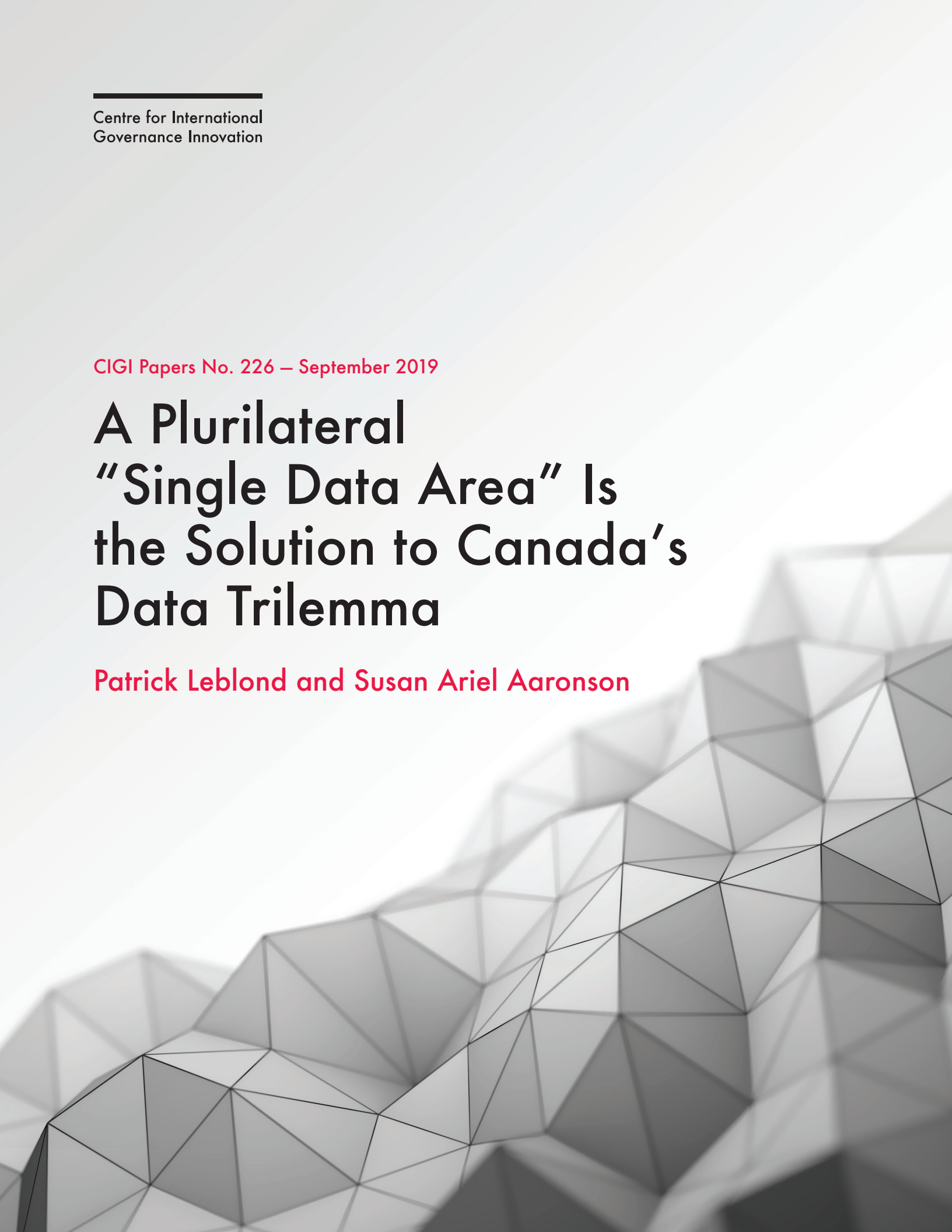
Centre for International
Governance Innovation

CIGI Papers No. 226 — September 2019

A Plurilateral "Single Data Area" Is the Solution to Canada's Data Trilemma

Patrick Leblond and Susan Ariel Aaronson



Centre for International
Governance Innovation

CIGI Papers No. 226 — September 2019

A Plurilateral "Single Data Area" Is the Solution to Canada's Data Trilemma

Patrick Leblond and Susan Ariel Aaronson

About CIGI

We are the Centre for International Governance Innovation: an independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis.

Our research initiatives focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners and have received support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

À propos du CIGI

Au Centre pour l'innovation dans la gouvernance internationale (CIGI), nous formons un groupe de réflexion indépendant et non partisan doté d'un point de vue objectif et unique de portée mondiale. Nos recherches, nos avis et nos interventions publiques ont des effets réels sur le monde d'aujourd'hui car ils apportent de la clarté et une réflexion novatrice pour l'élaboration des politiques à l'échelle internationale. En raison des travaux accomplis en collaboration et en partenariat avec des pairs et des spécialistes interdisciplinaires des plus compétents, nous sommes devenus une référence grâce à l'influence de nos recherches et à la fiabilité de nos analyses.

Nos projets de recherche ont trait à la gouvernance dans les domaines suivants : l'économie mondiale, la sécurité et les politiques internationales, et le droit international. Nous comptons sur la collaboration de nombreux partenaires stratégiques et avons reçu le soutien des gouvernements du Canada et de l'Ontario ainsi que du fondateur du CIGI, Jim Balsillie.

Credits

Director, Global Economy Robert Fay
Program Manager Heather McNorgan
Senior Publications Editor Jennifer Goyder
Graphic Designer Brooklynn Schwartz

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

Table of Contents

About the Authors

Patrick Leblond is a CIGI senior fellow. He is an expert in global economic governance and international political economy, regional economic integration, financial regulation, and business and public policy. At CIGI, Patrick specializes in the investigation of international trade in the areas of Canada's trade and economic agreements as well as its involvement in the multilateral system. Alongside his CIGI appointment, Patrick is associate professor and holder of the CN-Paul M. Tellier Chair on Business and Public Policy at the University of Ottawa's Graduate School of Public and International Affairs. Prior to his current professorship, Patrick was an assistant professor of international business at HEC Montréal and the director of the Réseau économie internationale at the Centre d'études et de recherches internationales de l'Université de Montréal. Patrick also holds the designation of chartered accountant and, before his career in academia, worked as a senior accountant and auditor at Ernst & Young in Montreal. He went on to work as a senior consultant, first in economic and financial consulting with Arthur Andersen & Co., and then later in business strategy consulting with SECOR Consulting.

Susan Ariel Aaronson is a CIGI senior fellow. She is an expert in international trade, digital trade, corruption, good governance and human rights. Susan writes on digital trade for CIGI.

