16

Data Is Different, So Policymakers Should Pay Close Attention to Its Governance

*Susan Ariel Aaronson**

A INTRODUCTION

The founders of Stitch Fix and Strava understood something basic about people. Humans like to use data to connect with other people and to compare with their peers. Based on those insights, these entrepreneurs were able to build two new digital service companies. Both Stitch Fix (a clothing service) and Strava (a social network) rely on personal data to provide services to their customers. Stitch Fix clients first answer a detailed questionnaire about their clothing likes and dislikes. In return, these customers receive clothes and style recommendations designed by stylists and artificial intelligence (AI) to help them look and feel better about themselves.[1] Meanwhile, runners, cyclists and triathletes turn to Strava to measure their performance and instantly compare it to others around the world.[2] The two companies could not succeed without the relatively free flow of data across borders. Data flows move across borders when individuals, companies or governments authorize data to be transferred from one country (the source of data) to another country where the data may be processed or used.[3]

* Susan Ariel Aaronson is Research Professor, George Washington University, Director of the Digital Trade and Data Governance Hub, and GWU Cross-Disciplinary Fellow. She is also Senior Fellow at the Centre for International Governance Innovation (CIGI). Contact: saaronso@gwu.edu. The chapter is based on a paper originally published in 2018 by the Centre for International Governance Innovation entitled 'Data Is Different: Why the World Needs a New Approach to Governing Cross-Border Data Flows'. The permission to publish by CIGI is kindly acknowledged.

[1] https://support.stitchfix.com/hc/en-us/articles/204222994-What-is-Stitch-Fix-How-Does-it-Work-FAQ.

[2] www.strava.com/about.

[3] United States International Trade Commission, Digital Trade in the US and Global Economies, Part 1, Investigation No 332-532, Publication 4415, July 2014; United States International Trade Commission, Digital Trade in the US and Global Economies, Part 2, Investigation No 332-540, Publication 4485, September 2014; J. Nicholson and R. Noonan,

https://doi.org/10.1017/9781108919234.021 Published online by Cambridge University Press

Firms have long relied on data to improve the efficiency and quality of goods and services. However, today market actors also utilize data to create entirely new services, such as personalized healthcare, and sectors such as apps, Internet-connected devices (Internet of Things, IoT), cloud service providers and AI. These sectors are the foundation of the data-driven economy: an economy built around the collection, preservation, protection, implementation and understanding of many different types of data. Although no one has exact figures, a significant portion of the data-driven economy is built on personal data – that is, data by and about people or a person.[4]

The data-driven economy portends major changes for the ability of individuals to shape their destiny and autonomy. Firms active in the data-driven economy are dependent upon data, much of which is personal data. According to the US National Institute of Standards (NIST), in the past, personal data was something that researchers had to ask for, store, analyze. Because it was not easy to collect personal data, scholars struggled to get sufficient information to do a full analysis. But today almost all our daily activities are data-collection opportunities, thanks to the mobile Internet, the IoT, and other data-driven technologies. Moreover, in the past, people could control their data to some extent because researchers, whether firms or individuals, had to obtain, or at least go through the motions of obtaining, consent. However, with the data-driven economy, people whose data is collected and used have provided their personal data without fully informed consent. To put it differently, despite mechanisms to opt in or out of data collection, people do not understand that in return for providing data that firms then monetize, they receive the many free services presented by digital technologies.[5] In this sense, while the mission of data-driven firms, such as Stitch Fix and Strava may be to help customers, their strategy for so doing may also conflict with long-accepted ideas about autonomy.[6]

Compared to Alibaba or Google, Stitch Fix and Strava are small players in the data-driven economy, but they are not atypical. Many of these firms see providing data services as akin to providing a public good. For example, Google's corporate mission is 'to organize the world's information and make it universally accessible and useful'.[7] Not surprisingly, researchers and policymakers now believe that data is

Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services (Washington, DC: US Department of Commerce, 2014), at 1.

4 World Economic Forum, *Personal Data: The Emergence of a New Asset Class* (Geneva: WEF, 2011); D. Ciuriak, 'The Economics of Data: Implications for the Data-Driven Economy', Centre for International Governance Innovation, 5 March 2018.

5 Australian Government Productivity Commission, 'Data Availability and Use', Productivity Commission Inquiry Report: Overview and Recommendations No 82 (2017).

6 P. D. König, 'The Place of Conditionality and Individual Responsibility in a "Data-Driven Economy"', *Big Data and Society* (2017); J. F. Childress, 'The Place of Autonomy in Bioethics', Hasting Center Report No 20 (1990), 12–17.

7 www.google.com/search/howsearchworks/mission/.

https://doi.org/10.1017/9781108919234.021 Published online by Cambridge University Press

the most traded good or service. In 2016, the McKinsey Global Institute asserted that the value of data flows has overtaken the value of global trade in physical goods.[8] According to the World Economic Forum, 'the world produces 2.5 quintillion bytes a day, and 90 per cent of all data has been produced in just the last two years'.[9]

To succeed in the data-driven economy, companies and researchers need access to significant amounts of data – what economists term 'economies of scale'. Policymakers in many countries want to encourage these scale economies with shared norms and rules, but they also want these norms and rules to explicitly limit trade in some types of data to ensure the safety and privacy of their citizens. In elaborating this rule framework decision-makers must develop a process that reassures their citizens that the rules-based system is transparent, accountable and open to citizens' input.[10] With shared norms and rules, the Internet would be less likely to fragment; more people would have greater access to information; and individuals could create and share more information.[11] Individuals might also be better able to obtain rents from their personal data and have some modicum of control over its use. However, policymakers around the world disagree on how and where to develop such shared rules.[12]

Many executives and policymakers argue that trade agreements are the appropriate venue in which to govern cross-border data flows, because they believe that when information flows across borders, these flows are essentially traded.[13] They have negotiated e-commerce and digital trade chapters for this purpose. Herein, we distinguish between e-commerce (goods and services delivered via the Internet and associated with a transaction) and 'digital trade', which includes 'e-commerce' as well as new data-based services, such as Stitch Fix, or social platforms, such as Twitter.[14]

[8] J. Bughin, 'The Ascendancy of Digital Trade: A New World Order?', *OECD Business Brief*, 2016.

[9] V. Thirani and A. Gupta, 'The Value of Data', *World Economic Forum: Industry Agenda*, 22 September 2017.

[10] S. A. Aaronson, 'The Digital Trade Imbalance and Its Implications for Internet Governance', CIGI Global Commission on Internet Governance Paper No 25 (2016).

[11] Ibid.

[12] D. Castro and R. Atkinson, 'Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy', Information Technology and Innovation Foundation, September 2014, at 2; The World Bank, *World Development Report 2016: Digital Dividends* (Washington, DC: The World Bank, 2016).

