Centre for International
Governance Innovation

CIGI Papers No. 240 – April 2020

Toward a Robust Architecture for the Regulation of Data and Digital Trade

Dan Ciuriak and Maria Ptashkina

Centre for International
Governance Innovation

CIGI Papers No. 240 — April 2020

Toward a Robust Architecture for the Regulation of Data and Digital Trade

Dan Ciuriak and Maria Ptashkina

About CIGI

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

À propos du CIGI

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

Credits

Director, Global Economy Robert Fay
Program Manager Heather McNorgan
Senior Publications Editor Jennifer Goyder
Publications Editor Lynn Schellenberg
Graphic Designer Sami Chouhdary

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

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

Centre for International Governance Innovation and CIGI are registered trademarks.

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

Table of Contents

About the Authors

Dan Ciuriak is a senior fellow at CIGI, where he is exploring the interface between Canada's domestic innovation and international trade and investment, including the development of better metrics to assess the impact of Canada's trade agreements on innovation outcomes. Based in Ottawa, Dan is the director and principal of Ciuriak Consulting, Inc. Dan is also a fellow in residence with the C. D. Howe Institute, a distinguished fellow with the Asia Pacific Foundation of Canada and an associate with BKP Economic Advisors GmbH of Munich, Germany. Previously, he had a 31-year career with Canada's civil service, retiring as deputy chief economist at the Department of Foreign Affairs and International Trade (now Global Affairs Canada).

Maria Ptashkina is an economics Ph.D. candidate at University Pompeu Fabra, Barcelona, Spain. Her main research interests include macroeconomics, international economics and trade policy. She is a former fellow at the International Center for Trade and Sustainable Development and former delegate from the Russian Federation to the Asia-Pacific Economic Cooperation Forum. Maria is a former member of intergovernmental policy research groups on issues related to international trade and investment (the Group of Twenty, BRICS [Brazil, Russia, India, China and South Africa] and the One Belt, One Road initiative).

Acronyms and Abbreviations

5G	fifth-generation
AI	artificial intelligence
BRICS	Brazil, Russia, India, China and South Africa
CUSMA	Canada-United States-Mexico Agreement
D9	Digital 9
FDI	foreign direct investment
G20	Group of Twenty
GATS	General Agreement on Trade in Services
GATT	General Agreement on Tariffs and Trade
GDPR	General Data Protection Regulation
IoT	Internet of Things
IP	intellectual property
OECD	Organisation for Economic Co-operation and Development
R&D	research and development
SMEs	small and medium-sized enterprises
TPP	Trans-Pacific Partnership
TRIPS Agreement	Agreement on Trade-Related Aspects of Intellectual Property Rights
WTO	World Trade Organization

Executive Summary

The digital transformation occurring worldwide poses significant challenges for a governance framework that evolved gradually and incrementally over centuries, shaped by lessons learned during the long era of industrialization and globalization in which much of today's technology was still science fiction. At the heart of the governance challenge is "datafication" — the capture of truly astronomical amounts of information on the functioning of societies, economies and even the industrial processes of firms. Once transformed into data, information can be analyzed and used to modify the behaviours that generated the information in the first place for economic, political or geopolitical advantage.

Given the multiple roles that data plays — as the medium of digital commercial transactions and digital trade, as a valuable capital asset, as part of the intangible infrastructure of the digital economy, and as the very fabric of a modern information society — the governance challenge is immense. Moreover, given the multitude and pervasiveness of data analytics applications, there is urgency in coming to grips with the regulation of data, since other governance challenges, ranging from climate change to income distribution, depend on safeguarding democratic processes and functional markets.

Numerous efforts are under way to address aspects of the regulation of data. These efforts include the recently launched e-commerce negotiations of the World Trade Organization (WTO), other work programs under the WTO, and the initiatives of the Group of Twenty (G20) on the free flow of data based on trust. There is, as well, work in more specialized areas, such as competition policy and intellectual property (IP), taxation in the digital realm, and multi-stakeholder processes addressing the plethora of other digital governance issues ranging from privacy to cyber security.

This paper suggests a conceptual framework for addressing the multi-dimensional policy dilemma that societies now face of reconciling the many competing policy priorities raised by digital transformation domestically and of preparing the ground for negotiations toward a robust and broadly accepted governance regime internationally, fit for purpose for the age of data.

Introduction

How will rules written for the world of 1994 fare in a world of talking teapots and connected cars?

—Anupam Chander (2019)

The digital transformation is generating exponentially growing flows of data within and across national borders and enabling the rapid development and virtually frictionless global dissemination of new technologies. These data flows and technologies touch virtually every aspect of our society and economy, dangling the promise of wealth and power to the winners of the race to commercialize, while also threatening pervasive economic disruption, raising the spectre of social dystopia and incentivizing strategic competition between nations. To say the least, these developments pose significant challenges for a governance framework that evolved gradually and incrementally, shaped by lessons learned during the long era of industrialization and globalization, in which much of today's technology was still science fiction.

At the heart of the governance challenge is "datafication" — the capture of truly astronomical amounts of information on the functioning of societies, economies and even the industrial processes of firms. Data applications are ubiquitous: data serves as the medium of digital commercial transactions, including cross-border trade; it has value as a capital asset, independent of the message it carries; it constitutes part of the intangible infrastructure of the digital economy, in particular for the rapidly expanding Internet of Things (IoT); and it embodies the information that is generated through social and political engagement in a modern information society.

Reflecting the value proposition that data offers, strategic competition to dominate the data-driven economy has already escalated into a full-blown trade and technology war between the two leading digital economies, the United States and China, with spillover effects on trading partners. Frictions are also being felt along other digital fault lines, including between the United States and the European Union; along the digital borders of the BRICS countries (Brazil, Russia, India, China and South Africa); and along the digital divide between the data "haves" and the "have-nots." These

conflicts are often mirrored in frictions within societies over how the economic gains from the new technologies are to be shared and how these technologies are to be governed and by whom.

Simply put, the postwar global governance model is being shaken to its foundations and governments are being driven to act. Ready or not in terms of policy development, governance reform will not wait.

A Multi-dimensional Policy Dilemma

Each of the roles of data requires its own governance regime. As a medium of transactions, cross-border data flows are, in principle, subject to commitments that countries have made under the WTO General Agreement on Trade in Services (GATS), which provides for technological neutrality for trade in services (see, for example, Janow and Mavroidis 2019, S2). This is the role of data that the Trans-Pacific Partnership (TPP) and the Canada-United States-Mexico Agreement (CUSMA) data provisions address.

However, whereas data was mostly "exhaust" when the GATS was developed — an unexploited by-product of commercial transactions, business and industrial processes, and other interactions — it has now become the most valuable asset of the digital age (the "new oil" [*The Economist* 2017]) and, indeed, the essential capital asset for the emerging data-driven economy (Ciuriak 2018b). It is hardly surprising that governments are seeking to capture this value through industrial policies and taxation reforms.

Further, states will need to take measures to ensure the security and integrity of their essential services both internally and externally, especially the "backbone" infrastructure services — finance, transportation, communications and energy (European Commission 2019). Metaphorically, a nation's digital borders must be as secure as its physical borders. With the rollout of the IoT and the flow of data into the inherently insecure "cloud" (which, from the perspective of any user of cloud services, is just some other entity's computers), the security challenges escalate not only from the perspective of vulnerability to hacking but also from the consequences of interference with the functioning of an infrastructure that increasingly acts as an interactive central nervous system for the economy.