In addition to her work at CIGI, Susan is research professor of international affairs and GWU Cross-Disciplinary Fellow at the George Washington University's Elliott School of International Affairs. At GWU, Susan recently completed a global project funded by the Hewlett Foundation that examined whether nations can find shared norms, definitions and strategies to reduce barriers to cross-border data flows. She was the former Minerva Chair at the National War College.

Susan is the author of six books and numerous articles. Her work has been funded by major international foundations including the MacArthur Foundation, the Ford Foundation and the Rockefeller Foundation; governments such as the Netherlands, United States and Canada; the United Nations, International Labour Organization and the World Bank; and US corporations including Google, Ford Motor Company and Levi Strauss & Co. Susan is also a frequent speaker on public understanding of globalization issues and international economic developments. She has often provided background and commentary on *Marketplace* radio and was a monthly commentator on *All Things Considered* and *Morning Edition*. Susan has appeared on CNN, CBC, the BBC and NPR to discuss trade and globalization issues. From 1995 to 1999, she was a guest scholar in economics at the Brookings Institution, and from 2008 to 2012, she was a research fellow at the World Trade Institute. In her spare time, Susan enjoys triathlons and ballet.

About Global Economy

Addressing the need for sustainable and balanced economic growth, the global economy is a central area of CIGI expertise. The Global Economy initiative examines macroeconomic regulation (such as fiscal, monetary, financial and exchange rate policies), trade policy and productivity and innovation policies, including governance around the digital economy (such as big data and artificial intelligence). We live in an increasingly interdependent world, where rapid change in one nation's economic system and governance policies may affect many nations. CIGI believes improved governance of the global economy can increase prosperity for all humankind.

Acronyms and Abbreviations

BCBS	Basel Committee on Banking Supervision
BRI	Belt and Road Initiative
CPTPP	Comprehensive and Progressive Agreement on Trans-Pacific Partnership
CUSMA	Canada-United States-Mexico Agreement
FSB	Financial Stability Board
FTA	free trade agreement
G20	Group of Twenty
GDPR	General Data Protection Regulation
IASB	International Accounting Standards Board
IMF	International Monetary Fund
OECD	Organisation for Economic Co-operation and Development
PIPEDA	Personal Information Protection and Electronic Documents Act
WTO	World Trade Organization

Executive Summary

With its relatively small population, Canada faces a challenge in terms of the amount of high-quality data that it can generate to support a successful data-driven economy. As a result, Canada needs to allow data to flow freely across its borders. However, it also has to provide a high-trust data environment if it wants individuals, firms and government to participate actively in such an economy. As such, Canada (and other countries) faces what can be called the data trilemma, whereby it is not possible to have simultaneously data that flows freely across borders, a high-trust data environment and a national data protection regime; one of these three objectives has to give so that only two are effectively possible at the same time.

To resolve the data trilemma, Canada should work with its key economic partners — namely the European Union, Japan and the United States — to develop a single data area that would be managed by an international data standards board. The envisioned single data area would allow for all types of personal and non-personal data to flow freely across borders while ensuring that individuals, consumers, workers, firms and governments are protected from potential harm arising from activities such as the collection, processing, use, storage or purchase/sale of data. If Canada and its economic partners share similar norms and standards for regulating data, then allowing data to flow freely across borders with these countries no longer risks undermining trust, which is crucial to a successful data-driven economy.

Introduction

Canada, like many other countries, wants to be a leader in the digital economy — an economy built on data-driven services and manufacturing. Such leadership is premised on two fundamental elements. First, firms, entrepreneurs and researchers need access to large pools of various types of (personal and non-personal) data (Aaronson 2018a, 2018b). Second, individuals, researchers and businesses need to trust that the data they use as well as generate is accurate, safe and secure (i.e., they will not be harmed by their use and generation of data).[1] Calls for Canada to develop a "national data strategy" or "strategic data policy" are based on these two elements (Aaronson 2018a; Balsillie 2018a; Breznitz 2018; CIGI 2018; Scassa 2019; Wolfe 2019).

Owing to the relatively small size of its population and markets, Canada is limited in terms of the amount of high-quality personal and public data that it can generate (Aaronson 2017): "scale in data is a huge problem for a small country like Canada" (Goldfarb and Trefler 2018, 20). Part of the solution to the issue of scale is to have easy access to data located outside of Canada's borders. However, obtaining access to such data also implies providing, in return, access to Canadian-based data to firms and researchers located outside Canada, since reciprocity is a fundamental principle underlying international cooperation in general and international economic agreements in particular (Keohane 1986).

The challenge for Canada, therefore, is to provide a high-trust data environment while ensuring that data can easily flow across borders. In a speech at the World Economic Forum's annual meeting in Davos in January 2019, Japanese Prime Minister Abe Shinzo called this goal (or challenge) "data free flow with trust" (Abe 2019). Adopting national policies to protect data generators and users can end up limiting the cross-border flow of data. For example, in the name of protecting personal data, the federal and some provincial governments require digital service providers to keep the data in Canada, which means that foreign service providers have to locate their servers in Canada. Furthermore, if companies based in Canada cannot guarantee that the personal data they export abroad will not be protected in accordance with Canadian laws and regulations, then they are expected under the current regime to keep the data in Canada. Conversely, if other countries adopt similar measures to protect the data located in their jurisdictions, then it becomes costlier, if not impossible, for Canadian

1 According to Venkatesh Shankar, Glen L. Urban and Fareena Sultan (2002, 327), trust is "the belief by one party about another party that the other party will behave in a predictable manner." For these authors, adopting a business perspective, online trust takes into account the viewpoints of firms' multiple stakeholders: customers, employees, suppliers, distributors, partners, stockholders and regulators. They define it as "a multidimensional construct whose underlying dimensions include reliability/credibility, emotional comfort, quality and benevolence" (ibid. 341).

businesses and researchers to access the data that they need to conduct their activities effectively.

As such, Canada (and other countries) faces what can be called the data trilemma, whereby it is not possible to have simultaneously data that flows freely across borders, a high-trust data environment and a national data protection regime; one of the these three objectives has to give so that only two are effectively possible at the same time.

Canada's current approach to cross-border data governance, which is based mainly on international trade agreements, cannot resolve the data trilemma. On the one hand, the commitments on data flows that Canada has undertaken in the Comprehensive and Progressive Agreement on Trans-Pacific Partnership (CPTPP) and the Canada-United States-Mexico Agreement (CUSMA),[2] should the latter ever come into force, are potential constraints on the federal and provincial governments' ability to develop new and improved data protection standards meant to ensure much-needed trust among individuals, firms and governments in the data-driven economy. On the other hand, given that such trade agreements allow for exceptions to the free flow of data across borders, then domestic data protection regulation adopted by Canadian governments could restrict such cross-border flows.[3]

If Canada's free-trade agreement (FTA) partners had data protection regimes in place that are equivalent to its own, then the Canadian government would not feel the need to restrict the flow of data to these countries and vice versa. In such a case, Canada and its partners would form what could be called a single data area. This is the best solution to the data trilemma.

