a European Approach, COM/2018/236 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236

European Commission, 2020a. EU UK Trade Agreement, 2020. December 20https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-857-F1-EN-ANNEX-1-PART-1.PDF

European Commission 2020b. 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, 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 (April 15, https://ssrn.com/abstract=3044858 or http://dx.doi.org/10.2139/ssrn.3044858

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

Ghosh, Dipayan Lindsay Gorman, Bret Schafer, and Clara Tsao: 2021 The Weaponized Web: Tech Policy Through the Lens of National Security, Alliance for Securing Democracy and the Kennedy School, January, https://securingdemocracy.gmfus.org/wp-content/uploads/2020/12/The-Weaponized-Web.pdf

Goldsmith, Jack and Tim Wu, 2006. Who Controls the Internet?: Illusions of a Borderless World, Oxford University Press.

Goldstein Josh A and Grossman, Shelby, 2021. How Disinformation Evolved in 2020, Brookings Tech Stream, January 4, https://www.brookings.edu/techstream/how-disinformation-evolved-in-2020/

Haggart, Blaine, Platform Regulation Is Too Important to Be Left to Americans Alone, January 18, 2021, https://www.cigionline.org/articles/platform-regulation-too-important-be-left-americans-alone?utm_source=cigi_newsletter&utm_medium=email&utm_campaign=joan-donovan-how-platforms-enabled-capitol-hill-riot

Dirk 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, 2017https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/

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, https://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?mc_cid=b3950438fc&mc_eid=d6ed88c5ef

Henschke Adam, Matthew Sussex & Courteney O'Connor (2020) Countering foreign interference: election integrity lessons for liberal democracies, Journal of Cyber Policy, 5:2,180-198, DOI: 10.1080/23738871.2020.1797136

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

Howard, Philip, 2014. The Production and Detection of Bots, NSF proposal, http://blogs.oii.ox.ac.uk/comprop/wp-content/uploads/sites/93/2015/01/Project-Description.pdf

Howard, Phillip, Woolley and Ryan Calo, 2018. Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration, Journal of Information Technology & Politics Volume 15, 2018 - Issue 2, https://www.tandfonline.com/doi/full/10.1080/19331681.2018.1448735

Infield, Thomas, 2020. Americans Who Get News Mainly on Social Media Are Less Knowledgeable and Less Engaged, Pew, November 16, https://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, September 30, https://go.recordedfuture.com/hubfs/reports/cta-2019-0930.pdf

Khalimov Yokuv,, Ilkhom Dzhamolov, Nurbonu Mamadikimzosa , Bakdaulet Anarbaev and Aksana Zamirbekova 2019. Reply-generating Farm", Nur-fans and Trolls. How Bots Work in Central Asian States? Central Asian Bureau for Analytical Reporting, November 26, https://cabar.asia/en/reply-generating-farm-nur-fans-and-trolls-how-bots-work-in-central-asian-states

Knutila, Aleksi, ,Lisa-Maria Neudert and Philip N.Howard, 2020 COMPROP Data Memo 2020.8, 0Global Fears of Disinformation Perceived Internet and Social Media Harms in142 Countries, December 15.

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

Dov H. Levin, When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results, *International Studies Quarterly*, Volume 60, Issue 2, June 2016, Pages 189–202, https://doi.org/10.1093/isq/sqv016

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

J. Ernesto López-Córdova and Christopher M. Meissner, 2008. The Impact of International Trade on Democracy: A Long-Run Perspective, World Politics, Vol. 60, No. 4 (Jul., 2008), pp. 539-575 (37 pages)

Lynskey, Orla, Regulating 'Platform Power' (February 21, 2017). LSE Legal Studies Working Paper No. 1/2017, Available at SSRN: https://ssrn.com/abstract=2921021 or http://dx.doi.org/10.2139/ssrn.2921021

Meltzer, Josh. 2019. Cybersecurity and Digital Trade: What Role for International Trade Rules?, (Brookings Glob. Econ. & Dev. Working Paper No. 132, 2019)

Meltzer, Joshua P. 2021. How APEC can Address Restrictions on Cross-border Data Flows, January, https://ab46bb92-a539-4d61-9a28-f77eb5f41c00.usrfiles.com/ugd/ab46bb_830a70b4f8dc4508a38d3e480ffa9cb2.pdf

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

Morrison, Sarah, Belinda Barnett, and James Martin, 2020. China's disinformation threat is real. We need better defenses 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

Mitchell, Amy, et al. 2020. Americans Who Mainly Get Their News on Social Media Are Less Engaged, Less Knowledgeable, Pew July 30, https://www.journalism.org/2020/07/30/americans-who-mainly-get-their-news-on-social-media-are-less-engaged-less-knowledgeable/

Monteiro and Teh: 2019.

Mozilla: 2021. Internet Health Report, https://2020.internethealthreport.org

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

Nakasone, Paul M. 2020, "Introduction A Cyber Force for Persistent Operations, in Schneider, Jacquelyn G. et al, "Ten Years In: Implementing Strategic Approaches to Cyberspace" (2020). Newport Papers. 45.