[13] Aaronson, note 10; J. Meltzer, 'The Internet, Cross-Border Data Flows and International Trade', Brookings Institution Issues in Technology Innovation No 22 (2013).

[14] National and international organizations have not agreed on a common definition of digital trade. According to the OECD, digital trade can be defined as all cross-border trade transactions that are either digitally ordered, facilitated or delivered (see OECD and IMF, 'Measuring Digital Trade: Results of OECD/IMF Stocktaking Survey', BOPCOM 17/07 (2017), at 4). The United States defines digital trade as goods and services delivered via the Internet and/or associated technologies (see R. F. Fefer, S. I. Akhtar, and W. M. Morrison, 'Digital Trade and US Trade Policy', Congressional Research Service Report R44565 (2019)). The

While countries have begun to build a regulatory environment for e-commerce, it is unclear how to build an effective enabling environment for data. Many developing countries are not yet ready for such rule-making. After all, the bulk of firms like Strava and Stitch Fix are being created in middle-income and wealthy countries.[15] In many developing countries, business people are hobbled by obstacles such as unstable Internet connections, limited funding, inadequate numbers of researchers, and complementary policies, and infrastructure.[16] Moreover, while many countries have open data strategies for government-funded or public data, others have not yet figured out how to ensure that when firms mine the personal data of their users, they protect it from misuse, theft, or human rights violations. Firms that do not adequately protect the data that they collect, monetize, and share could lead users to experience problems such as identity theft, manipulative marketing or discrimination.[17] Users deserve a chance to shape new rules and to influence how firms use data.[18]

This chapter examines the new role of data in trade and explores how trade in data differs from trade in goods and services. Clearly, data is different and may need a distinct set of rules. Although there are six different types of data, we focus on two types: public data and personal data (information that relates to an identified or identifiable individual). We then examine several analogies used by analysts to describe data as an input, which can help us understand how data could be regulated. Next, we discuss how trade policymakers are regulating trade in data and how these efforts have created a regulatory patchwork. Finally, we suggest an alternative approach noting that any agreement must be built by and for the people whose data serve as its foundation. Before trade negotiators try to develop rules regarding cross-border data flows, they must acknowledge the special character of data and focus first on creating an effective enabling environment, then built trust in that new economy by empowering people around the world to control their data.

government of Australia notes 'electronic commerce (e-commerce) and digital trade refer to the trade of goods and services using the Internet including the transmission of information and data across borders' (see https://dfat.gov.au/trade/services-and-digital-trade/pages/e-commerce-and-digital-trade.aspx). I could not find an official Canadian definition, but Canada used the term digital trade in its most recent WTO reform proposals.

[15] WTO, *World Trade Report 2018: The Future of World Trade: How Digital Technologies Are Transforming Global Commerce* (Geneva: WTO, 2018).

[16] C. Golobski, 'Capitalizing on Industry 4.0 in Africa', Brookings Institution: Africa in Focus, 3 July 2018, available at www.brookings.edu/blog/africa-in-focus/2018/07/03/capitalizing-on-industry-4-0-in-africa/.

[17] UNCTAD, 'Data Protection and Privacy Legislation Worldwide', available at https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

[18] S. A. Aaronson and P. Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO', *Journal of International Economic Law* 21 (2018), 245–272.

https://doi.org/10.1017/9781108919234.021 Published online by Cambridge University Press

B THE PECULIARITIES OF DATA AND THE ROLE OF DATA IN TRADE

Data and information have long been a key component of trade, but as noted earlier, data has also created new forms of trade. However, cross-border data flows are quite different from trade in goods or other types of services for many reasons: First, many services from payroll to data analytics rely on access to cross-border data flows. These data flows may yield a good or a service, or both.[19] Second, trade in digital services differs from trade in other services because suppliers and consumers do not need to be in the same physical location for a transaction to occur. Third, trade in data is fluid and frequent, and location is hard to determine on the borderless network. Trade in the same set of data can occur repeatedly in nanoseconds – for instance, when millions of people download Drake's latest song. As a result, researchers and policymakers may find it hard to determine what is an import or export. They may also struggle to ascertain when data or data sets are subject to domestic law (such as intellectual property law) and what type of trans-border enforcement is appropriate.[20] Fourth, when data flows across borders, it may or may not be affiliated with a transaction. Hence, it is hard to describe some of these flows as 'traded'.[21] Fifth, economists generally agree that many types of data are public goods, which governments should provide and regulate effectively. Furthermore, when states restrict the free flow of data, they reduce access to information, which in turn can diminish economic growth, productivity and innovation domestically and globally.[22] Such restrictions can also affect the functioning of the Internet.[23] Sixth, trade in data occurs on a shared platform (the Internet) that is held in common. Seventh, and as earlier mentioned, much of the data flowing across borders and powering new sectors is personal data – digital data created by and about people. While they may benefit from services built on that data, the people who are the source of it do not control it. Data is their asset, yet they cannot manage, exchange and account for it.[24]

[19] A. Ariu, 'Services vs. Goods Trade: Are They the Same?', National Bank of Belgium Working Paper Research No 237 (2018).

[20] E. Goldman, 'The Open Act: Significantly Flawed but More Salvageable Than SOPA/PROTECT IP', *Ars Technica*, 12 December 2011; B. de la Chapelle and P. Fehlinger, 'Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation', CIGI Global Commission on Internet Governance Paper No 28 (2016).

[21] Nicholson and Noonan, note 3; US Department of Commerce, *Measuring the Value of Cross-Border Data Flows* (Washington, DC: US Department of Commerce, 2016), at 3.

[22] K. E. Maskus and J. H. Reichman, 'The Globalization of Private Knowledge Goods and the Privatization of Global Public Goods', *Journal of International Economic Law* 7 (2004), 279–320, at 284–285; OECD, 'Economic and Social Benefits of Internet Openness', OECD Digital Economy Papers No 257 (2016).

[23] J. Force-Hill, 'The Growth of Data Localization Post Snowden: Analysis and Recommendations for US Policymakers and Industry Leaders', *Lawfare Research Paper* 2 (2014), 1–40, at 32; L. Daigle, 'On the Nature of the Internet', CIGI Global Commission on Internet Governance Paper No 7 (2015).

[24] WEF, note 4, at 11.

https://doi.org/10.1017/9781108919234.021 Published online by Cambridge University Press

Recent surveys show that people around the world are increasingly concerned about how firms use, protect, control and trade personal data. A 2018 poll of 25,262 Internet users in twenty-five countries found that half of Internet users surveyed are more concerned about their online privacy than they were a year ago, reflecting growing concern around the world about online privacy and the power of social media platforms.[25] Citizens want their governments to strengthen data protection laws and to beef up enforcement. In 2017, the Australian government stated that 'governments that ignore potential gains through consumer data rights will make the task of garnering social license needed for other data reforms more difficult'.[26]

In sum, cross-border data flows may not fit the traditional definition of trade. Policymakers should thus at least question whether the traditional model of trade rules needs reforms to reflect the specificities of data.