An effective single data area allows for various forms of (personal and non-personal) data to flow freely across borders because the common (or equivalent) data protection regime(s) ensure that the area's individuals, consumers, workers, firms and governments do not suffer any harm from the collection, processing, use and sale of the data.[4] In such a high-trust single data area, people, firms and perhaps even governments would have few or no qualms with allowing various forms of data to move across the member states' borders, knowing that their data is well protected in a similar way everywhere within the area.

This type of single data area would welcome and support (financially and technically) any country willing to subscribe to and defend its shared norms and policies. It would be a plurilateral agreement focused on developing and enforcing high-quality regulatory standards for the collection, processing, use and sale of personal and non-personal data. In other words, the single data area — managed by an international data standards board — would provide what Sean McDonald (2019) calls "effective, ethical and international" data governance.[5] Any single data area member applying the standards in an effective manner would qualify to have data flow freely in and out with other member states.[6] As a result, it would provide a common regulatory environment for governing data that would allow various types of data to flow freely across member states' borders while providing a high degree of confidence among those who generate, process, use and buy/sell the data that the risk of harm associated with their participation in the data-driven economy is minimized (such risk can most probably never equal zero). As such, the envisaged single data area would go much further than digital/data rights-based conventions and declarations or trade agreements with digital or e-commerce chapters, which are all limited to general principles.[7] It would also go further than the proposal for a World Trade Organization (WTO) 2.0 or a digital stability board (Balsillie 2019; Ciuriak 2019; Fay 2019).

2 In the United States, the agreement is called the United States-Mexico-Canada Agreement (USMCA).

3 For a detailed discussion of this issue, see Leblond (forthcoming 2019).

4 Debates about data protection tend to focus mainly, if not solely, on personal data; however, the authors' view is that a single data area should not be limited to personal data if the common data protection regime is to provide a high degree of trust among individuals, firms and so on.

5 The content of such data governance in terms of standards and regulations is beyond this paper's scope.

6 Wealthier member states such as Canada, the European Union, Japan and the United States could provide financial and technical assistance to low- and middle-income countries to put in place the single data area's data governance regime with the goal of eventual membership in the single data area and its international data standards board. This would help address the fact that a large number of countries, including industrialized ones, "are struggling to govern the many different types and uses of data" (Aaronson 2019).

7 McDonald (2019) provides a list of such proposals.

To be clear, the single data area proposed in this paper should not be confused with a single digital market, like the one that the European Union is trying to develop.[8] Such a single data area would not be concerned with the rules that apply to the export and import (i.e., cross-border flows) of digital goods and services between the area's members, as these rules would be left to trade agreements, whether bilateral, plurilateral or multilateral. This means that standards and regulations governing data within the single data area would be separate from those governing international trade in goods and services.

Creating such a single data area would be no easy feat, as there are currently neither globally accepted standards for data protection nor comprehensive multilateral rules governing cross-border data flows (Aaronson and Leblond 2018; Ciuriak and Ptashkina 2018; Fefer 2019). Nevertheless, the timing appears to be right for such a project. First, a number of countries, including Canada, have aligned or are working to align their data protection regimes with the European Union's General Data Protection Regulation (GDPR) in order to continue doing business in Europe. As such, these countries are already forming a type of single data area, but one that is bilateral in nature and centred on EU rules and standards. Second, large digital firms such as Facebook and Google are now calling for international data protection rules that would make it easier for them to operate across borders (i.e., as a solution to the data trilemma). For this reason, they are putting pressure on the United States to adopt a national data protection regime that would align with that of the European Union; however, the United States is unlikely to be willing to depend on the European Union for setting its data protection rules. Third, China is offering countries that are part of its Belt and Road Initiative (BRI) the opportunity to also participate in what it calls the Digital Silk Road, which would involve bringing the countries under the umbrella of China's data realm. An effective single data area could therefore offer a viable alternative to the Digital Silk Road.

A plurilateral single data area with its own standard-setting and monitoring body (an international data standards board) represents the best approach to resolving the data trilemma for Canada and its key economic partners. If Canada wants to become a leader in the data-driven economy, then it should put the proposed single data area at the heart of its national data strategy and take the lead on its creation.

The Data Trilemma

Policy makers have lots of reasons to try to link the free flow of data and data protection. According to Dan Ciuriak (2018a, 6), "there is a need for free flow of data, including on a cross-border basis," because data is "intrinsic to commercial transactions." He sees data as the "fifth freedom" of commerce, with free movement of goods, services, capital and labour as the other four. For instance, Magnus Rentzhog (2015), in a study of Swedish companies from a wide range of sectors, found that moving data across borders easily was crucial for the well-functioning of these firms' global value chains. Thus, legal and regulatory limits on cross-border data flows can act as beyond-the-border obstacles to trade (Aaronson 2018c; Ciuriak and Ptashkina 2018; Cory 2017; Rentzhog and Jonströmer 2014). For example, Martina Francesca Ferracane and Erik van der Marel (2019) find that policies that restrict the cross-border flow of data have a negative impact on trade in digital services. Such restrictions can also hurt innovation and productivity. For instance, Avi Goldfarb and Daniel Trefler (2018, 23) indicate that there is some empirical evidence that suggests that data protection regulation can affect innovation negatively. For their part, Ferracane, Janez Kren and van der Marel (2019) find that limits on the cross-border movement and domestic use of data negatively impact the productivity of the firms that rely on such data, confirming the results obtained in an earlier study (Bauer, Ferracane and van der Marel 2016).