Finally, in parallel with the security concerns are the myriad issues raised in transposing the rules and norms governing social and political behaviour into the digital realm. These issues run the gamut from "surveillance capitalism" (Zuboff 2019) to state surveillance (an issue that is now flaring in democracies in connection with the digital tracing technologies being considered as part of the response to the COVID-19 pandemic [McDonald 2020]); to the use of personally identifiable information for commercial and political objectives, including "fake news" and targeted messaging for manipulation of electorates; to the governance of urban spaces; and, indeed, to many other areas.[1] The vastness of the scope of these issues is due in part to the protean nature of data. Not only can data be used and reused in endless configurations and applications underpinning value capture and creation, but it also can act as a source of feedback to change the world that generated it in the first place. This feedback generates its own governance demands since it comes complete with the biases built into data, given the means of its collection and the populations from which it is sourced. These issues can be grouped under the broad rubric of "sovereignty," because they affect how states govern themselves, and democratic legitimacy demands that governance principles shape, rather than be shaped by, the digital transformation.

Governance Will Not Wait

Given the urgency of addressing these issues, governments worldwide have been galvanized into action to develop digital strategies and governance reforms; issue-specific policy research programs have been launched across the range

1 A sense of the breadth of challenges directly or tangentially related to governance is provided by a remarkable volume of short commentaries triggered by the reaction to the letting of a contract to Google's Sidewalk subsidiary to develop a "smart city" on Toronto's waterfront. See Ahmed et al. (2019).

Box 1: Digital Economy Governance Initiatives

Numerous initiatives are under way to address the issues raised by the digital transformation.

- At the WTO, negotiations have begun on electronic commerce (WTO 2019a), and new empirical work is being undertaken on the moratorium on tariffs on electronic transmissions (WTO 2019c).
- The G20 reached agreement on the "Osaka Track" program to promote an open digital economy based on trust — "Data Free Flow with Trust" (Sugiyama 2019a) — and continues to work on elaborating what that requires.
- The Digital 9 (or D9) governments are sharing best practices on applying the digital transformation to public administration to facilitate the delivery of public services and solve common problems.
- The Organisation for Economic Co-operation and Development (OECD) has a long-standing work program to address the tax challenges posed by the digitalization of the economy (OECD 2019b); this effort is key to settling the flaring conflict over the taxation of entities that conduct business in an economy without a "permanent establishment" in that economy that can be subjected to taxation under existing bilateral tax treaties (Hufbauer 2020).
- The International Grand Committee on Disinformation and "Fake News" is delving into the plethora of governance issues raised by the evolution of the information society (Stone 2019).
- Activity on cyber security is in high gear, given international tensions, and building on long-standing multilateral cooperation and coordination in this area (Butler and Lachow 2012; Chernenko, Demidov and Lukyanov 2018; Gates and Ma 2019). Multi-stakeholder processes on cyber security currently under way (see Gates and Ma 2019, 20) include the following:
  - the Paris Call for Trust and Security in Cyberspace, a multi-stakeholder initiative launched in November 2018 and involving 65 countries, 334 companies and 138 universities and non-profit organizations;
  - the Global Commission on the Stability of Cyberspace, an independent multi-stakeholder platform focused on norms and policies to enhance international security and stability in cyberspace;
  - the Global Conference on Cyberspace, also known as the "London Process," a series of multi-stakeholder conferences that led to the establishment of the Global Forum on Cyber Expertise, which focuses on identifying best practices in developing cyber security frameworks;
  - the Geneva Dialogue on Responsible Behaviour in Cyberspace; and
  - corporate initiatives such as the Cybersecurity Tech Accord, a coalition of more than 100 global technology companies with a commitment to protect and empower civilians online and to improve the security, stability and resilience of cyberspace, and the Charter of Trust, founded in 2018 at the Munich Security Conference, which brings together 17 leading global companies and organizations to combat malicious cyber attacks.
- Various efforts are under way aimed at supporting the participation of developing countries and promoting inclusion (see, for example, Gates and Ma 2019).
- Finally, there has been a call to address the US-China conflict with a revised international framework. The revision would provide an intermediate option between "deep integration" and "decoupling" in terms of providing countries the latitude to maintain the industrial policies, technological systems and social standards of their choice and to protect these policy choices domestically, subject to their not imposing unnecessary and asymmetric burdens on foreign actors, while maintaining trade rules that prevent beggar-thy-neighbour policies (US-China Trade Policy Working Group 2019).

of digitalization issues, and multilateral efforts are under way in various fora to address the systemic regulatory challenges (see Box 1).

This paper suggests a conceptual framework for a coherent integration of the proliferating reform efforts noted above. In particular, it groups the various issues under the pillars of "economic value capture," "sovereignty" in public choice and "national security," and considers how policies adopted in these areas can be reconciled with commitments under a multilateral framework for international commerce adapted for the digital age.

Whether the regime that satisfies the multiple constraints will feature more or less policy space for national governments is not clear at this stage; what *is* clear is that domestic policy space needs to be redefined for the digital age and the interface with international trade governance recalibrated.

The Economic Value Capture Pillar

The exploitation of data promises great rewards but makes no promises at all regarding the sharing of those rewards, neither within economies, nor between economies. The early returns on the data-driven economy suggest that there are significant rents and that these flow in a concentrated manner to a handful of global firms that provide digital platforms or otherwise command global market power. For example, the European Commission estimates that digital platforms will capture 30–40 percent of the value created in industrial value chains.[2]

It is no surprise that jurisdictions worldwide are looking to find a way to capture some of the gains for their own economies. From a systemic perspective, policy makers will need to employ sound strategies tailored to the economics of the data-driven economy to avoid the kind of buildup of pressure that helped fuel the rise of populism in the past decade. Doing so will likely involve new flexibility in at least four areas: ownership and access with regard to economic exploitation of data; engagement and investment of the public sector; experimentation regarding capture and distribution of benefits from data assets to maximize prosperity; and creating dynamic innovation systems (Ciuriak 2019a).

Data Governance and the Economic Exploitation of Data

Many countries are working on national data strategies to facilitate the economic exploitation of data, with a view to capturing its economic and social benefits (OECD 2019a). The need for comprehensive data governance regimes is now well understood (see, for example, CIGI 2018; Scassa 2019).

From a systemic perspective, the extent and distribution of benefits will be influenced, perhaps heavily, by societal choices on several major unsettled issues, namely, "ownership" of data; frameworks for providing access to data to promote competitive marketplaces in a context highly conducive to market concentration; and setting boundaries on commercial exploitation.

Unlike other productive assets, data does not fit into a neat framework around which markets can easily be structured with vested ownership rights, and transparent asset values and transaction prices (Ciuriak 2019c). Indeed, for many types of data, the very concept of ownership is problematic (Leyser and Richardson 2018). For example, transactional data is shared by many parties, and information on activity in public spaces is inherently public, meaning that decisions regarding data need to encompass a societal, as well as an individual, point of view (ibid.). At the same time, data does not fit the description of the alternative to a private good — namely, a freely accessible commons — because access and exploitation depend on investment at scales beyond the reach of most. Further, individual bytes of data cannot be reasonably priced and compensated (the administrative costs of compensation would likely be impossibly large).[3]

2 See https://ec.europa.eu/growth/industry/policy/digital-transformation/big-data-digital-platforms_en.

3 Quite paradoxically, while data cannot necessarily be exclusively owned, it can be sold – at least in secondary markets, as part of the valuation of a firm. Thus, various mergers and acquisitions transactions are characterized by the market as "data plays," where the valuation of the company is based on the value of data being acquired. For example, PayPal's acquisition of the firm Honey Science for US$4 billion was described as follows: "The acquisition is a pure data play and the power of data for personalization cannot be underestimated, which is why I'm not surprised by the massive price tag on this acquisition" (Taulli 2019).