C NEW USES FOR DATA REQUIRE NEW WAYS OF THINKING ABOUT DATA

When individuals try to describe how firms are using data to reorder markets, they often compare data to other longstanding inputs to the provision of goods and services. In so doing, they hope to create greater understanding of the import and value of data. As an example, the World Economic Forum describes data as the oxygen of digital life.[27] In contrast, *The Economist* describes data as a new type of raw material, such as oil, on par with capital and labour.[28] However, law professor Lauren Scholz notes that this analogy is not helpful because the supply of oil is limited and only one actor can use a given portion of oil at one time. However, if you have access to data, then you can use it to create information and value.[29] Other analysts describe data as a form of capital, which can be shared and leveraged within and between organizations.[30] They note that the big data firms, such as Google, Facebook, Amazon, Uber, Stitch Fix and Strava, commodify and monetize data, creating new revenues and/or functions for the company.[31]

[25] Centre for International Governance Innovation, *2018 CIGI-Ipsos Global Survey on Internet Security and Trust* (Waterloo: CIGI, 2018).

[26] Australian Government Productivity Commission, note 5, at 2.

[27] M. Sönmez, 'Could Japan Become a Role Model for the Fourth Industrial Revolution?', *World Economic Forum*, 2 July 2018, available at www.weforum.org/agenda/2018/07/could-japan-become-a-role-model-for-the-fourth-industrial-revolution/; 'Data Is Oxygen of Digital Life: Mukesh Ambani', *Governance Now*, 16 February 2017, available at www.governancenow.com/news/regular-story/data-oxygen-digital-life-mukesh-ambani.

[28] 'Special Report: Data, Data Everywhere', *The Economist*, 27 February 2010.

[29] L. H. Scholz, 'Big Data Is Not Big Oil: The Role of Analogy in the Law of New Technologies', *Tennessee Law Review* 86 (2019), 863–893.

[30] 'The Rise of Data Capital', *MIT Technology Review*, 21 March 2016; J. Sadowski, 'Companies Are Making Money from Our Personal Data but at What Cost?', *The Guardian*, 31 August 2016.

[31] Sadowski, note 30; World Economic Forum, note 4.

https://doi.org/10.1017/9781108919234.021 Published online by Cambridge University Press

Meanwhile, some other scholars posit that we should think about data as labour, as in the early phases of the industrial revolution. We provide our data for free to firms that turn around and monetize this information. But you and I, like the workers of yore, lack bargaining power and are unable to meaningfully negotiate over payments for our data. Most of us are not sufficiently protected from misuse of our personal data or violations of our privacy. In this way, we are denied a share of the economic value of our data, just as workers in the early industrial age. We are facilitating a massive transfer of wealth from ordinary people to the tech titans.[32] In search of evidence, two scholars traced the AI supply chain and found invisible labour, outsourced or crowdsourced, hidden behind interfaces and camouflaged within algorithmic processes. They note '[s]ometimes this labor is entirely unpaid, as in the case of the Google's reCAPTCHA. In a paradox that many of us have experienced, to prove that you are not an artificial agent, you are forced to train Google's image recognition AI system for free, by selecting multiple boxes that contain street numbers, or cars, or houses'.[33] Moreover, these scholars note that treating data like capital exacerbates inequality and limits the productivity gains from big data and AI. They suggest that we should organize collectively to form a 'data labor union' that would bargain for fees for assessing our data. The union could certify data quality and guide 'users to develop their earning potential'. Meanwhile, data collectors 'must allow users to understand, withdraw, and transfer their data across competitors'.[34] Only by organizing collectively can we control how our data are used.

Still other scholars argue that personal data is a form of property that individuals can assert rights to control and to access.[35] This concept underpins the European Union's General Data Protection Regulation (GDPR). The notion that data is a form of personal property that people should be able to control also undergirds other countries' approaches, such as those of Brazil and China.[36]

[32] E. Posner, 'On Cultural Monopsonies and Data-as-Labor', 31 January 2018, available at http://ericposner.com/on-cultural-monopsonies-and-data-as-labor/.

[33] K. Crawford and V. Joler, *Anatomy of an AI System: The Amazon Echo as an Anatomical Map of Human Labor, Data and Planetary Resources* (New York: AI Now Institute and Share Lab, 2018), available at https://anatomyof.ai/, at section XVIII.

[34] I. A. Ibarra et al., 'Should We Treat Data as Labor? Moving beyond "Free"', *Proceedings of the American Economic Association*, 1 (2018), 1–5, at 3–4.

[35] T. Scassa, 'Considerations for Canada's National Data Strategy', Centre for International Governance Innovation, 5 March 2018, available at www.cigionline.org/articles/considerations-canadas-national-data-strategy; B. Wylie, 'Governance Vacuums and How Code Is Becoming Law in Data Governance in the Digital Age', in CIGI (ed), *Special Report 2018: Data Governance In the Digital Age* (Waterloo: CIGI, 2018), 86–91, D. Breznitz, 'Data and the Future of Growth: The Need for Strategic Data Policy', Centre for International Governance Innovation, 19 April 2018, available at www.cigionline.org/articles/data-and-future-growth-need-strategic-data-policy.

[36] M. Ramey, 'Brazil's New General Data Privacy Law Follows GDPR Provisions', Covington and Burling, 20 August 2018, available at www.insideprivacy.com/international/brazils-new-general-data-privacy-law-follows-gdpr-provisions/.

If we view data as property, then corporations would have to pay the data generators (you and I) for permission, collection and use of data. The big firms would probably not offer services for free if we had to pay. Moreover, firms would then have an incentive to keep data accurate and carefully stored.[37] But law professor Lisa Austin warns that if you think about data as property, you have to balance the ownership claims of the owners of personal data with those of the firms processing and monitoring that data.[38] Nor can we ensure that our private information is not misused. As law professor Teresa Scassa has noted, privacy laws are ill fitted to a context in which data is a key economic asset.[39]

Finally, the UK government has introduced the notion that data is similar to infrastructure. In a paper prepared for the National Infrastructure Commission, the authors noted 'the managed and built environments increasingly depend upon data in real time. New mechanisms for the assembly, management and processing of data provide a new impetus for thinking how the data is best managed so that society can best utilize its resources, solve the most problems and provide the most social good for most people'.[40] In this view, government plays an important role providing and regulating data and promoting its sharing and consumption.[41]

Except for data as property, these analogies have not significantly influenced national and international regulations. Moreover, these analogies miss an important aspect of the nature of personal data. It is a by-product of our thinking, actions and simply living. It is not one thing, and thus, we should not simply view it as a resource, or as our property, capital, labour, or infrastructure.