If the free flow of data provides economic benefits to the firms exploiting them, their unregulated use can have not only important economic but also personal and political costs. On a personal level, identity theft and fraud, for example, can be emotionally and financially very costly (Grant 2017). Politically, fake news and stolen data, for example, can affect election results and undermine democracy (Jardine 2019; Judge and Pal 2019). Economically, a lack of trust can lead consumers to avoid online activities. For instance, in a survey of 25,262 internet users in 25 countries, 50 percent

8 See https://ec.europa.eu/digital-single-market/en.

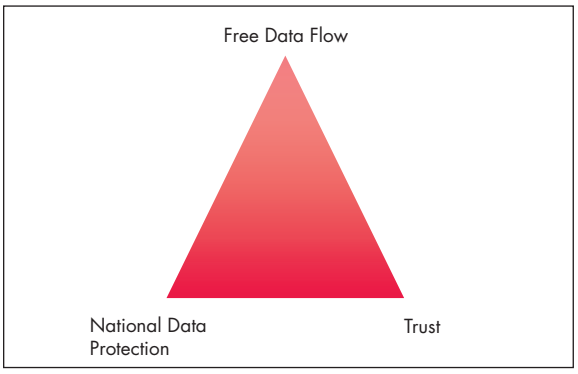
of respondents indicated that they never buy goods or services online because they do not trust shopping online (CIGI-Ipsos 2018). Reduced trust in the consumption of goods and services can also arise because of biased data for training artificial intelligence algorithms, which can lead firms and governments to discriminate against certain types of individuals, workers, consumers or businesses during the conduct of their activities (Munro 2019; Silberg and Manyika 2019).[9] Finally, if those who own data do not trust that they will be properly compensated for making their data available to others to pursue profit-generating activities, then they will refrain from making such data available to others. As Ciuriak (2018a, 6) argues, data as "an intangible capital asset" should be adequately compensated, which probably requires government intervention, in a way similar to intellectual property rights protection.

Therefore, to build trust, there is, in certain circumstances (for example, to protect privacy, security, competition, culture and so on), a need for the regulation of data collection, access, use and transfer. For example, the use of and access to people's data should be fair, transparent, accountable and subject to individuals' explicit consent. Moreover, the use of personal data should not lead to discrimination and bias when people seek to obtain a good or a service, whether it is from the private or the public sector. Another example is the protection of proprietary business data against uncompensated commercialization by others. On the other hand, access to data should not be controlled in such a way that it limits competition and innovation.

So the big question for policy makers is how to allow for data to flow freely across borders while maintaining a high degree of trust among individuals, firms and governments that they will not be harmed in terms of privacy, consumption (price, choice or access), competition, innovation, security and so on. Strong data protection laws and regulations are necessary to create such trust. The problem is that such laws and regulations, if developed independently from other countries, can limit the cross-border flow of data and have negative economic consequences, as mentioned above. For instance, 73 percent of respondents to the 2019 CIGI-Ipsos Global Survey on Internet Security and Trust indicated that they wanted their online data and personal information to be physically stored on a secure server in their own economy (CIGI-Ipsos 2019).

Policy makers, therefore, face a data trilemma whereby the following three elements are highly unlikely to hold simultaneously: data flows freely across borders; national data protection laws and regulations that are distinct from those of other countries are in place; and there is a high level of trust in the data environments among individuals, consumers, businesses and governments (see Figure 1).[10] Only two of the three elements are likely to be obtained at the same time. For instance, strong national data protection laws and regulations should lead to high trust levels but, to do so, they risk imposing restrictions on cross-border data flows. If policy makers want to ensure the free flow of data across borders while maintaining national data policies, then they may have to accept weaker data protection measures that could negatively affect trust. Finally, if policy makers want data to flow freely across borders while ensuring a high degree of trust surrounding the collection and use of data, then the only option is to cooperate with other countries to develop and enforce common, high-quality protection standards and regulations for personal as well as non-personal data (see also Meltzer 2019).

Figure 1: The Data Trilemma



Source: Authors.

9 According to the 2019 CIGI-Ipsos Global Survey on Internet Security and Trust, "less than half of global citizens express at least some degree of confidence that any of the algorithms they use are unbiased, in any context" (CIGI-Ipsos 2019).

10 In his presentation at the International Monetary Fund (IMF) Statistical Forum in November 2018, Jim Balsillie indicated that capturing economic value, ensuring cyber security and protecting sovereignty (in terms of democracy and privacy) in the data-driven economy poses a challenge to countries' compliance with the commitments they have undertaken in international trade agreements (Balsillie 2018b).

A Single Data Area as the Solution to the Data Trilemma

As discussed in the previous section, the solution to the data trilemma is an international data-protection umbrella whereby member states agree on common standards and rules for protecting privacy, consumption, competition and cyber security as well as fostering innovation. With such high-quality common data-protection standards, there is no need for a government to restrict cross-border data flows. It is then left to firms, and possibly even individuals, to decide where they want their data to be stored and accessed since they all face the same rules and regulations that provide a high degree of trust to go about their business as they see fit.

Canadian policy makers must, therefore, work with their key economic partners such as Japan, the European Union and the United States to develop a single data area *for all types of data.* The European Union's approach to protecting personal data and its cross-border transfers provides a basis for building such a single data area. Moreover, pressures for putting in place comprehensive data protection rules at the national level in the United States provide an opportunity for Canada to push for the creation of a plurilateral single data area.

The European Union's Bilateral Approach for Personal Data

The European Union has been pursuing a form of bilateral single data area for personal data since the mid-1990s, by unilaterally imposing its regulations on partner countries that want to transfer personal information from the European Union. The European Union's commitment to online data protection began with the 1995 Directive on Data Protection, which prohibited the transfer of personal data to non-EU countries that do not meet the "adequacy" standard for privacy protection. As new technologies emerged, policy makers and the public realized the European Union's data protection framework needed updating. In 2016, the European Union adopted the GDPR, which took effect on May 25, 2018, and provides stricter rules on the use of data that can be attributed to a person or persons.[11] The GDPR is built on individuals' explicit consent for their personal data to be collected and processed, including when doing so takes place outside the European Union's borders. Where earlier data protection regulations allowed data controllers to rely on implicit consent, the GDPR requires individuals to signal agreement by "a statement or a clear affirmative action" (Maldoff 2016).[12]

By allowing personal data to flow outside its borders only when other countries' data protection regimes are deemed "adequate," the European Union is prodding those countries that want their firms to have access to EU data without having to set up their operations in the European Union (for example, to sell goods or services online) to adopt data protection laws and regulations that are similar to the European Union's. As a result, it creates a de facto bilateral single data area between the European Union and the countries deemed adequate where personal data can flow freely across borders. As of September 2019, the European Union had recognized Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, the United States and Uruguay as providing adequate protection for personal data. It was also in discussion with South Korea.[13]

States that want to become adequate 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. Since adequacy is a time-consuming and costly process, the GDPR also offers alternative options to transfer personal data from the European Union to countries that the

11 EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, [2016] OJ, L 119, online: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN>.

12 For a discussion of the GDPR's performance after one year of being into effect, see Jeanette Herrle and Jesse Hirsh (2019). For a more critical perspective, see Eline Chivot and Daniel Castro (2019).

13 See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

European Union does not view as "adequate."[14] For instance, an organization may use specific binding corporate rules or model contracts approved by the European Union in order to be allowed to move personal data outside the European Union. In other words, specific organizations can receive authorization from the European Commission to access EU personal data from abroad if they meet the GDPR's requirements.