Closely related to the issue of ownership is that of boundaries on commercial exploitation. These boundaries may be based on societal preferences in areas such as surveillance, the application of the precautionary principle to moderate the pace of the implementation of new technologies, and the establishment of standards, especially as regards future data-driven artificial intelligence (AI) and IoT implementation. Some differences have already emerged across jurisdictions in such areas as the use of facial recognition.

Access is another area of potential differentiation of public policies. The data-driven economy has evolved on the basis of proprietary libraries generated by firms as part of their commercial or industrial activities or obtained from public sources, including data generated by public administration activities (for example, collection of geostatistical data) that is increasingly provided freely by governments as "open data" to stimulate the development of applications. However, this free enterprise model is precisely the one raising numerous public policy issues, including market dominance and the plethora of issues related to standards, bias, manipulation and so forth. Moreover, there is an inherent "anti-commons" problem with this model, given that data has the public good characteristic of being non-rivalrous, while proprietary data and algorithms generated on data are protected trade secrets.

How these issues are addressed has important implications for market structures and the distribution of benefits. In the case of the platform companies, the options range from regulation as utilities to some form of mandatory data sharing. Market intermediation based on regulated data trusts, which absorb the library costs, operate under fiduciary principles and practices, and provide the data at a competitive fee to clients, is another and seemingly market-friendly approach that is being promoted in some jurisdictions (McDonald 2019). In the case of small firms, competitive access to data, coupled with access to data analytic tools through the "platform as a service" business model, could mitigate the tendency toward extreme market outcomes that the proprietary data model generates and facilitate the participation in the data-driven economy of small and medium-sized enterprises (SMEs) from developing economies.

Public Sector Engagement

The public good nature of data — combined with the acceleration of the pace of innovation, which implies shorter time horizons for recoupment of investment — suggests that there is a newly expanded role for public sector investment in the data-driven economy. Industrial policy has been making a comeback in recent years, with the data-driven economy putting wind in its sails as governments worldwide are engaging heavily through publicly funded research and development (R&D), public procurement policies to support specific emerging technologies, and favourable regulatory policies in the hope of gaining or capturing a leading role in this new economy. These countries include the United States, which has prioritized AI, quantum information systems, advanced communication networks and advanced manufacturing (White House 2020); the European Union, which targets the same technology nexus under its "Industry 4.0" program (European Parliament Research Service 2015; see also European Commission 2017 and Morrisson and Pattinson 2019 for updates); the United Kingdom, which has adopted a "mission-oriented industrial policy" that aims to address "grand challenges," one of which is AI and data (HM Government 2017); and Japan, which has a "connected industries" policy aimed at this same nexus of emerging technologies under its "Society 5.0" initiative. China has set similar objectives in its Made in China 2025/AI 2030 programs, although these programs are no longer publicly mentioned, as they have attracted fire from the United States and the European Union — indeed, one of the main criticisms levelled against the new US-China Trade Agreement is that it fails to dismantle China's industrial policy.

Notwithstanding the general consensus against such government policies, Gene M. Grossman (1990, 118-19), while conservatively leaning against the use of subsidies, taxes and strategic trade policies, draws two key conclusions at odds with the current consensus:

- The arguments for industrial policy do not apply to all industries: "The nature of the problem makes case-by-case analysis unavoidable." In other words, "horizontal" treatment is not the optimal way to consider industrial policy.
- The strongest case for government intervention rests on support at the early stage of the development of technologically innovative

products, which involves large R&D expenditures and features significant learning-by-doing effects. In such cases, market innovation would take place at an inefficiently slow pace. The emerging data-driven economy appears to be replete with such early-stage opportunities.

Accordingly, a reconceptualization of public sector engagement in the economy, based on economically meaningful filters, is needed to reconcile what governments are actually doing with what the consensus framework (and the rules based on it) calls for. Absent such reconceptualization, there will be needless international friction.

Prosperity in an Asset-based Economy

The data-driven economy promises to intensify the skewing of income distribution that was witnessed in knowledge-based economies in the past several decades. The era of the knowledge-based economy saw a steep rise in the share of intangible assets in the market capitalization of companies and a steady rise in the profit share of national income. AI applications promise to intensify these trends: deployed as a factor of production, AI can be thought of as "machine knowledge capital." In this role, it competes for income share with white-collar work. In addition, by making robots more flexible, AI allows machines to compete away a still greater income share from manual labour. Given the economics of "superstars" (Rosen 1981), the best AI applications will capture disproportionate market share and outsized returns. As protected IP, AI will thus further skew income flows and wealth shares.

From the patterns of income distribution observed in the last few decades, the most prosperous communities will be those that collect the rent in this asset-based economy; the least prosperous will be those that pay the rent. The income gradient across these communities will be steep and result in commensurate skewing of economic welfare, access to services and even lifespan. The question that communities and the societies in which they are embedded will face is how to actually capture benefits in this economy and how to distribute them. The system will need to have the flexibility to allow experimentation.

Innovation System Dynamism

Communities that have the capacity to innovate will prosper if they accumulate rent-generating technology. Doing so means accumulating a roster of companies that apply and develop technology; it also can involve providing public support for the scaling up of start-ups and promoting outward investment to acquire technology or technology-rich companies. By the same token, communities will also have an interest in protecting their innovation systems from what would be (from their perspective) inward foreign direct investment (FDI) that is extractive or predatory in nature.

Traditional frameworks for FDI have been premised on the understanding that FDI brought with it technology and best practices, as well as connections to global markets. However, in the innovation sectors, FDI can be dangerous. The US Department of Justice and Federal Trade Commission have launched investigations of the major US tech companies' business practices, including as to whether they have engaged in anticompetitive mergers or acquisitions (Kendall, McKinnon and Seetharaman 2019). National policy frameworks for FDI thus need to be reviewed and likely revised. Other issues that need review include the role of FDI by state-owned or state-linked enterprises and how to ensure that developing countries are not denied the capacity to benefit from knowledge spillovers by allowing for technology transfer conditionality in FDI approvals, which is contrary to where the current discussion of China's development policies is going.

The Sovereignty Pillar

Given the shift of political discourse onto digital platforms where it is susceptible to manipulation, the sovereignty pillar becomes an essential part of the governance regime. The sovereignty pillar safeguards the integrity of a country's social choice mechanisms, which, in turn, determine everything from the political stripe of the governing party to gender policies, environmental commitments, and distributional issues such as access to health care, low income support and so forth.