There are no reliable statistics about the types, value and amounts of data exchanged across borders and what percentage of cross-border data flow consists of personal data. Both Canada[42] and in the United States,[43] are trying to estimate the value of these flows. Despite the lack of exact numbers, we can hypothesize that a significant portion of the data exchanged across borders is personal data. People's ability to control their data, like other issues of autonomy, is becoming a civil rights issue.[44] According to Ravi Naik, individuals' rights to data protection 'have too often been ignored, and it is taking a groundswell of citizen activism to flip the script and hold power to account by individuals asking for their data and determining its use. We

[37] Breznitz, note 35.
[38] L. Austin, 'We Must Not Treat Data Like a Natural Resource', *Globe and Mail*, 9 July 2018.
[39] Scassa, note 35, at 9.
[40] P. Kawalek and A. Baya, 'Data as Infrastructure', A Report for UK National Infrastructure Commission UK, 14 December 2017, at 1.
[41] Ibid.
[42] Statistics Canada, 'The Value of Data in Canada: Experimental Estimates', 10 July 2019, available at www150.statcan.gc.ca/n1/pub/13-605-x/2019001/article/00009-eng.htm.
[43] US Department of Commerce, note 26.
[44] König, note 6; S. A. Aaronson, 'Data Minefield: How AI Is Prodding Governments to Rethink Trade in Data', in CIGI (ed), *Special Report: Data Governance In the Digital Age* (Waterloo: CIGI, 2018).

https://doi.org/10.1017/9781108919234.021 Published online by Cambridge University Press

are at a watershed moment of a citizen-led demand for data rights, with the hallmarks of a new civil rights movement enmeshed within it'.[45] Some countries, such as Chile, Colombia, Mexico, Turkey and Ecuador, are making personal data protection a constitutional right, although they differ as to the efficacy of enforcement.[46]

Truth is, these analogies can only go so far in guiding public policy because the new economy is behaving in ways that few of us understand. For example, the market for data is opaque: we really do not know how firms use our data. In these conditions, data holders/gatherers can deny or grant access to data; they do not have to let people know what data they have collected, whether it is accurate, how they use it and if they sell it.[47] In opaque markets, policymakers should develop policies that facilitate transparency and accountability, as counterweights to opacity. Breznitz argues in this sense that governments must establish the market for data and set the rules for how data are gathered and used.[48] Meanwhile, the Australian Productivity Commission says that governments must move markets from a system based on risk aversion and avoidance (which is not working) to one based on transparency and confidence in data processes.[49]

Despite their flaws, two of these analogies may be useful to trade policymakers, as they seek to develop rules governing cross-border exchange of data. First, at the national level, developing country policymakers who see data as a form of basic infrastructure could be more willing to establish data plans. Smart management of all types of data will enable more people to benefit from such data and to create new data-driven services attuned to specific economies and cultures. In contrast, the data as labour analogy might help trade policymakers as they attempt to bridge national strategies and create international rules governing data. In the late nineteenth century, many industrializing states developed national regulations to improve work conditions and protect workers from the vagaries of globalization. These regulations helped raise wages, which in turn led to improvements in labour productivity and greater trade. But not all states adopted such worker protections and trade policymakers feared a race to the bottom among states competing for lower wages and working conditions. The members of the League of Nations established an International Labour Organization (ILO) with rules that would help them find common ground to improve workplace conditions, facilitate peace and encourage trade.[50] We may need a similar organization to help mitigate the differences among national data approaches, if not the WTO.

[45] R. Naik, 'Let's Take Back Control of Our Data – It's Too Precious to Leave to the Tech Giants', *The Guardian*, 3 October 2017.

[46] O. Molina, 'Personal Data Protection Is a Constitutional Right in Chile', *IAPP*, 22 June 2018, available at https://iapp.org/news/a/personal-data-protection-is-a-constitutional-right-in-chile/.

[47] Breznitz, note 35.

[48] Ibid.

[49] Australian Government Productivity Commission, note 5, at 2.

[50] M. Huberman, *International Trade and Labor Standards in History* (New Haven, CT: Yale University Press, 2002); International Labour Organization, *Rules of the Game: A Brief Introduction to International Labor Standards* (Geneva: ILO, 2014).

D THE CURRENT STATE OF RULES GOVERNING CROSS-BORDER DATA AND THE RISE OF DATA REALMS

Policymakers have been trying for years to create global rules to govern cross-border data flows both at the World Trade Organization (WTO) and in bilateral and regional trade agreements. The multilateral trade forum of the WTO includes several agreements that address issues affecting data and digital trade. They include the Information Technology Agreement; the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS); and the General Agreement on Trade in Services (GATS). The GATS is the most relevant to the new data-driven services; it has chapters on financial services, telecommunications, computer and media services. But the GATS predates the invention of the Internet and World Wide Web and says nothing explicitly about cross-border data flows. Nonetheless, the WTO panels and the Appellate Body have interpreted the agreement as applying to various online services. While they acknowledge that the agreement is technically neutral – that it was written to apply to changing technologies – academics, business leaders and various governments, including the United States, have argued that the WTO's rules need both amplification and clarification to apply to new data-driven services, such as those provided by Stitch Fix and Strava.[51] Meanwhile, WTO members established a work programme on e-commerce in 1998 and have agreed to waive customs duties on electronic transmissions. They also appear to have made progress on negotiations on data, as a leaked text reveals.[52]

At the Eleventh WTO Ministerial Conference in Buenos Aires in December 2017, Australia, Japan and Singapore, with the support of sixty-seven other WTO members, launched the E-Commerce Joint Statement Initiative. They hoped to encourage a consensus on what members should negotiate and how.[53] To further that effort, countries issued proposals and background papers. A group of African countries, also supported by India, advocated keeping the discussions within the WTO's current exploratory work programme, which has conducted work on e-

[51] M. Burri, 'Should There Be New Multilateral Rules for Digital Trade?' Think Piece for the E15 Expert Group on Trade and Innovation of the ICTSD and WEF, 2013; H. Lee-Makiyama, 'Future-Proofing World Trade in Technology: Turning the WTO IT Agreement (ITA) Into the International Digital Economy Agreement (IDEA)', ECIPE Working Paper No 4 (2011); WTO, Work Programme on Electronic Commerce: Ensuring That Trade Rules Support Innovative Advances in Computer Applications and Platforms Such as Mobile Applications and the Provision of Cloud Computing Services, Communication from the United States, S/C/W/339, 20 September 2011; S. A. Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?', *World Trade Review* 18 (2018), 1–37.