As a complement to the GDPR, the European Union has also recently adopted a regulation to support the free flow of non-personal data across the union.[15] The regulation's main objective is to prohibit any data localization requirement or other administrative restriction on the flow of non-personal data within the European Union, except when such a requirement is for "public security" purposes. The regulation does not apply to data-processing services taking place outside the European Union, which means that member states remain free to impose data localization requirements on foreign service providers; however, such requirements cannot be specific to a particular member state, as the regulation applies to "those who provide processing services in the Union without an establishment in the Union."[16] So, unlike the GDPR, there is no adequacy mechanism available for non-EU countries in the case of non-personal data, which potentially reduces trade opportunities and competition. A plurilateral single data area with common standards and regulations governing data creates an opportunity for other countries, such as Canada, to convince the European Union to accept that non-personal data could also flow without restrictions with single data area partner countries.

An Opportunity for Canada to Push for a Plurilateral Single Data Area

Canada's current personal data protection regime, the Personal Information Protection and Electronic Documents Act (PIPEDA), was originally passed in 2000 in order to meet the requirements of the European Union's Data Protection Directive of 1995.[17] A year later, the European Union deemed PIPEDA "adequate" for the directive's purposes, thereby allowing personal data to be transferred from the European Union to Canada without additional safeguards. The European Union's adequacy decision prevented Canadian firms from having to demonstrate that they individually complied with the provisions contained in the EU directive in order to collect or receive personal data from the European Union.

According to Teresa Scassa (2018), PIPEDA does not meet the new standards set by the European Union's GDPR, since it barely met those of the Data Protection Directive. For example, the GDPR requires explicit consent from individuals for personal data to be transferred outside the European Union whereas PIPEDA does not.[18] This means that Canada could soon lose its adequacy with EU data protection rules and, as a result, data flows between Canada and the European Union could be impeded, which would negatively affect trade and business activities between the two jurisdictions. Maintaining digital access to the European Union is very important for Canadian business, since it is Canada's second-largest economic partner.

The GDPR's introduction combined with well-publicized privacy breaches in Canada and abroad (for example, Equifax, Cambridge Analytica) and Canadians' concerns about the privacy and security

14 See https://edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en.

15 EC, *Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union,* [2018] OJ, L 303/59, online: <https://eur-lex.europa.eu/eli/reg/2018/1807/oj>.

16 *Ibid*, Preamble, art 15.

17 There are two federal laws that govern personal data and information in Canada. The Privacy Act sets the rules for how the federal public sector collects, uses and discloses personal information. PIPEDA does the same for the private sector (see www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15). PIPEDA only applies to commercial, for-profit activities. As such, it does not apply to non-profit and charity organizations, unless they conduct commercial activities that involve personal information. The Office of the Privacy Commissioner of Canada, which is responsible for implementing both acts, defines personal information as "data about an 'identifiable individual'...that on its own or combined with other pieces of data, can identify you as an individual" (see www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_63_s4). As such, it indicates that the following types of information are not (generally) considered personal: information about a business or an organization; information that is not possible to link back to an identifiable person (i.e., it has been anonimized); and information that is not about an individual and whose connection with a person is too weak or far-removed.

18 PIPEDA relies on the accountability principle whereby an organization transferring the data abroad is accountable for how the data is used and disclosed outside Canada's borders. As such, it has to make sure that such use and disclosure are in accordance with Canadian privacy regulations. However, once the organization has received consent to collect and process the personal information, it does not need additional explicit consent in order to be able to transfer it abroad.

of their personal information[19] explain why the Office of the Privacy Commissioner of Canada is now considering requiring organizations based in Canada to get explicit consent from individuals before they can transfer personal data abroad. It is also putting forward the idea that it should have the authority, like in the European Union, to undertake proactive inspections of organizations' practices to enhance accountability, as opposed to waiting until a complaint has been filed.[20] The above-mentioned circumstances also explain why the Government of Canada, in May 2019, introduced a Digital Charter[21] and a white paper about PIPEDA's modernization with the objective to enhance trust in the digital economy.[22]

A key issue for Canada, however, is whether modernizing PIPEDA and maintaining GDPR adequacy would affect Canadian firms' access to the US market, given how Canada's economy depends on trade and investment with its southern neighbour. Currently, respecting the GDPR does not contravene US law and, therefore, does not prevent a Canadian firm from operating in the United States where it uses personal data on US individuals.[23] This is because the United States does not yet have comprehensive data protection legislation in place at the national level (Fefer 2019; O'Connor 2018), although there are a number of proposals in the works (Fefer 2019; Kerry 2019). Such proposals could very well lead the United States to adopt national data protection legislation that follows in the GDPR's footsteps. There are three reasons for this. First, the EU-US Privacy Shield is at risk of falling apart because the European Union thinks that the US side is not managing the process effectively (Evans and Togawa Mercer 2018). Second, US digital technology companies operating internationally already have to comply with the GDPR. Finally, in the absence of US federal laws that require companies to get informed consent to use personal data or establish a baseline commercial data privacy framework, state-level legislation has begun to emerge to fill the void left by the federal government.[24] As a result, there are now strong pressures by technology firms such as Apple, Facebook, Google and Microsoft for the United States to come up with a national personal data protection regime that is aligned with the GDPR so that it is ultimately considered "adequate" by the European Commission, which would allow firms on both sides of the Atlantic to move personal data freely (Abril 2019; Pfeifle 2018; Pichai 2019; Scott 2019). As Henry Farrell (2019) points out: "Businesses hate restrictive rules, but they hate them much less than they hate uncertainty."

Developing data protection rules aligned with the European Union's GDPR is, however, an inadequate solution to the data trilemma for Canada, the United States and other countries. First, it remains bilateral in nature. Even if the European Union considers partner countries to have adequate personal data protection regimes in place, it does not mean that such data can flow freely between the non-EU partner countries. This is why European Commissioner Věra Jourová (2019) talked of creating "a network of adequacy findings where data can flow freely" around a "common approach" based on the GDPR. Second, it is only concerned with personal data, focused mainly on privacy issues, which means that issues associated with other types of data and their processing are left unaddressed, possibly undermining trust as a result. Finally, this solution makes the European Union the sole rule maker for deciding data protection standards; it also means that only the European Union gets to decide which countries can participate in this GDPR network.