The issue of sovereignty, however, raises the risk of "system friction" (Ostry 1992). Historically and traditionally, social norms have differed across countries; the implications of these differences may get amplified in the digital age. One can contrast, for example, the concerns over China's

use of digital technologies (including facial recognition) for purposes of its Social Credit reputation-scoring system with those over digital personal rating systems employed in Western market contexts by eBay, Airbnb, credit rating services and so forth, which operate in similar ways. Although surveillance capitalism raises its share of worries (Zuboff 2019), the differences in context — including the role of state power and the absence of an independent judiciary in China — heighten for many the threat perception in the latter context (Kobie 2019).

Difficulties also emerge in another dimension. Biometric data technology — ranging from facial recognition to retina or iris scans, fingerprints, voiceprints, scans of hands and so forth[4] — is being deployed ubiquitously in the absence of elaborated protocols for use,[5] with no social consensus within polities and certainly without a widely accepted useful standard for multilateral purposes.

The most prominent current flashpoint is facial recognition, and it is meeting with resistance at the grassroots of societies. For example, calls have been made for a moratorium on the deployment of facial recognition in the United States (Garvie and Moy 2019). San Francisco has issued an ordinance banning its use by city agencies, including the police force, based on an assessment that the "propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits, and the technology will exacerbate racial injustice and threaten our ability to live free of continuous government monitoring."[6] Protesters from Hong Kong to Santiago to Baghdad have attacked surveillance cameras as the visible manifestation of state control (and, in Hong Kong, they have adopted technology to defeat surveillance [Mahtani 2019], a sign of things to come).

Privacy policy also faces more general issues. In the absence of a commonly accepted definition, there are different traditions in defining what constitutes "personal data" or "personally identifiable information" (Schwartz and Solove 2011) and in identifying the limits on information use, data collection or disclosure of information (Schwartz and Solove 2014). While it is almost universally accepted that individual privacy should be safeguarded, there are policy trade-offs associated with stricter privacy rules. For example, since data (including personal data) is an input for AI algorithms, stricter regulations can jeopardize the development of AI applications. At the same time, companies that embrace stricter data policy regulations can increase clients' confidence and attract more users (Goldfarb and Tucker 2012).

Such trade-offs set up a tension within national policy frameworks that will likely resolve in different policy mixes in countries with strong "offensive" potential in the data-driven economy, versus those with mainly "defensive" interests. These outcomes might vary systematically across countries by size, with different choices being seen as optimal for large versus small population economies. In the international context, there is potential for a regulatory race to the bottom, as some countries adopt lax privacy policies with a view to supporting domestic companies to grow and also to attract FDI. In this regard, Avi Goldfarb and Daniel Trefler (2019) compare privacy policies to labour and environmental regulations, where some evidence of this dynamic has been found (Davies and Vadlamannati 2013; Beron, Murdoch and Vijverberg 2003; Fredriksson and Millimet 2002).

Established WTO Mechanisms

With steeply increasing cross-border transfers of data, including personal information, differences in regulatory approaches could create system friction and ultimately require international arbitration. In this regard, WTO law contains some important built-in flexibilities, including in the General Agreement on Tariffs and Trade (GATT), GATS and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement). These flexibilities are established through the "general exceptions," which seek to balance economic and non-economic

4 This list is from the Illinois General Assembly (2008).

5 Darrell West (2019) makes 10 recommendations for promoting the acceptable of use of facial recognition, but this proposed list underscores the absence of an agreed framework.

6 See City of San Francisco (2019, art. 1(d)). In addition to this San Francisco ordinance, three states (Illinois, Texas and Washington) have biometric privacy laws, and a recent legal test under the 2008 Illinois Biometric Information Privacy Act enforced a penalty for the non-consensual taking of a fingerprint of a minor as a biometric entry pass into an amusement park (Gemalto 2020). However, the United States has emphasized self-regulation by data firms at the federal level, making it legal in the other 47 states for software to identify an individual using images taken without consent while they are in public (ibid.). The European Union sees things differently, having outlawed the non-consensual harvesting of biometric data under its General Data Protection Regulation (GDPR).

interests (such as, for example, protection of public morals or public order). Analysis of the history of the use of these exceptions sheds some light on the ways the sovereignty pillar can be implemented in the emerging digital economy, taking into account, of course, the general provisos that WTO dispute settlement decisions have no formal precedent value for future cases[7] and that the data-driven economy will likely create novel factual circumstances.

With respect to goods trade, GATT article XX (general exceptions) has featured prominently in a number of WTO disputes (Ministry of Economy, Trade and Industry 2016, part II, chapter 4). While GATT applicability to future digital trade disputes might be quite limited, given the nature of the data-driven economy,[8] the GATT history does provide some insights. First, panels have taken into account the relationships between policy objectives (the "justifiable reasons") and measures, as well as the appropriateness of the methods used; in particular, they have examined whether the measures of concern can reasonably be explained by the policy objectives and whether less-trade-restrictive measures are available. Second, actual impacts on trade were examined. Overall, there are few instances where a defence based on justifiable reasons was upheld; in most cases, the measures were determined to be inconsistent with the WTO agreements. This tendency may be read as bias in favour of trade or as the result of a selection process that results in weak cases not going to the panel stage.

With respect to services trade, there has been only one dispute that directly invoked the relevant GATS measure, article XIV (general exceptions) — namely, *United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services* (*US — Gambling*), the complaint initiated by Antigua and Barbuda.[9] The complainants argued that the US ban on online gambling was inconsistent with its commitments under GATS; the United States countered that its measures were covered by the "public morals" exception allowed under GATS article XIV. This case established the applicability of GATS to the digital realm through the principle of technological neutrality with regard to the different modes of supply: "prohibition on one, several or all of the means of delivery included in mode 1... constitutes a limitation on the total number of service operations...within the meaning of Article XVI:2(c)" (cited in Burri 2017, 97).[10] Upon appeal, the Appellate Body found that the case advanced by the United States failed to satisfy the requirements of the chapeau of article XIV[11] and thus found the measure to be protectionist. This decision suggests that high standards would be applied for data and privacy measures that hinder trade.

While GATS article XIV(c)(ii) provides for exceptions based on "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts," privacy policy has not yet been addressed within the WTO dispute settlement process.[12]

Workability of WTO Disciplines in the Digital Age

The foregoing suggests that the WTO framework provides scope for countries to establish rules in areas of sovereign governance for the digital realm and to defend them in international arbitration, while still imposing disciplines on outright protectionism.

Many countries follow the so-called "geographically based approach" to data privacy: data must be protected where it is created and, in order

7 The informal practice of treating past decisions as precedents has been argued by the United States to inappropriately qualify members' rights and obligations. This is one of the bones of contention that have led to the suspension of the Appellate Body. Steve Charnovitz (2019), however, documents past US reliance on precedents in GATT/WTO disputes.

8 The issue of whether digital products are goods or services or something else has not been resolved at the WTO. This issue is under discussion in the context of the WTO moratorium on tariffs on electronic transmissions.

9 See www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm.

10 Further to this point, the Appellate Body's December 21, 2009, ruling in a later dispute, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, clarified that distribution can cover both physical delivery and online delivery. See www.wto.org/english/tratop_e/dispu_e/cases_e/ds363_e.htm.

11 In *US – Gambling*, the Appellate Body viewed the chapeau as establishing three prohibitions: against arbitrary discrimination between countries where the same conditions prevail; against unjustifiable discrimination between countries where the same conditions prevail; and against the use of a justification as a disguised restriction on international trade. These standards are cumulative in nature.