Newman, Lily Hay, 2016. Hacker Lexicon: What Is the Attribution Problem?, Wired, December 24, https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/?redirectURL=https%3A%2F%2Fwww.wired.com%2F2016%2F12%2Fhacker-lexicon-attribution-problem%2F

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, Institute for the Future, https://www.iftf.org/fileadmin/user_upload/images/DigIntel/IFTF_State_sponsored_trolling_report.pdf

Mavroidis, Petros C. 2016. Regulatory Cooperation: Lessons from the WTO and the World Trade Regime. E15 Task Force on Regulatory Systems Coherence – Policy Options Paper. E15Initiative. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum. https://e15initiative.org/publications/regulatory-cooperation-lessons-wto-world-trade-regime/

Meltzer Joshua P. 2020. How APEC can address Restrictions on Cross-border Data flows, APEC Business Advisory Council, June

Methven O'Brien, Claire and Jørgensen, Rikke Frank and Hogan, Benn Finlay, Tech giants: human rights risks and frameworks (December 15, 2020). Available at SSRN: https://ssrn.com/abstract=

Office of the High Commissioner for Human Rights, UN 2020. Report on Disinformation, https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Report-on-disinformation.aspx

Ibid., 2017. " Joint Declaration on Freedom of Expression and Fake news, Disinformation and Propaganda, https://www.ohchr.org/Documents/Issues/Expression/JointDeclaration3March2017.doc

Organization for Economic Cooperation and Development (OECD) 2011. Communique on Principles for Internet Policymaking,"2011, http://www.oecd.org/internet/innovation/48289796.pdf

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

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

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

Osborne, Charli, Bad bots now make up 20 percent of web traffic, ZD net, April 17, 2019, https://www.zdnet.com/article/bad-bots-focus-on-financial-targets-make-up-20-percent-of-web-traffic/

Pamment, J., The EU's role in fighting disinformation: Crafting a new disinformation framework, Carnegie Endowment for International Peace Working Paper, September 2020; available at https://carnegieendowment.org/2020/07/15/eu-s-role-in-fighting-disinformation-taking-back-initiative-pub-82286.

Park Advisors: 2019. WEAPONS OF MASS DISTRACTION: Foreign State-Sponsored Disinformation in the Digital Age, March, https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf

Pinchis-Paulsen, Mona. 2020 Trade Multilateralism and U.S. National Security: The Making of the GATT Security Exceptions, 41 MICH.J. INT'LL. 109 (2020). Available at: https://repository.law.umich.edu/mjil/vol41/iss1/4

Porotsky, Sophia, 2019. Analyzing Russian Information Warfare and Influence Operations, Global Security Review, June 10, https://globalsecurityreview.com/cold-war-2-0-russian-information-warfare/

Resende, Michael Meyer, Marek Mracka, and Rafael Goldzweig, 2019 "EU EOMS Core Team Guidelines for Observing Online Campaign (2.0)," European Union Election Observation, June 3, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf

Reuters, 2020. "Australia demands coronavirus enquiry, adding to pressure on China," April 19, https://www.cnbc.com/2020/04/19/australia-demands-coronavirus-enquiry-adding-to-pressure-on-china.html

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

John Gerard Ruggie, 1982. International Regimes, Transactions, and Change: Embedded Liberalism in the Postwar Economic Order, International Organization, 36 INT'L REGIMES 379, 392

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

Reuters Staff: 2020. WTO confirms launch of Australia-China trade dispute over barley, December 21, https://www.reuters.com/article/us-australia-china-barley/wto-confirms-launch-of-australia-china-trade-dispute-over-barley-idUSKBN28V2GJ

Schmitt MN, Vihul L (eds) (2017) Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, Cambridge

Snower, Dennis and Paul Twomey, 2020. Humanistic Digital Governance, CES Ifo Working Papers, 8792, December 2020

Stoller, Matt, 2021. Take the Profit Out of Political Violence, Big, January 19, https://mattstoller.substack.com/p/take-the-profit-out-of-political?token=eyJ1c2VyX2lkIjoyMDAwMDM1LCJwb3N0X2lkIjozMTU2ODg1OCwiXyI6InZPeWt2IiwiaWF0IjoxNjExMDcxMDUyLCJleHAiOjE2MTEwNzQ2NTIsImlzcyI6InB1Yi0xMTUyNCIsInN1YiI6InBvc3QtcmVhY3Rpb24ifQ.rXTnreEpDBg2du4CTywzjf1EPYlUHb9i1Ybo1H-IjKU

Sukhankin, Sergey, 2019. THE WESTERN ALLIANCE IN THE FACE OF THE RUSSIAN (DIS)INFORMATION MACHINE: WHERE DOES CANADA STAND? University of Calgary and Canada Global Affairs Institute,, Vol. 12:26, September, https://d3n8a8pro7vhmx.cloudfront.net/cdfai/pages/4258/attachments/original/1567979739/The_Western_Alliance_in_the_Face_of_the_Russian_%28Dis%29information_Machine_Where_Does_Canada_Stand.pdf?1567979739