It would, therefore, be best for Canada, the United States and other countries with adequate data protection regimes to build on the European Union's GDPR approach and work toward the

19 According to Ipsos (2018), 85 percent of surveyed Canadians indicated that they are concerned about the privacy and security of their personal information while 67 percent of respondents agreed that internet advertising is an invasion of privacy. A more recent survey, conducted by the Office of the Privacy Commissioner of Canada (2019), found that close to 90 percent of Canadians were concerned about their online information: "The vast majority are at least somewhat concerned about people using their online information to attempt to steal their identity (90%), about companies or organizations using this information to make decisions about them (88%), and about social media platforms gathering their personal information to create detailed profiles about them (87%)."

20 See www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transfers-for-processing/.

21 See https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html.

22 See https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html.

23 Non-personal data is, for the most part, not regulated on both sides of the Canada-US border. An interesting and potentially important question, which is beyond this paper's scope, is whether meeting GDPR standards would contravene Canada's commitments on data flows under CUSMA. For a detailed analysis of CUSMA's data flow provisions, see Leblond (forthcoming 2019).

24 For example, inspired by the GDPR, the State of California adopted the California Consumer Privacy Act in May 2018, which is set to come into force at the beginning of 2020 (for details, see Ghosh 2018). For a list of what other US states have done in terms of data protection legislation, see Serrato et al. (2018).

creation of a true plurilateral single data area by adopting common regulatory and enforcement standards for both personal and non-personal data. Mark Zuckerberg, CEO of Facebook, has recently shifted his position on data protection and now calls for "a globally harmonized framework" for privacy and data protection that would build on the GDPR (Zuckerberg 2019). The *Financial Times*' editorial board quickly came out in support of Zuckerberg's idea of global standards based on the GDPR (The Editorial Board 2019).

As part of the national data strategy that it has been called upon to develop, Canada should take the leadership role in creating a single data area with commonly agreed rules on, for example, free flow of data, clarification of exceptions, clarification of practices that can distort market access for data and rules to guide countries in responding to such practices. In collaboration with the European Union and Japan, which is now GDPR-adequate, Canada could use the increasing pressures on the US Congress to develop federal-level data protection laws and regulations as an opportunity to help convince the United States to participate in the creation of a single data area based on shared norms and standards. In such a single data area, all forms of data would then be free to flow across the borders of the states that are members of the area while ensuring a high degree of trust as a result of strong data protection standards in terms of both regulation and enforcement. Such an approach represents the best solution to Canada's data trilemma.

A Single Data Area Should Be Developed Outside the WTO

Although the authors have argued elsewhere that developing common rules to govern data and trade internationally should take place at the WTO (Aaronson 2018a; Aaronson and Leblond 2017; Aaronson and Leblond 2018), they now think that such a plurilateral agreement on common data protection standards should be pursued separately from the broader WTO "trade-related aspects of electronic commerce" process that Canada is already engaged in.[25] Joshua P. Meltzer (2019, 26) comes to a similar conclusion when he writes: "What is lacking is a parallel agenda [to trade agreements] aimed at giving domestic regulators confidence that achieving domestic regulatory goals will not be undermined by allowing data to leave their jurisdiction."

There are three main reasons for a single data area to be developed outside the WTO's framework. First, the WTO does not have the expertise to develop data protection standards; it can only call on member states to have such a regime in place based on standards developed by other organizations, in a way similar to what the e-commerce/digital trade chapters do in the CPTPP and CUSMA.[26] Governing data through trade agreements, which rely on uncertain general exceptions, can potentially undermine national data protection regimes (Leblond, forthcoming 2019). The WTO's focus, therefore, should be limited to the particularities of trade in digital goods and services.

Second, being more limited in scope, a separate international agreement on data protection standards could be easier to adapt to evolving technological changes than a more comprehensive agreement on "trade-related aspects of electronic commerce" that deals with both data and trade in digital goods and services. Such an

25 At the WTO's eleventh ministerial conference in Buenos Aires in December 2017, some 75 members, including Canada, issued a joint statement whereby they recognized the important role of the WTO in promoting open, transparent, non-discriminatory and predictable regulatory environments in facilitating electronic commerce" (WTO 2017). They also indicated that they would begin exploratory work toward "future WTO negotiations on trade-related aspects of electronic commerce." As a result, a number of discussion rounds took place in 2018 in Geneva in order to delimit the scope of potential plurilateral negotiations; however, differences between the European Union and the United States, which had emerged during the Trade in Services Agreement negotiations, quickly (re)surfaced (Fortnam 2018): the European Union wanted to limit the negotiations' scope to electronic signatures, encryption and transparency (as in the Comprehensive Economic and Trade Agreement) while the United States wanted an agreement that would ultimately contain much broader provisions on cross-border data flows and data localization, similar to what is found in the Trans-Pacific Partnership and CUSMA. On January 25, 2019, during the World Economic Forum's annual meeting in Davos, more or less the same group of WTO members issued a new joint statement on electronic commerce to "confirm [their] intention to commence WTO negotiations on trade-related aspects of electronic commerce" (WTO 2019). As of May 2019, little progress had been made as "the submissions so far do not show much progress in narrowing the gulf between the major trading powers" (Beattie 2019).

26 On April 26, 2019, the United States communicated its proposal for a multilateral digital trade agreement at the WTO. According to Bryce Baschuk (2019), this proposal follows closely the digital trade chapter found in CUSMA. It also calls for members to bridge the differences in their data protection regimes.

approach based on standard setting for data-protection regulation and enforcement would help address Ciuriak's (2018b) concern that, given the rapidly evolving nature of the data-driven economy, data is not "treaty ready."

Third, and finally, the current WTO "trade-related aspects of electronic commerce" process (now called the "Osaka Track," see below) includes China and Russia, two countries that have, to a large extent, walled off their digital realm with very different standards of data protection than Canada or other Western countries.[27] As a result, it is highly unlikely that the WTO process will produce anything (if it does at all) close to what is found in the CPTPP and the CUSMA. It is indicative that in its trade negotiation with the United States, China refused to ease its restrictions on data and digital trade (Politi and Mitchell 2019). As such, should there ever be a WTO agreement on trade-related aspects of e-commerce, it would likely be a superficial accord based on general principles with emphasis on the "legitimate public policy objective" general exception. Such an agreement would not be very useful since it would not resolve the data trilemma in terms of free cross-border data flows and high levels of trust in the data-driven economy.

If not the WTO, then where should the standards for a single data area be developed and governed? One option is the Organisation for Economic Co-operation and Development (OECD), which has already developed privacy guidelines for personal data.[28] One potential problem with this option is that the European Union is not an OECD member, although it is represented by its member states; however, the latter often pursue national rather than European interests in international forums where the European Union is not present. Furthermore, given that the OECD is a club of wealthier countries, it would be impossible for non-member countries to join the single data area as full-fledged members; they could only join by adopting the standards and being deemed adequate like in the current EU GDPR framework. This means that developing countries that might want to join the single data area and have a say on its future would not be able to do so. As a result, it could unnecessarily limit the single data area's international scope and the associated economic benefits that result from a larger network of countries with the same regulatory and enforcement standards when it comes to data governance.