[52] WTO, Work Programme on Electronic Commerce, Ministerial Decision of 13 December 2017, WT/MIN(17)65, WT/L/1032, 18 December 2017. Bilaterals.org released this draft text in February 2021, which I confirmed was correct with WTO secretariat staff. https://www.bilaterals.org/IMG/pdf/wto_plurilateral_ecommerce_draft_consolidated_text.pdf.

[53] All WTO documents relevant to e-commerce discussions are available at www.wto.org/english/tratop_e/ecom_e/ecom_e.htm.

https://doi.org/10.1017/9781108919234.021 Published online by Cambridge University Press

commerce-related topics within various WTO bodies, such as its Council for Trade in Services and Council for Trade in Goods.[54] Overall, not only is there a lack of consensus on e-commerce issues among the members but also it is often apparent that many of the members do not understand the differences, nor do they clearly distinguish between e-commerce and the provision of data-driven services.[55]

Despite this, on 25 January 2019, some seventy-six WTO members agreed to commence dedicated e-commerce talks. The announcement of this initiative was not greeted with universal acclaim. While business groups lauded it, civil society organizations and international labour groups came out against the talks and argued that a new agreement could threaten jobs, privacy and data security.[56] The members of the WTO did not only disagree about whether or not these talks should proceed, they also disagreed about the scope of the talks.[57] Many states – including the United States, Canada, China, Japan, the EU, Australia, Brunei, Hong Kong, Kazakhstan, Korea, Mongolia, New Zealand, Singapore, Chinese Taipei, Thailand, Georgia, Iceland, Liechtenstein, Moldova, Montenegro, Norway, Russia, Switzerland, Macedonia and the Ukraine – are keen to move the talks forward. With regard to data flows in particular, while the United States, Canada, the EU and Brazil generally want to create interoperable and universal rules and limit barriers to cross-border data flows, Russia and China are more concerned with maintaining internal social and political stability and are more open to using domestic regulation to limit such flows.[58] Developing countries are also divided. Policymakers and business leaders in most countries acknowledge that traditional e-commerce could help their farmers and firms trade directly with consumers around the world.[59] So, they are willing to negotiate 'e-commerce', but many are leery of negotiating data-driven services, given that they may lack domestic data-driven firms.

Meanwhile, the United States, the EU, Australia, Canada and other nations have placed language governing cross-border data flows in e-commerce chapters of their free trade agreements. As the data-driven economy has expanded in importance, the US, Mexico, Canada, the EU and Japan have recently renamed the newer versions of these chapters 'digital trade' chapters. Nations are also negotiating and agreed to digital economy specific agreements such as the Digital Economy Agreement of

[54] WTO, Work Programme on Electronic Commerce, Communication from the African Group, WT/MIN(17)/22, 6 December 2017.

[55] L. Kihara, 'China and US among 76 WTO Members Pushing for New E-Commerce Rules', *Reuters*, 25 January 2019; 'E-Commerce: A New Initiative Aims to Modernise Global Trading Rules', *The Economist*, 31 January 2019.

[56] H. Monicken, 'US China over 70 Others Announce Intent to Launch E-Commerce Talks', *Inside US Trade*, 31 January 2019.

[57] *The Economist*, note 55.

[58] Aaronson and Leblond, note 18.

[59] UNCTAD, *Information Economy Report 2017: Digitalization, Trade and Development* (Geneva: UNCTAD, 2017); UNCTAD, 'UNCTAD B2C E-Commerce Index 2018: Focus on Africa', *UNCTAD Technical Notes on ICT for Development* No 12 (2018).

Australia and Singapore, US Japan Digital Economy Agreement, and the Digital Economy Partnership of Chile, New Zealand, and Singapore.[60]

The first agreement, the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) went into effect in 2019 among eleven nations bordering the Pacific including Australia, Japan, Mexico, Chile and Canada. These nations agreed to the free flow of data across borders as a default, with limited exceptions. All signatories also must adopt a minimum level of privacy regulation. In contrast, the EU–Japan Free Trade Agreement (FTA), which also went into effect in 2019, puts personal data protection at its core. The EU–Japan Free Trade Agreement is the first FTA of the EU that includes rules on data but it also ensures that personal data is adequately protected not only under the agreement but additionally through an adequacy decision of the European Commission – the first such decision under the GDPR heightened standards of data protection.[61]

The US government next used CPTPP, whose e-commerce chapter is identical to that negotiated under the Transpacific Partnership Agreement (TPP) as a building block for the renegotiation of the North American Free Trade Agreement (NAFTA). NAFTA 2.0, now called the United States–Mexico–Canada Agreement (USMCA), has several interesting elements designed to promote data-driven economic growth. It seems designed to promote AI and other data-driven services. First, the USMCA contains a proper chapter on 'digital trade' (chapter 19), rather than one on e-commerce. Secondly, like CPTPP, it bans mandated disclosure of source code. But differently from the CPTPP, it also promotes AI by encouraging the parties to provide public information (information developed or provided to public entities) in a machine-readable and open format that can be 'searched retrieved, used, reused, and redistributed'.[62]

While the United States and Canada have made regulating barriers to cross-border data flows a priority, the EU has made personal data protection a priority. The EU will only sign FTAs that contain language regarding the free flow of data if its FTA partner(s) adequately protect personal data. These nations must go through a process of becoming 'adequate'. Specifically, these states must create independent government data protection agencies, register databases with those agencies and, in some instances, obtain prior approval from the European Commission before personal data processing may begin.[63] This process is both time-consuming and

[60] For details, see Chapter 1 and 2 in this volume.

[61] S. A. Aaronson, 'The Digital Trade Imbalance and Its Implications for Internet Governance', CIGI Global Commission on Internet Governance Paper No 25 (2016); European Commission, 'International Data Flows: Commission Launches the Adoption of Its Adequacy Decision on Japan', *Press Release*, 5 September 2018.

[62] Article 19 USMCA.

[63] European Commission, 'European Commission Endorses Provisions for Data Flows and Data Protection in EU Trade Agreements', *European Commission: Daily News*, 31 January 2018; European Commission, 'Questions and Answers on the Japan Adequacy Decision', *Memo*, 17 July 2018; European Commission, 'Horizontal Provisions for Cross-Border Data Flows and

expensive, as the EU's digital trade partners must devote resources to data protection, a difficult choice for nations with limited governance expertise or funds.