12 Scholars have considered a hypothetical challenge of data privacy regulations within the WTO legal system (Thierer 2018). Its application critically depends on the scope of the definition of the private sphere of individuals. That being said, L. Lee Tuthill (2016) and Daniel Crosby (2016) argue that the WTO agreements provide sufficient policy room to impose limitations on data flows or to require data localization on grounds of privacy and data protection.

to export data, the destination country must demonstrate that it has equivalent levels of protection. This approach implies that the source country determines the minimum level of data protection, which invokes the principle of an "adequate level of data protection" (Weber 2012); however, adequacy is in the eyes of national legislatures, and democratic legitimacy will demand that minimum standards not become de facto maximum ceilings for protection.

In any litigation, of particular importance would be the relationship of the issue in relation to trade. Where a case involves the GATS, a country's schedule of individual commitments comes into play: if a country did not undertake any liberalization obligations in a particular services sector, it would be fully safeguarded in applying a discriminatory measure in such a sector. In this regard, the lack of progress on the Trade in Services Agreement means that many countries have more policy space available to adapt as regulation for the digital transformation, without constraint of trade rules. If the active discussions on an e-commerce agreement reach fruition, that flexibility would be circumscribed, although countries would have had a reasonable forewarning of the issues.

One major caveat applies: the introduction of data measures in regional preferential agreements, in particular through the Comprehensive and Progressive Agreement for Trans-Pacific Partnership and the CUSMA, circumscribes flexibility. For example, while these agreements recognize the legitimacy of measures for online consumer protection, personal information protection and shielding from unsolicited commercial electronic communication, the robustness of the measures is left largely to the discretion of domestic regulators, and measures must be consistent with the primary objective of ensuring the flow of data across borders. Thus, the CUSMA states unequivocally in article 19 that "no 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." This stipulation sets up a potentially problematic regulatory chill in an area where regulation has yet to catch up with risks and is not yet "treaty ready" (Ciuriak 2018a).

The National Security Pillar

The WTO national security exceptions as set out in GATT article XXI were crafted in 1947 in light of the experience of World War II. They allow countries to take trade measures that are otherwise inconsistent with their GATT/WTO obligations under circumstances that relate to fissionable materials (that is, nuclear weapons), traffic in arms, or measures taken in time of war or other emergencies in international relations. These measures were framed for a membership that was essentially co-extensive with a hegemonic region, conceived in an era when physical borders also were largely coincident with economic borders, and based on implicit assumptions that physical borders were effectively policed and defended.

These are not the conditions that raise concerns in the modern digital context. Reflecting this, the recently concluded CUSMA, which provides national security exceptions using article XXI-type language, drops the specific examples. However, by not replacing them, it leaves open the question of what would be the scope of threats that would rise to a level that warrants invoking a national security exception to limit trade or other commercial interactions. In particular, the requirement of an "emergency" to defend measures under the existing WTO regime is hard to read in the kinds of national security concerns that have been raised in connection with the IoT infrastructure build-out, which have to do with access to data on an ongoing basis through backdoors in IoT equipment and so forth.

Experience in Applying the National Security Exception under the Rules-based System

The challenge of developing a national security exception fit for purpose for the digital age is made more difficult by the fact that the WTO has little experience in dealing with national security issues as an exception. GATT article XXI was not invoked for the first 70 years following its introduction. The comparable provisions under the GATS' article XIV *bis* and under the TRIPS Agreement's article 73 have never been tested.

This Pandora's box has now been opened and a number of trade-restrictive policies that were justified on national security grounds have been challenged at the WTO. Current disputes include several mounted in respect of national security tariffs imposed by the United States on imports of steel and aluminum. Qatar has brought a case against the United Arab Emirates; the latter objected to Qatar's panel request, saying that it and eight other countries were forced to take measures in response to Qatar's funding of terrorist organizations, citing article 73 of the TRIPS Agreement, as well as article XXI of the GATT and article XIV *bis* of the GATS.[13] China has raised Australia's exclusion of Huawei from its rollout of fifth-generation (5G) networks at the WTO Council on Goods, labelling Australia's measures a "discriminatory market access prohibition on 5G equipment" (WTO 2019d). Another dispute that might involve national security is the request for WTO consultations by Korea in respect of Japan's Amended Export Licensing Policies and Procedures, which Korea argues impose "unduly stringent export licensing policies and procedures whenever export of such products and technologies are destined for Korea" (WTO 2019e; Sugiyama 2019b).

So far, only one case, *Russia — Measures Concerning Traffic in Transit* (*Russia — Transit*), brought by Ukraine against the Russian Federation, has gone the distance in WTO dispute settlement, with an unchallenged panel report released (WTO 2019b). One of the major issues addressed in this case is whether the national security exception is wholly "self-judging" or "non-justiciable" (for a discussion of this issue, see, for example, Alford 2011). If it were deemed to be so, a WTO member invoking this exception would be free to determine whether the applied measure is in its own national security interests and the WTO panel could make no further findings in this regard. Russia, supported by the United States, argued in favour of this interpretation; the WTO panel, however, ruled otherwise, making a strong statement that WTO rules do indeed determine the legitimacy of measures applied under the security exceptions (this has been described as the panel asserting WTO "stewardship" over the trade system in this respect; Heath 2019).

A second issue addressed by the panel — and arguably the more important one from the perspective of framing a national security exception for the digital economy — was the requirement for an emergency for the national security exception to be sustained: that is, there must be "a fundamental change of circumstances which radically alters the factual matrix" (WTO 2019b, para. 7.108). Having identified an emergency in international relations, the panel found that the measures in question were not "so remote from, or unrelated to" the emergency as to make it "implausible" that they were adopted to protect Russia's essential security interests as impacted by that emergency (ibid., para. 7.145). The panel's decision was not appealed, leaving the panel report as the sole WTO jurisprudence on this issue.

A third issue is that governments contesting national security matters are unlikely to divulge information that could be used to infer their capabilities or methods; remarkably, in *Russia — Transit*, the two antagonists discussed the national security event of concern as only hypothetical (Heath 2019)! The tendency of governments to treat any information bearing on national security as classified suggests that there will be non-trivial problems in establishing the fact base to be considered in adjudicating a trade dispute triggered by a cyber incident.

The framing of a national security exemption for the digital age has not been materially advanced through regional trade agreements.[14]

Toward a National Security Exception for the Digital Era

The foregoing leads to several conclusions. First, the legacy measures in the WTO Agreement do not provide a compelling intuitive point of departure for a workable framework for the digital domain; the national security exceptions will thus likely need to be developed on a tabula rasa basis. Second, the emergence of new threats across the entire economic spectrum means that commitments to services trade made in the context of the economy as it was in the early 1990s, which

13 The panel in this case, DS526, has requested an extension and indicated its report would not be circulated until the second half of 2020 (WTO 2019f).

14 Cyber security is addressed in the CUSMA in article 19.15, but this agreement uses non-binding language that only stipulates that countries "shall endeavor" to "build the capabilities of their respective national entities responsible for cybersecurity incident response" and "strengthen existing collaboration mechanisms for cooperating." In addition, the CUSMA recognizes and promotes the risk-based approach to cyber security issues.

informed the negotiation of the WTO, need to be reviewed. This process would ideally also be carried out in the context of the negotiation of a new WTO instrument addressing data. Third, drawing a clear distinction between digital flows that constitute "digital products" and "electronic transmissions" in general would help limit the intrusion of the unconstrained national security regime for information into the generally well-regulated world of trade in goods and services.