Another possible venue for governing data could be the IMF, as suggested by Jim Balsillie (Orol 2018). Balsillie has called on the IMF to "catalyze a new Bretton Woods moment" for the digital economy. He argues that the IMF and its members need to work together to come up with common rules for the digital age. Although the IMF, with its 189 member states, would resolve the OECD's limited membership problem, it is hard to see how it can credibly address global data governance since it does not have proven technical expertise on data protection and digital economy policy issues. The IMF's expertise rests, for the most part, on macroeconomic policy and international finance. Furthermore, the IMF has limited regulatory and standard-setting experience, since other international bodies or forums are responsible for these things in the banking and finance world.

A more suitable option would be to set up a new international standard-setting body for data regulation. Such a new body could, for example, be modelled on the Basel Committee on Banking Supervision (BCBS),[29] which sets standards for banking regulation, or the International Accounting Standards Board (IASB), which sets international standards for financial reporting.[30] This international data standards board would be responsible for devising common standards to ensure a high degree of trust in the data-driven economy among the single data area's individuals,

27 For details on the Chinese data realm, see Aaronson and Leblond (2018). Nigel Cory (2019) goes so far as to argue that China should be disqualified from participating in the WTO negotiations on trade-related aspects of electronic commerce, because of the country's strong restrictions on cross-border data flows and weak protection of individuals' online privacy. For an analysis of Russia's digital regime, see Seddon and Foy (2019).

28 See www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

29 Robert Fay (2019) argues that the Financial Stability Board (FSB) offers a useful model for creating what he calls a "digital stability board" that would "take its mandate from global leaders and coordinate work on global principles and standards for the big data and AI realm, while working with domestic agencies responsible for data and AI policy to best reflect national values and customs" (see also Balsillie 2019). The FSB's key role is to coordinate a number of international financial standard-setting bodies such as the BCBS and the IASB; its actual standard-setting capacity is limited. This is why the authors think that the BCBS or the IASB might be a better model for an international data standards board, although the latter's monitoring and assessment capacity would likely be superior to that of the BCBS and IASB.

30 Hirsh (2019) suggests that financial regulation could be a good model for regulating social media platforms. Vallée (2019), for his part, compares data to capital.

consumers, workers, businesses and governments so that all forms of data could flow freely across borders. Michel Girard (2019, 1) argues that there is an urgent need for international standards for big data analytics: "issues such as consent and scrubbing requirements, anonymization, data quality and consistency will need to be standardized in addition to data consent, ownership, collection, processing, aggregation, transmission, storage, analysis, certification and disposal." Paul Vallée (2019) proposes the development of standards and certification processes so that organizations would be "verified" as trustworthy to carry on data-related activities as well as share data with each other, thereby allowing data governance authorities with proactive rather than retroactive accountability enforcement powers.[31] An international data standards board would also be responsible to monitor that single data area member states apply and enforce the common standards adequately; its frequent assessments would determine if a member state is able to continue taking full part in the single data area or not (for example, restrictions on cross-border data flows could be limited to the type of data where standards are not being applied or enforced properly).

A Single Data Area as an Alternative to China's Digital Silk Road

A single data area between Canada, the European Union, Japan, the United States and other "like-minded" countries would have the added benefit of offering a strong alternative to China's Digital Silk Road. China is using the BRI to bring countries inside its Great Firewall, by offering to help them build an internet infrastructure modelled on its own (Hornby 2018). According to Chen Zhaoxiong, vice minister of China's Ministry of Industry and Information Technology, the aim is to "promote the 'digital silk road' to construct a community of common destiny in cyberspace" (Moody and Yu 2017). As such, firms in BRI countries that have opted to adopt the Great Firewall architecture are able to access China's large consumer population and benefit from relatively low data protection standards; however, in return, China's large data-driven firms such as Alibaba and Tencent obtain privileged access to these markets in Asia and Africa, whereby being under the Great Firewall's umbrella curtails competition from Western firms such as Google and Facebook. In other words, China's Digital Silk Road initiative aims to create a single data area but with very different standards for governing data than what individuals and businesses can expect in liberal democracies. Thus, it seems important for Canada and its potential single data area partners to offer an alternative single data area of a similar scale to China's Great Firewall.

Developing a single data area that would act as an alternative to the Digital Silk Road does not mean that Canada and its partners should not engage with China and the other countries that prefer the Chinese data umbrella. Such engagement could take place under the Group of Twenty's (G20's) aegis in order to provide a minimum of interoperability between the two data areas, if possible. If a majority of countries in the G20 shared the same data governance standards, it would probably make it easier to exert pressure on China to open up its own data area and allow more data flows and digital trade to take place and, thus, prevent a clear digital divide between the international data standards board-led single data area and the China-led Digital Silk Road.[32] For this reason, the Osaka Declaration on the Digital Economy that was issued during the G20 leaders' meeting held in Osaka, Japan, on June 28-29, 2019, is a welcome step in the right direction;[33] however, the fact that the so-called Osaka Track appears to be limited to renewing the signatories' "commitment to work together building on the Joint Statement in Davos [see footnote 25 above] and confirm our commitment to seek to achieve a high standard agreement with the participation of as many WTO Members as possible" is problematic, since, as

31 This would satisfy the first basic principle advocated by Nigel Cory, Robert D. Atkinson and Daniel Castro (2019, 7) for a global framework to provide "data free flow with trust": "firms should be held accountable for managing the data they collect, regardless of where they store, process, or transfer the data."

32 For a discussion of the policies that G20 countries could pursue in order to support the digital economy and the free flow of data, see Chen et al. (2019).

33 See www.international.gc.ca/world-monde/international_relations-relations_internationales/g20/2019-06-29-g20_declaration-declaration_g20.aspx?lang=eng.

argued above, the WTO is not the right venue for effectively achieving "data free flow with trust."

Conclusion

With its relatively small population, Canada faces a challenge in terms of the amount of high-quality data that it can generate for supporting a successful data-driven economy. As a result, Canada needs to allow data to flow freely in and out of its borders. Canada should therefore work with its key economic partners, namely the European Union, Japan and the United States, to develop a single data area that would allow for all types of data to flow freely across borders while ensuring that individuals, consumers, workers, firms and governments are protected from potential harm arising from activities such as the collection, processing, use, storage or sale of data. If Canada and its economic partners share similar norms and standards for regulating data, then allowing data to flow freely across borders with these countries no longer risks undermining trust, which is crucial to a successful data-driven economy. As such, a single data area with common standards is the best way for Canada and its partners to resolve the data trilemma in an effective manner.