Taggart, Blayne, 2021. Platform Regulation Is Too Important to Be Left to Americans Alone, January 18, https://www.cigionline.org/articles/platform-regulation-too-important-be-left-americans-alone

Tagliabue, Fabio, Luca Galassi, and Pierpaolo Mariani, The "Pandemic" of Disinformation in COVID-19, Nature Public Health Emergency Collection, August 1, pp, 1-3, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7395797/

Tan, Su-lin, 2020, China-Australia relations: Canberra's plan to scrap research accord labelled 'act of revenge' over trade dispute , South China Morning Press, December 30, https://www.scmp.com/economy/china-economy/article/3115827/china-australia-relations-canberras-plan-scrap-research

Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., and McCue, M. (2018). Addressing Hybrid Threats, http://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-7574

Tucker, Joshua A. Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan, Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature, Hewlett Foundation, March, https://tinyurl.com/yxvw6e6b

Tworek, Heidi, "The Dangerous Inconsistencies of Digital Platform Policies," January 13, https://www.cigionline.org/articles/dangerous-inconsistencies-digital-platform-policies

UNCTAD, 2019. Making Digital Platforms Work for Development UNCTAD Policy Brief No. 73 20 Mar 2019,

University of Baltimore and Cheq, 2019. THE ECONOMIC COST OF BAD ACTORS ON THE INTERNET: FAKE NEWS | 2019https://s3.amazonaws.com/media.mediapost.com/uploads/EconomicCostOfFakeNews.pdf

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

UK Parliament, 2019. Disinformation and 'fake news': Final Report, February 18, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179112.htm#_idTextAnchor082

US Department of Justice, "United States of America vs. Internet Research Agency," filed 16 February 2018, https://www.justice.gov/file/1035477/download

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

US Senate,

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

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

Vilmer, Jean-Baptiste Jeangène Vilmer et al., Information Manipulation: A Challenge for Our Democracies (Paris: Policy Planning Staff and the Institute for Strategic Research of France, August 2018), https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf

Wardle, Claire and Hossein Derakhshan, 2017. Information Disorder, Toward an interdisciplinary framework for research and policymaking Council of Europe, September 27, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Wojcik, Stefan, and Solomon Messing, Aaron Smith, Lee Rainie and Paul Hitlin, 2018. Bots in the Twittersphere, Pew Research Center, April 9, https://www.pewresearch.org/internet/2018/04/09/bots-in-the-twittersphere/

Wood, Brian and Rahim, Rasha, The Birth and the Heart of the Arms Trade Treaty (December 10, 2015). SUR 22 - v. 12 n. 22, 15 - 29, 2015, Available at SSRN: https://ssrn.com/abstract=2837750

Woolley, Samuel C and Phillip N. Howard, 2016. Political Communication, Computational Propaganda,and Autonomous Agents, International Journal of Communication10, http://ijoc.org.

World Economic Forum: 2020. A Roadmap for Cross-Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy, June, http://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf

World Health Organization: 2020. Coronavirus disease 2019 (COVID-19)Situation Report –86, April, https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200415-sitrep-86-covid-19.pdf?sfvrsn=c615ea20_6

WTO, 2018. WTO Council for Trade in Services, Report of the Meeting Held on 2 March 2018, Note by the Secretariat, S/C/M/134, 5 April 2018.

World Trade Organization, 2012. World Trade Report 2012: Trade and Public Policies; A Closer Look at Non- tariff Measures in the 21st Century, Geneva (2012) 3

WTO: 2021a Adapting to the digital trade era: challenges and opportunities, WTO Chairs Programme, Edited by Maarten Smeets, https://www.wto.org/english/res_e/booksp_e/adtera_e.pdf

WTO, 2021b, World Trade Report: Government Policies to Promote Innovation in the Digital Age, https://www.wto.org/english/res_e/publications_e/wtr20_e.htm

Wu, M. (2017). Digital trade-related provisions in regional trade agreements: Existing models and lessons for the multilateral trade system. ICTSD

Wu, Tim. 2019 China's Online Censorship Stifles Trade, Too, The New York Times, February 4, https://www.nytimes.com/2019/02/04/opinion/china-censorship-internet.html

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

Yakovleva, Svetlana, Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy (November 11, 2019). 74 University of Miami Law Review 416 (2020), Available at SSRN: https://ssrn.com/abstract=3463076

Zeiler, Thomas W., 1999. Free Trade, Free World: The Advent of the GATT, Chapel Hill, University of North Carolina Press.

Zhang, Stevie and Esther Chan, 2020. I**t's crucial to understand how misinformation flows through diaspora communities, First Draft, December 11, https://firstdraftnews.org/latest/misinfo-chinese-diaspora/**

Zuboff, Shoshanna (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Profile Books