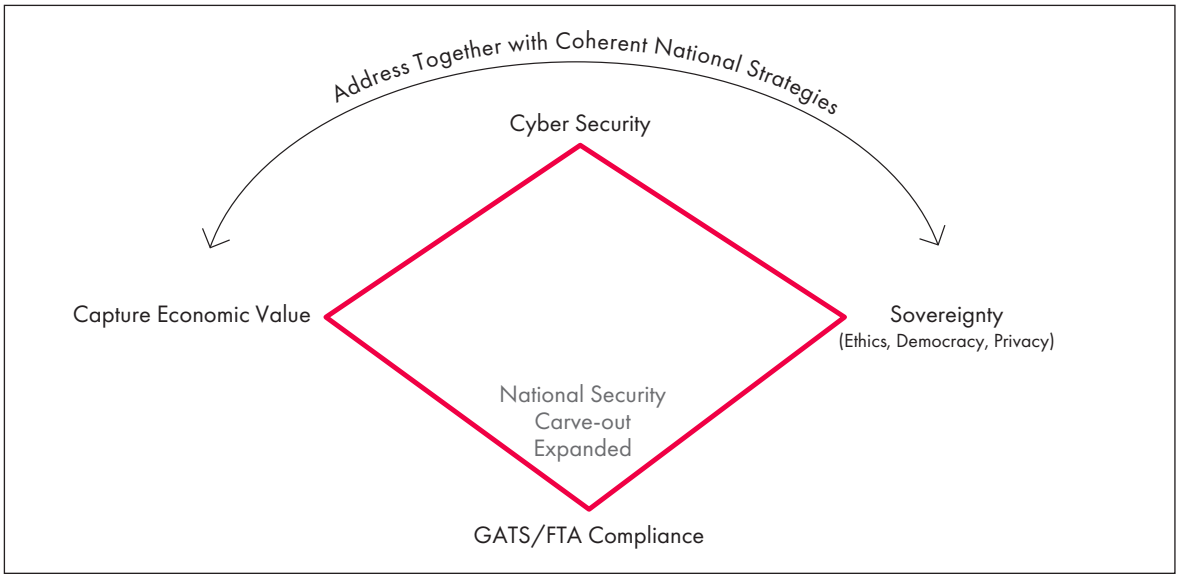
Discussion: Toward a Global Data Governance Framework

Given that the state remains the basic unit for economic and social organization in the most fundamental terms of safeguarding national security, establishing economic frameworks and providing for social security (a point that has been underscored by the national responses to the COVID 19 pandemic), a priority will inevitably be placed by states on preserving their ability to carry out these functions as the digital transformation unfolds. In this regard, they face challenges at two levels: reconciling the tensions between these three primary objectives at the national level; and managing their international relations in a context where international treaties constrain policy space. Jim Balsillie (2018) describes how this challenge can be visualized (see Figure 1).

Ideally, domestic policy frameworks would have been adapted to the digital age and coherent national strategies would have been developed before international treaties were negotiated. However, governments do not have the luxury of starting with a clean slate on which to etch their idealized schemes. Moreover, there are several major complicating factors.

First, the three major digital jurisdictions — the United States, China and the European Union — have sharply differing strategies, which reflect the hands that they hold (Ciuriak and Ptashkina 2018). The EU implementation has placed greater weight on the sovereignty pillar, emphasizing privacy protection and the development of its internal Digital Single Market (Viola 2018), notwithstanding concerns that this approach is holding back its ability to develop its digital economy to capture economic value (for example, see comments from Jack Ma, then chairman of Alibaba, cited in Soo [2019]). The United States has opted for an open

Figure 1: Policy Framework for the Knowledge-based, Data-driven Economy



Source: Adapted and reprinted with permission from Balsillie (2018).
Note: FTA = free trade agreement.

trade regime, as this enables its leading firms to capture economic value globally, except in areas where China has taken a lead, where the United States emphasizes national security (although the breadth of the national security claims makes them colourable as tactics for value capture in a contest with Chinese interests). China emphasizes sovereignty but, unlike the European Union, with a national security angle, as its Great Firewall controls the messaging within its national borders. As a by-product, the Great Firewall also enables China to capture economic value through the promotion of local companies, such as, for example, WeChat (competitor of WhatsApp and Facebook) or Alibaba (competitor of Amazon).

This strategic behaviour on the part of the three main digital jurisdictions creates stumbling blocks for small open economies, which need national data strategies to capture value, but also need to comply with the European Union's GDPR and face both geopolitical pressure to align on national security grounds and geo-economic pressure aimed at limiting their ability to capture rents. Developing countries, which are rules- and regime-takers, are most vulnerable in this context and need a multilateral process in which they have greater collective bargaining power to establish a sustainable arrangement. Of particular importance in this regard would be a resolution to the WTO moratorium on tariffs on digital products and to the OECD/G20 Inclusive Framework discussions on nexus and profit allocation rules, which take into account the principle of aligning profits with underlying economic activities and value creation in the new digital context (OECD 2019b).

Second, in our information society, control of information represents an independent source of power. Accordingly, the major platform companies are themselves significant players in shaping the rules. With effectively unlimited financial resources showered on them by financial markets supercharged by negative real policy interest rates, and exploiting the technology newly developed by millions of highly trained Ph.D.s around the world, modern tech CEOs have power over resources that rivals that of most governments and engage in such projects as space flight that formerly were the sole province of the state. Moreover, they have influence over public opinion that dwarfs that of the traditional newspapers of record, yet do not face the checks and balances that circumscribe the political power of the Fourth Estate in traditional democracies — especially as regards transparency.

Third, the institution best placed to host the negotiation of a new interface between nations and the international commercial system — the WTO — has been effectively sidelined. As summarized in Ciuriak (2019b), the various reform efforts currently under way would ideally be integrated to ensure a coherent regime that would likely feature significant reforms in at least eight major areas:

- a regime for the trade-related aspects of data exchange;
- the sovereignty exceptions outlined above;
- the national security exception regime;
- a regime for most-favoured-nation treatment in the digital domain and for granting preferences as a derogation from that regime;
- competition policy measures tailored for a world of global superstar firms;
- an updated IP regime that reflects the changed nature of innovation and the advent of new forms of IP, such as AI;
- an investment regime tailored for the knowledge-based, innovation-intensive economy, where knowledge spillovers are a vital asset underpinning development; and
- an overhaul of the treatment of the public sector role in the economy (an issue that is likely to move front and centre in a post-pandemic context).

The regulation of data flows and digital trade is an area of active international ferment with multiple exercises under way in various multilateral institutions, at the national level, and in ad hoc policy forums worldwide. This paper's analysis supports a broadened framework for integrating multiple threads, starting with the e-commerce negotiations, other work programs under the WTO and the G20 initiatives, but also integrating the work in more specialized areas, such as competition policy and IP, and in multi-stakeholder processes addressing the plethora of social governance issues that are emerging with the digital transformation. While it is not likely that a new "digital round" can be mobilized before a détente is reached in the technology war between the United

States and China, the rapidity of change in the modern innovation context — where machine learning collapses the time to explore innovation space — suggests that time is of the essence in working out a sustainable "solution space" for this new economy. The future will come soon enough — and probably sooner than we think.