Meanwhile, policymakers in China restrict the free flow of data and information not only across borders but also within China. In so doing, Chinese officials maintain social stability and the power of the Communist Party.[64] However, China participated in the negotiation of Regional Comprehensive Economic Partnership (RCEP), a mega-regional trade agreement. RCEP includes Australia, Indian, Japan, South Korea and New Zealand as well as the nations of the Association of Southeast Asian Nations (ASEAN).[65] The RCEP' allows member states to impose whatever national regulatory restrictions they wish, as long as they are applied in a non-discriminatory way (are applied equally to domestic and foreign businesses).The provisions are not disputable.[66]

Thus, the three big digital markets – the United States, EU and China – have taken different approaches to cross-border data flows. This patchwork approach is causing another problem for many nations. Nations, such as Canada, Mexico and Australia, that have or seek to build strong trade relationships with the big three must choose which approach they would follow.[67] Countries that choose more than one such market will face high regulatory costs, as their costs of compliance would rise, given different standards.[68]

In a recent scholarly study, the WTO secretariat confirmed this patchwork of rules. It examined regional trade agreements that have incorporated specific provisions related to e-commerce. They found significant heterogeneity among the seventy-five chapters that explicitly address e-commerce. For example, these FTAs have different objectives, scope and definitions. The FTAs also define and

for Personal Data Protection in EU Trade and Investment Agreements', February 2018, available at https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

[64] Aaronson and Leblond, note 18. See also Chapter 12 in this volume.

[65] J. Panday, "RCEP's Digital Trade Negotiations Remain Shrouded in Secrecy', Electronic Frontier Foundation, 16 May 2017, available at www.eff.org/deeplinks/2017/05/rcep-negotiations-remain-shrouded-secrecy; Australian Government Department for Foreign Affairs and Trade, 'Barriers to Australian Trade and Investment in Regional Comprehensive Economic Partnership (RCEP Countries)', 2018, available at www.dfat.gov.au/trade/agreements/negotiations/rcep/Pages/barriers-to-australian-trade-and-investment-in-regional-comprehensive-economic-partnership-rcep-participating-countries.aspx.

[66] Asia Trade Center, 'E-Commerce and Digital Trade Proposals for RCEP', Working Paper (2016); Asia Trade Center, 'TPP11 and RCEP Compared', Policy Brief No 17-12 (2017) and P. Leblond 'Digital Trade: Is RCEP the WTO's Future?' Centre for International Governance Innovation, 23 November, available at https://www.cigionline.org/articles/digital-trade-rcep-wtos-future..

[67] Aaronson and Leblond, note 18.

[68] A Carson, 'European Regulators, FTC Unveil Cross-Border Data Transfer Tool', *IAPP News*, 7 March 2014, available at https://iapp.org/news/a/european-regulators-ftc-unveil-cross-border-data-transfer-tool/; A. Carson, 'EU and APEC Officials Agree to Streamline BCR/CBPR Application Process', *IAPP News*, 26 May 2015, available at https://iapp.org/news/a/eu-and-apec-officials-agree-to-streamline-bcrcbpr-application-process/.

limit different barriers to trade, and most importantly, some thirty-eight of the seventy-five have different provisions related to the domestic legal framework in which e-commerce takes place. Finally, some forty-four of the seventy-five include language on personal data protection but again with very different definitions and obligations.[69]

Developing countries are likely to have the most problems adapting to the data-driven economy. These countries will be customers of AI and other data-driven sectors, rather than producers. According to Kai-Fu Lee, a venture capitalist and former computer scientist, the bulk of profit from the data-driven economy and particularly AI will go to the United States and China: 'AI is an industry in which strength begets strength: The more data you have, the better your product; the better your product, the more data you can collect; the more data you can collect, the more talent you can attract; the more talent you can attract, the better your product. It's a virtuous circle, and the USA and China have already amassed the talent, market share and data to set it in motion'.[70]

Finally, many developing countries have not yet adopted effective rules protecting personal data online or established rules for the use of public data. Based on data from 2017 the UNCTAD reports that 57 per cent of all countries (some 107 countries of which 66 were developing or transition economies) have put in place legislation to secure the protection of data and privacy. In this area, Asia and Africa show a similar level of adoption, with less than 40 per cent of countries having a law in place. Some 21 per cent of countries have no law at all; and 10 per cent are in the process of drafting legislation.[71] Moreover, most of adopted legislation contains rules that are not consistent with either the OECD Guidelines for the Protection of Personal Information and Transborder Data Flows[72] or EU's GDPR.[73]

Moreover, some countries hoard and refuse to share publicly held data with their citizenry.[74] In general, data gains value as it is shared, but it has little value if governments hoard it. While there is little empirical proof, open data appears to have important spillover effects including increasing civil discourse, improved public welfare and a more efficient use of public resources. But many states lack right to information laws or do not allow their citizens to view or comment on the

[69] J.-A. Monteiro and R. Teh, 'Provisions on Electronic Commerce in Regional Trade Agreements', WTO Working Paper No 11 (2017). For a more recent enquiry, see Chapter 1 in this volume.

[70] K.-F. Lee, 'The Real Threat of Artificial Intelligence', *The New York Times*, 24 June 2017.

[71] UNCTAD, note 17. UNCTAD had no data for 12 per cent of the countries reviewed.

[72] OECD, *Guidelines for the Protection of Personal Information and Transborder Data Flows* (Paris: OECD, 1980; updated in 2013).

[73] Consumers International, *The State of Data Protection Rules around the World: A Briefing for Consumer Organizations* (London: Consumers International, 2018), available at www.consumersinternational.org/media/155133/gdpr-briefing.pdf.

[74] The World Bank, note 12, at 241–247; B. Dennis, 'Scientists Are Frantically Copying US Climate Data Fearing It Might Vanish under Trump', *The Washington Post*, 13 December 2016.

data they hold.[75] So not only is there a patchwork for FTAs but there is also a patchwork of approaches to governing various types of data as well.

Without sufficient understanding and interaction with data-driven firms and their customers, developing country policymakers may struggle to effectively advocate for their short- and long-term interests in the data-driven economy. Zimbabwe provides an example: the government signed a strategic cooperation framework agreement with a Chinese start-up, CloudWalk Technology, for a large-scale facial recognition programme. Zimbabwe will export a database of their citizens' faces to China, allowing CloudWalk to improve their underlying algorithms with more data. The government allegedly agreed to the system to improve public safety, while the company wanted to improve the accuracy of its facial recognition system which was based on Chinese faces and needed a wider range of facial types. However, the government of Zimbabwe could use this system to more closely monitor its citizens, which could undermine social stability and trust.[76] While such a situation may be rare, it provides a strong rationale for Zimbabwe and other countries to develop and debate a strategy for protecting personal data.

E A PATH FORWARD

Humans have long exchanged data between borders, but never have they traded so much data or benefited from so many new services built on data. These new services may make us smarter, richer, more flexible and more efficient. But not all countries or people are ready to participate in this brave new world. The OECD recently noted that 'governments and stakeholders have a responsibility to shape a common digital future that improves peoples' lives and boost economic growth for countries at all levels of development, while ensuring that nobody is left behind'.[77] However, for governance to succeed and be trusted, it needs to be built on shared norms and rules.