Works Cited

Ahmed, Nasma, Matthew Claudel, Zahra Ebrahim, Christopher Pandolfi and Bianca Wylie, eds. 2019. *Some Thoughts...* https://some-thoughts.org/doc/Somethoughts.pdf.

Alford, Roger. 2011. "The Self-Judging WTO Security Exception." *Utah Law Review* 2011 (3): 697–759.

Balsillie, Jim. 2018. "Measuring Intangible Assets (IP & Data) for the Knowledge-based and Data-driven Economy." Presentation to the IMF Statistical Forum, November 20. www.imf.org/en/News/Seminars/Conferences/2018/04/06/6th-statistics-forum.

Beron, Kurt J., James C. Murdoch and Wim P. M. Vijverberg. 2003. "Why Cooperate? Public Goods, Economic Power, and the Montreal Protocol." *The Review of Economics and Statistics* 85 (2): 286–97.

Burri, Mira. 2017. "The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation." *UC Davis Law Review* 51: 65–133. https://lawreview.law.ucdavis.edu/issues/51/1/Symposium/51-1_Burri.pdf.

Butler, Bob and Irving Lachow. 2012. "Multilateral Approaches for Improving Global Security in Cyberspace." In "International Engagement on Cyber 2012: Establishing Norms and Improving Security," special issue, *Georgetown Journal of International Affairs*: 5–14.

Chander, Anupam. 2019. "The Internet of Things: Both Goods and Services." *World Trade Review* 18 (S1): s9–s22.

Charnovitz, Steve. 2019. "The Myth of No WTO Precedent: The Attack on the Appellate Body — Events of 9 December 2019." *International Economic Law and Policy* (blog), December 9. https://ielp.worldtradelaw.net/2019/12/the-myth-of-no-wto-precedent.html.

Chernenko, Elena, Oleg Demidov and Fyodor Lukyanov. 2018. "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms." Council of Councils Global Governance Working Paper, February 23. New York, NY: Council on Foreign Relations.

CIGI. 2018. *A National Data Strategy for Canada: Key Elements and Policy Considerations*. CIGI Paper No. 160. Waterloo, ON: CIGI. www.cigionline.org/publications/national-data-strategy-canada-key-elements-and-policy-considerations.

City of San Francisco. 2019. "Administrative Code — Acquisition of Surveillance Technology." Draft as amended in Committee, May 6. File No. 190110. https://sfbos.org/ordinances-2019.

Ciuriak, Dan. 2018a. *Digital Trade: Is Data Treaty-Ready?* CIGI Paper No. 162. Waterloo, ON: CIGI. www.cigionline.org/publications/digital-trade-data-treaty-ready.

———. 2018b. "The Economics of Data: Implications for the Data-Driven Economy." In *Data Governance in the Digital Age*. CIGI Essay Series. Waterloo, ON: CIGI. www.cigionline.org/publications/data-governance-digital-age.

———. 2019a. *The Data-driven Economy: Implications for Canada's Economic Strategy*. CIGI Policy Brief No. 151. Waterloo, ON: CIGI. www.cigionline.org/publications/data-driven-economy-implications-canadas-economic-strategy.

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

———. 2019c. "Data as a Contested Economic Resource: Framing the Issues." Paper presented at the Just Net Coalition, Friedrich Ebert Foundation and Bread for the World Workshop, "Data and Digital Intelligence as People's Resources: Reclaiming Freedom and Control in a Data-based Society," Berlin, Germany, November 23–24.

Ciuriak, Dan and Maria Ptashkina. 2018. "Started the digital trade wars have: Delineating the regulatory battlegrounds." Opinion, RTA Exchange, January 9. Geneva, Switzerland: International Centre for Trade and Sustainable Development.

Crosby, Daniel. 2016. "Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments." E15 Initiative Policy Brief, March. Geneva, Switzerland: International Centre for Trade and Sustainable Development and World Economic Forum.

Davies, Ronald B. and Krishna Chaitanya Vadlamannati. 2013. "A Race to the Bottom in Labor Standards? An Empirical Investigation." *Journal of Development Economics* 103 (1): 1–14.

European Commission. 2017. "Investing in a smart, innovative and sustainable Industry: A renewed EU Industrial Policy Strategy." Document No. COM(2017) 479 final, September 13. Brussels, Belgium: European Commission.

———. 2019. "The EU Cybersecurity Act brings a strong agency for cybersecurity and EU-wide rules on cybersecurity certification." News Digibyte, June 26. https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity.

European Parliament Research Service. 2015. "Industry 4.0: Digitalisation for productivity and growth." Briefing, September 22. Brussels, Belgium: European Parliament. www.europarl.europa.eu/RegData/etudes/BRIE/2015/568337/EPRS_BRI(2015)568337_EN.pdf.

Fredriksson, Per G. and Daniel L. Millimet. 2002. "Strategic Interaction and the Determination of Environmental Policy across U.S. States." *Journal of Urban Economics* 51 (1): 101–22.

Garvie, Clare and Laura M. Moy. 2019. *America Under Watch: Face Surveillance in the United States*. Washington, DC: Center on Privacy & Technology, Georgetown Law. www.americaunderwatch.com/.

Gates, Melinda and Jack Ma (co-chairs). 2019. *The Age of Digital Interdependence: Report of the UN Secretary-General's High-level Panel on Digital Cooperation*. Geneva, Switzerland: United Nations.

Gemalto. 2020. "Biometric data and data protection regulations (GDPR and CCPA)." Gemalto.com, January. www.gemalto.com/govt/biometrics/biometric-data.

Goldfarb, Avi and Daniel Trefler. 2019. "Artificial Intelligence and International Trade." In *The Economics of Artificial Intelligence: An Agenda*, edited by Ajay Agrawal, Joshua Gans and Avi Goldfarb, 463–92. Cambridge, MA: National Bureau of Economic Analysis.

Goldfarb, Avi and Catherine Tucker. 2012. "Privacy and Innovation." In *Innovation Policy and the Economy* (12), edited by Josh Lerner and Scott Stern, 65–90. National Bureau of Economic Analysis.

Grossman, Gene M. 1990. "Promoting new industrial activities: A survey of recent arguments and evidence." *OECD Journal: Economic Studies* 14: 87–125.

Heath, J. Benton. 2019. "Trade, Security and Stewardship (Part III): WTO Panels as Factfinders under Article XXI." *International Economic Law and Policy Blog*, May 7. https://ielp.worldtradelaw.net/.

HM Government. 2017. *Industrial Strategy: Building a Britain fit for the future*. Industrial Strategy White Paper. London, UK: Government of the United Kingdom.

Hufbauer, Gary Clyde. 2020. "How Congress Can Help Overturn the French Digital Tax." *Realtime Economic Issues Watch* (blog), January 7. Washington, DC: Peterson Institute for International Economics. www.piie.com/blogs/realtime-economic-issues-watch.

Illinois General Assembly. 2008. *Biometric Information Privacy Act*. 740 ILCS 14/1 et seq. www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

Janow, Merit E. and Petros C. Mavroidis. 2019. "Digital Trade, E-Commerce, the WTO and Regional Frameworks." *World Trade Review* 18 (S1): S1–S7.

Kendall, Brent, John D. McKinnon and Deepa Seetharaman. 2019. "FTC Antitrust Probe of Facebook Scrutinizes Its Acquisitions." *The Wall Street Journal*, August 1.

Kobie, Nicole. 2019. "The complicated truth about China's social credit system." *Wired*, June 7.

Leyser, Ottoline and Genevra Richardson, eds. 2018. *Data ownership, rights and controls: Reaching a common understanding — Discussions at a British Academy, Royal Society and techUK seminar on 3 October 2018*. London, UK: British Academy.

Mahtani, Shibani. 2019. "Hong Kong protesters coordinate tech-savvy effort to beat Chinese state surveillance." *The Independent*, June 16. www.independent.co.uk/news/world/asia/hong-kong-protests-china-surveillance-tech-telegram-extradition-bill-a8960911.html.

McDonald, Sean. 2019. "Reclaiming Data Trusts." Opinion, March 5. www.cigionline.org/articles/reclaiming-data-trusts.

———. 2020. "The Digital Response to the Outbreak of COVID-19." Opinion, March 30. www.cigionline.org/articles/digital-response-outbreak-covid-19.

Ministry of Economy, Trade and Industry. 2016. "Chapter 4: Justifiable Reasons." In *2016 Report on Compliance by Major Trading Partners with Trade Agreements: WTO, EPA/FTA and IIA*, "Part II: WTO Rules and Major Cases," 327–50. Tokyo, Japan: Ministry of Economy, Trade and Industry. www.meti.go.jp/english/report/data/2016WTO/gCT16_1coe.html.

Morisson A. and M. Pattinson. 2019. "Industry 4.0: A Policy Brief from the Policy Learning Platform on Research and innovation." Lille, France: Interreg Europe Policy Learning Platform. www.interregeurope.eu/fileadmin/user_upload/plp_uploads/policy_briefs/INDUSTRY_4.0_Policy_Brief.pdf.

OECD. 2019a. "Data in the Digital Age." OECD Going Digital Policy Note, March. Paris, France: OECD. www.oecd.org/going-digital/data-in-the-digital-age.pdf.

———. 2019b. "Secretariat Proposal for a 'Unified Approach' under Pillar One." Public Consultation Document, October 9–November 12. Paris, France: OECD.

Ostry, Sylvia. 1992. "The domestic domain: the new international policy arena." *Transnational Corporations* 1 (1): 7–26.

Rosen, Sherwin. 1981. "The Economics of Superstars." *The American Economic Review* 71 (5): 845–58.

Scassa, Teresa. 2019. "Why Canada needs a national data strategy." *Policy Options*, January 15. Montreal, QC: Institute for Research on Public Policy.

Schwartz, Paul M. and Daniel J. Solove. 2011. "The PII Problem: Privacy and a New Concept of Personally Identifiable Information." *New York University Law Review* 86: 1814–94.

———. 2014. "Reconciling Personal Information in the United States and European Union." *California Law Review* 102 (4): 877–916.

Soo, Zen. 2019. "Alibaba's Jack Ma says he is 'worried' Europe will stifle innovation with too much tech regulation." *South China Morning Post*, May 17. www.scmp.com/tech/big-tech/article/3010606/alibabas-jack-ma-says-he-worried-europe-will-stifle-innovation-too.

Stone, Tobias. 2019. "Summary of the 'Disinformation and "fake news": Final Report' published by the Digital, Culture, Media and Sport Committee of the British Parliament." *Medium*, March 5. https://medium.com/@tswriting/summary-of-disinformation-and-fake-news-final-report-published-by-the-digital-culture-media-4e62158be7c2.

Sugiyama, Satoshi. 2019a. "Abe heralds launch of 'Osaka Track' framework for free cross-border data flow at G20." *The Japan Times*, June 28. www.japantimes.co.jp/news/2019/06/28/national/abe-heralds-launch-osaka-track-framework-free-cross-border-data-flow-g20.

———. 2019b. "Japan agrees to WTO consultation with South Korea amid trade dispute." *The Japan Times*, September 20. www.japantimes.co.jp/news/2019/09/20/business/japan-agrees-wto-consultation-south-korea-amid-trade-dispute.

Taulli, Tom. 2019. "Why PayPal Paid $4 Billion for Honey Science." *Forbes*, November 23.

The Economist. 2017. "The world's most valuable resource is no longer oil, but data." *The Economist*, May 6.

Thierer, Johannes. 2018. "Privacy as an Obstacle: Data Privacy Laws under the GATS." *Freilaw* 01/2018: 8–15.

Tuthill, L. Lee. 2016. "Cross-border data flows: What role for trade rules?" In *Research Handbook on Trade in Services*, edited by Pierre Sauvé and Martin Roy, 357–84. Cheltenham, UK: Edward Elgar Publishing.

US-China Trade Policy Working Group. 2019. *US-China Trade Relations: A Way Forward*. The US-China Trade Policy Working Group Joint Statement, Shanghai, October 18. https://rodrik.typepad.com/US-China%20Trade%20Relations%20-%20A%20Way%20Forward%20Booklet%20(for%20print).pdf.

Viola, Roberto. 2018. "European Dimension of the Digital Economy." *Shaping Europe's digital future* (blog), September 28. https://ec.europa.eu/digital-single-market/en/blogposts/european-dimension-digital-economy.

Weber, Rolf H. 2012. "Regulatory Autonomy and Privacy Standards under the GATS." *Asian Journal of WTO & International Health Law and Policy* 7 (1): 25–48.

West, Darrell M. 2019. "10 actions that will protect people from facial recognition software." Artificial Intelligence and Emerging Technology Initiative report, October 31. Washington, DC: Center for Technology Innovation at Brookings. www.brookings.edu/research/10-actions-that-will-protect-people-from-facial-recognition-software/.

White House. 2020. "Budget 2020: Research and Development." Washington, DC: The White House. www.whitehouse.gov/wp-content/uploads/2019/03/ap_21_research-fy2020.pdf.

WTO. 2019a. *Joint Statement on Electronic Commerce*. WTO Doc. No. WT/L/1056, January 25.

———. 2019b. *Russia — Measures Concerning Traffic in Transit: Report of the Panel*. WTO Doc. No. WT/DS512/R, April 5. www.wto.org/english/tratop_e/dispu_e/512r_e.pdf.

———. 2019c. "Workshop on the moratorium on customs duties on electronic transmissions." April 29. Geneva, Switzerland: WTO. www.wto.org/english/tratop_e/ecom_e/wkmoratorium29419_e.htm.

———. 2019d. "Members adopt draft decision to improve tariff and import data, discuss trade concerns." News, May 28. www.wto.org/english/news_e/news19_e/mark_28may19_e.htm.

———. 2019e. *Japan — Measures Related to the Exportation of Products and Technology to Korea: Request for Consultations by the Republic of Korea*. WT/DS590/1, G/L/1325, G/TFA/D3/1, G/TRIMS/D/45, S/L/431, IP/D/42, September 16. www.wto.org/english/tratop_e/dispu_e/cases_e/ds590_e.htm.

———. 2019f. *United Arab Emirates — Measures Relating to Trade in Goods and Services, and Trade-Related Aspects of Intellectual Property Rights: Communication from the Panel*. WTO Doc. No. WT/DS526/4, October 2. www.wto.org/english/tratop_e/dispu_e/cases_e/ds526_e.htm.

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

Centre for International
Governance Innovation

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

@cigionline