Policymakers should first work at the national level to develop a national strategy for data and then move towards interoperability of approaches rather than harmonization. They must find a way to conduct discussions on data governance that build public trust, consistent with the multi-stakeholder processes embedded in other forms of Internet governance. Against this backdrop, this chapter suggests five steps for moving forward, summarized below.

[75] World Wide Web Foundation, *Open Data Barometer – Leaders Edition* (Washington, DC: World Wide Web Foundation, 2018); Centre for Law and Democracy, 'Global right to information by indicator', available at www.rti-rating.org/country-data/by-indicator/Indicators.

[76] I. Hogarth, 'AI Nationalism', 13 June 2018, available at www.ianhogarth.com/blog/2018/6/13/ai-nationalism; S. Jie, 'China Exports Facial ID Technology to Zimbabwe', *Global Times*, 12 April 2018.

[77] OECD, 'Going Digital in a Multilateral World: An Interim Report to Ministers', Executive Summary Meeting of the Council at Ministerial Level, 30–31 May 2018, available at www.oecd.org/going-digital/project/going-digital-interim-overview.pdf.

Step 1: Encourage States to Develop Plans for the Regulation and Exchange of Different Types of Data

Given the complexity of data, its role in new services and the importance of data to economic health and political stability, every nation should develop a strategy for how public and personal data are to be used and exchanged across borders (a national data plan). The plan should focus on ensuring that most public data sets are open, and personal data, especially personally identifiable information,[78] is adequately protected. Such a plan should address issues of ownership, control, equity (i.e. that the data is developed and analyzed in an even-handed manner) and monetization of data (who can earn money for data and how). Policymakers will also have to address issues related to the cloud and data transfer – how a country can control the transfer of data that might include personally identifiable information or data that is important for national security.[79]

It will not be easy for most states to develop such a plan. Policymakers will need guidelines, incentives and technical assistance. Most advanced economies are in the early stages of developing such plans, as they wrestle with disinformation, ethics of AI and digital disruption of various sectors. But some nations/trade blocs are way ahead. The EU, for instance, has developed an EU-wide data strategy focusing on types of data, giving citizens in the EU some control over use of their data. The EU has also established a road map which enables EU policymakers to monitor member states' progress.[80] Meanwhile, the UK, Canada and Australia are in the process of developing their own data plans to match their digital trade strategies. Mexico, Australia and Brazil have too put forward public data or data innovation strategies and Canada is in the process of developing one.[81] In addition, some countries are putting in place plans to facilitate the development of data-driven sectors. As an example, the seventy-five members of the Open Government Partnership pledge to develop plans to make public data open to all. The D7 is a group of countries

[78] Personally identifiable information (PII) is information that, when used alone or with other relevant data, can identify an individual. PII may contain direct identifiers (e.g. passport data) that can identify a person uniquely, or quasi-identifiers (such as race) that can be combined with other quasi-identifiers to recognize an individual.

[79] Scassa, note 35.

[80] European Commission, Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy Accompanying the Document Communication Building a European Data Economy, SWD(2017) 2 final, COM(2017) 9 final.

[81] For Brazil, see 'Estratégia Brasileira para a transformação digital: e-digital', available at www.mctic.gov.br/mctic/export/sites/institucional/estrategiadigital.pdf; for Canada, see Government of Canada, 'Innovation, Science and Economic Development Canada: Government of Canada Launches National Consultations on Digital and Data Transformation', 19 June 2018, available at www.canada.ca/en/innovation-science-economic-development/news/2018/06/government-of-canada-launches-national-consultations-on-digital-and-data-transformation.html; for Australia, see Australian Chamber of Commerce and Industry, 'The Digital Economy: Opening up the Conversation', 30 November 2017, available at www.australianchamber.com.au/wp-content/uploads/2018/01/digital_economy_strategy_submission.pdf.

https://doi.org/10.1017/9781108919234.021 Published online by Cambridge University Press

(Estonia, Israel, New Zealand, South Korea, the UK, Canada and Uruguay) committed to encouraging the data-driven economy and e-government.[82]

International trade and development organizations, such as the World Bank and UNCTAD, could work with civil society groups skilled in data issues (such as Privacy International or the Open Government Partnership) to bring these issues to the fore and provide technical assistance.

Step 2: Give People Greater Voice and Greater Control over Their Data

For the data-driven economy to succeed it must be built on a foundation of trust, and users must have legal protections and greater control over their data. A growing number of data protection plans include some element of consumer control over personal data. Policymakers should call for an international meeting to establish an interoperable approach to data protection and control, which allows nations to evolve their own complementary approaches. The meeting should be attended by a diverse set of individuals, firms and agencies involved in privacy and data protection issues, and it should be tasked to build on existing principles, such as the APEC and OECD Privacy Principles.[83] The organizers of such a meeting could establish a website that will be 'marketed' by participating governments. The architects of the site could then ask netizens to crowdsource ideas about how to build on these existing principles while simultaneously empowering people to control their personal data.[84] Companies and data protection officials have already found some common ground on helping companies that move data globally to transcend different regulatory strategies.[85] But there seems to be a growing sense that the US approach is too focused on ensuring that personal data can be utilized as a commercial asset, while the EU has put its citizens first and protect their personal data as a matter of a fundamental right.

Step 3: Clarify the Rules and Exceptions to the Rules, So Nations Do Not Restrict Cross-Border Data Flows More Frequently or Broadly than Necessary

Like other treaties, a data-driven economy agreement should include exceptions to the rules. Nations can use the exceptions to 'excuse' violations to the agreement when they pursue other important policy objectives. (Figure 16.1 shows that governments have a wide range of reasons to restrict cross-border data flows.) Countries can only use these exceptions, however, if they do so in the least trade distorting manner. Yet, so far, there is no clear model that policymakers can follow to distinguish between legitimate and trade-distorting data flow regulation. The current language in trade

[82] See www.digital.govt.nz/digital-government/international-partnerships/d7-group-of-digital-nations/.

[83] For an overview of data protection laws and regulations, see Consumers International, 'Digital Index: Data Protection and Privacy', available at https://digitalindex.consumersinternational.org/search/category/data-protection-and-privacy/subcategory/personal-data-protection/page/1.

[84] WEF, note 4.

[85] Carson, note 68.

https://doi.org/10.1017/9781108919234.021 Published online by Cambridge University Press

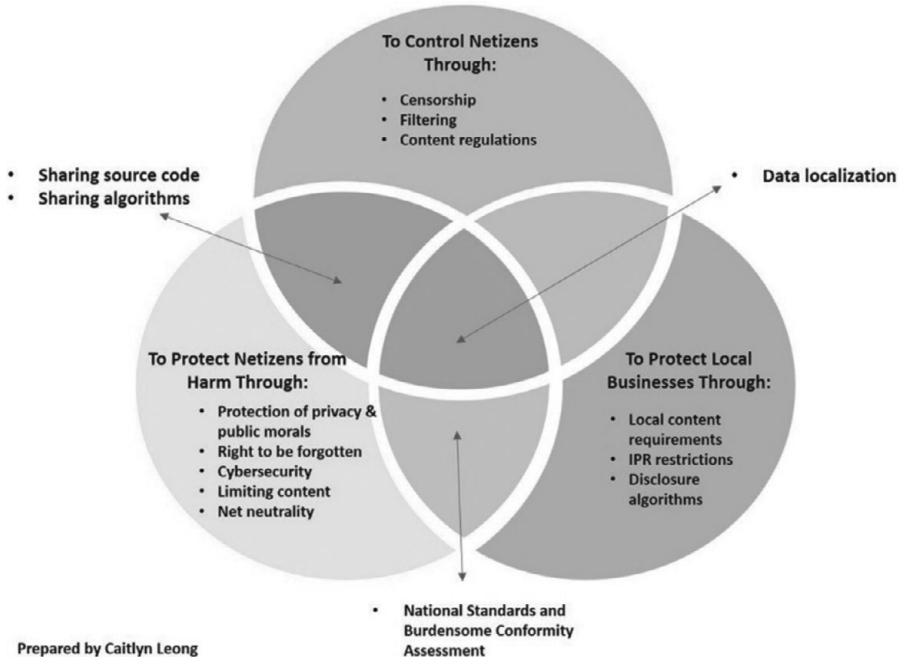

FIGURE 16.1. Why and how do governments restrict cross-border information flows? Prepared by Caitlyn Leong

agreements is vague and states must rely on trade disputes to develop clarity and some degree of legal certainty. However, there have been few disputes to provide guidance and policymakers have not yet agreed on updating the WTO law language with regard to the general exception clauses or other specific exceptions.

Policymakers should begin by delineating how and when nations can use the exceptions to limit cross-border flows in the name of protecting domestic security or cybersecurity. For example, some governments, such as India, Brazil, the United States and the UK, have called on companies to provide backdoors to encrypted communications to help law enforcement. However, such an encryption backdoor would undermine trust and the effectiveness of encryption as a tool for keeping individuals, firms and governments safe online.

Step 4: Provide Clarity on What Types of Practices Should Be Banned Because They Are Trade Distorting

Beyond data localization and taxation of e-commerce, there is little agreement as to what measures distort cross-border data flows.[86] For example, many Western

[86] WTO, note 52; Aaronson, note 51.

https://doi.org/10.1017/9781108919234.021 Published online by Cambridge University Press

countries believe that censorship is a trade barrier, which can undermine the many benefits of the Internet. Yet, no trade agreement discussing cross-border data flows mentions censorship, filtering or Internet shut-downs as a barrier to trade that should be regulated. Many states censor, filter or shut down the Internet for a variety of reasons, including safeguarding government authority, fighting terrorism, maintaining national security or protecting local businesses. When they censor, filter or shut down the Internet, they determine what data will be available within their borders.[87] Authoritarian states are not the only states that censor data. The Indian government, the world's largest democracy and a technology leader, has had fifty-four Internet shut-downs, more than any other nation in 2017. Human rights groups view these shut-downs as an intentional form of censorship which distorts the free flow of data. These shut-downs have also huge economic costs, estimated at some $3 billion for the period 2012–2017 for India alone.[88] Brookings scholar Darrell West estimated that globally, Internet shut-downs cost some $2.4 billion in 2015 alone.[89] Policymakers must find common ground on defining and regulating these practices or they cannot reap the benefits of economies of scale on data. Such practices may also create costly spillovers, such as reducing Internet stability and hampering scientific progress.[90]

Step 5: Delineate How Nations Should or Should Not Respond to State Actions That Distort Cross-Border Data Flows

Trade agreements allow signatories to respond to the trade distorting practices of their partners with compensatory practices. The agreement should clearly state that party responses should be limited and proportional in such instance and define accordingly the legal test. Moreover, any agreement should also clearly state that adopting protectionist strategies, such as tariffs and quotas, or turning to strategies, such as malware, are inappropriate responses, which could reduce cross-border data flows, are prohibited. According to trade scholar Patrick Leblond, 'Ideally, the response should increase the costs of doing business and penalize proscribed practice, but not penalize the sources of data'.[91] Data protectionism will beget

[87] A. Chander and U. P. Lê, 'Breaking the Web: Data Localization vs. the Global Internet', UC Davies Legal Studies Research Paper No 378 (2014).

[88] R. Kathuria et al., *The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India* (New Delhi: Indian Council for Research on International Economic Relations, 2018).

[89] D. West, 'Internet Shutdowns Costs Countries $2.4 Billion Last Year', Brookings Report, 6 October 2016, available at www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/.

[90] S. Box, 'Internet Openness and Fragmentation: Toward Measuring the Economic Effects', CIGI Global Commission on Internet Governance Paper No 36 (2016).

[91] P. Leblond, email to author, 10 July 2018.

further data protectionism and undermine the utility of the Internet.[92] We may be seeing evidence of this digital trade wars already between the United States and the EU: After the US Secretary of Commerce Wilbur Ross called the EU approach to data protection trade distorting in May 2018,[93] the EU proposed tax and regulatory policies to challenge what some see as the monopolistic control of US Internet giants.[94]

F CONCLUSION

The world is awash with data and there is no consensus on how to regulate it. The five outlined steps can help nations prepare for future negotiations and build value from data. These ideas will not address all the issues that arise in regulating cross-border data flows, and any new approach is likely to face many challenges, especially from those vested in the existing organizations and approaches to governing data. But clearly, we are stuck in a rut on trade and must creatively address the trade and non-trade dimensions of cross-border data flows. Policymakers from a wide range of countries may be more willing to compromise if they see that their citizens will benefit from clear, interoperable rules and from receiving funds for their data. Moreover, this approach could help firms accommodate national differences regarding ethics of data usage, disinformation and other upcoming regulatory issues. It could also give developing countries greater leverage in the discussions on data flows, where they would ordinarily be 'rule takers'.[95] Finally, these ideas could help more countries better integrate data-driven firms and their traditional firms. By collaborating and rethinking the process of global rule-making on data, we will be better able to achieve the change we wish to see in the world – where people have greater autonomy and control over their data and data drives equitable growth.

[92] Box, note 90; OECD, note 21.

[93] W. Ross, 'EU Privacy Laws Are Likely to Create Barriers to Trade', *Financial Times*, 30 May 2018.

[94] European Commission, 'Digital Taxation: Commission Proposes New Measures to Ensure That All Companies Pay Fair Tax in the EU', *Press Release*, 21 March 2018.

[95] Aaronson and Leblond, note 18.