This means that Canada's current approach to cross-border data flow governance, which relies on international trade agreements, is inadequate. Trade agreements that include e-commerce or digital trade chapters are essentially negotiated exceptions to the free flow of data across borders in order to reflect existing data protection policies that might conflict with the free flow of data. But as Canada develops new laws and regulations to better govern data, its trade commitments in FTAs such as the CPTPP and CUSMA could ultimately negate the effectiveness of such future data protection policies (Leblond, forthcoming 2019). The same logic applies to a specific agreement on trade-related aspects of electronic commerce that would be negotiated under the WTO's aegis. This is why the WTO is not the right venue for developing common standards to govern data for the proposed single data area. It would be best to create a dedicated body for such a role: an international data standards board. As a result, the WTO could focus its attention on issues specific to trade in digital goods and services. Countries that espouse the same standards of data protection as Canada and its partners would be warmly welcomed and firmly supported (financially and technically) to join the proposed single data area through membership in the international data standards board.

In spite of the challenges that creating a new international regime for data governance presents, it appears to be the right moment for Canada to take the lead in rallying its key economic partners to create a single data area. An increasing number of countries are adopting (personal) data protection regimes modelled on the European Union's GDPR in order for their firms to be able to do digital business with the European Union. There are mounting pressures and proposals in the United States for comprehensive data protection legislation to be adopted at the national level. Given that US multinational digital firms already have to comply with the GDPR's rules, they are pushing for such legislation to be in line with the GDPR. In fact, for firms operating multinationally, the best outcome would be harmonized standards for governing personal and non-personal data under a single data area; however, these standards have to be of the highest quality to ensure that all stakeholders trust they will not be harmed from the collection, processing, sharing and sale of all types of data. This is the best way to resolve the data trilemma.

Works Cited

Aaronson, Susan Ariel. 2017. *Information Please: A Comprehensive Approach to Digital Trade Provisions in NAFTA 2.0.* CIGI Paper No. 154. Waterloo, ON: CIGI. www.cigionline.org/publications/information-please-comprehensive-approach-digital-trade-provisions-nafta-20.

———. 2018a. *Data Is Different: Why the World Needs a New Approach to Governing Cross-border Data Flows.* CIGI Paper No. 197. Waterloo, ON: CIGI. www.cigionline.org/publications/data-different-why-world-needs-new-approach-governing-cross-border-data-flows.

———. 2018b. "Data Minefield? How AI Is Prodding Governments to Rethink Trade in Data." In *Data Governance in the Digital Age.* Waterloo, ON: CIGI. www.cigionline.org/sites/default/files/documents/Data%20Series%20Special%20Reportweb.pdf.

———. 2018c. "What Are We Talking about When We Talk about Digital Protectionism?" *World Trade Review* First View, August 6. www.cambridge.org/core/journals/world-trade-review/article/what-are-we-talking-about-when-we-talk-about-digital-protectionism/F0C763191DE948D484C489798863E77B.

———. 2019. *Data Is a Development Issue.* CIGI Papers No. 223. Waterloo, ON: CIGI. www.cigionline.org/sites/default/files/documents/paper%20no.223.pdf.

Aaronson, Susan Ariel and Patrick Leblond. 2017. "NAFTA is the wrong venue to govern digital trade." *The Globe and Mail*, September 13. www.theglobeandmail.com/report-on-business/rob-commentary/nafta-is-the-wrong-venue-to-govern-digital-trade/article36249592/.

———. 2018. "Another Digital Divide: The Rise of Data Realms and its Implications for the WTO." *Journal of International Economic Law* 21 (2): 245–72.

Abe, Shinzo. 2019. "'Defeatism about Japan is now defeated': Read Abe's Davos speech in full." Speech at World Economic Forum, Davos, Switzerland, January 23. www.weforum.org/agenda/2019/01/abe-speech-transcript/.

Abril, Danielle. 2019. "This Is What Tech Companies Want in Any Federal Data Privacy Legislation." *Fortune*, February 21. fortune.com/2019/02/21/technology-companies-federal-data-privacy-law/.

Balsillie, Jim. 2018a. "Jim Balsillie: Canada needs a national data strategy." *The Toronto Star*, January 30. www.thestar.com/opinion/contributors/2018/01/30/jim-balsillie-canada-needs-a-national-data-strategy.html.

———. 2018b. "Measuring Intangible Assets (IP & Data) for the Knowledge-based and Data-driven Economy." Presentation at the IMF Statistical Forum, November 20. www.ineteconomics.org/uploads/papers/Balsillie-IMF-Presentation.pdf.

———. 2019. "Jim Balsillie: 'Data is not the new oil — it's the new plutonium.'" *The Financial Post,* May 28. https://business.financialpost.com/technology/jim-balsillie-data-is-not-the-new-oil-its-the-new-plutonium.

Baschuk, Bryce. 2019. "U.S. WTO E-Commerce Offer Reflects USMCA Digital Trade Chapter." Bloomberg Law, May 6. https://news.bloomberglaw.com/international-trade/u-s-wto-e-commerce-offer-reflects-usmca-digital-trade-chapter.

Bauer, Matthias, Martina F. Ferracane and Erik van der Marel. 2016. *Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization.* Global Commission on Internet Governance Paper No. 30, May. Waterloo, ON and London, UK: CIGI and Chatham House (Royal Institute of International Affairs). www.cigionline.org/publications/tracing-economic-impact-regulations-free-flow-data-and-data-localization.

Beattie, Alan. 2019. "WTO in for the long haul on ecommerce talks." *The Financial Times,* May 9. www.ft.com/content/946fd256-722f-11e9-bf5c-6eeb837566c5.

Breznitz, Dan. 2018. "Data and the Future of Growth: The Need for Strategic Data Policy." In *Data Governance in the Digital Age*. Waterloo, ON: CIGI. www.cigionline.org/sites/default/files/documents/Data%20Series%20Special%20Reportweb.pdf.

Chen, Lurong, Wallace Cheng, Dan Ciuriak, Fukunari Kimura, Junji Nakagawa, Richard Pomfret, Gabriela Rigoni and Johannes Schwarzer. 2019. "The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies." Trade, Investment and Globalization Think-20 Japan 2019. t20japan.org/wp-content/uploads/2019/03/t20-japan-tf8-4-digital-economy-economic-development.pdf.

Chivot, Eline and Daniel Castro. 2019. "What the Evidence Shows About the Impact of the GDPR After One Year." June 17. Washington, DC and Brussels, Belgium: Center for Data Innovation. www2.datainnovation.org/2019-gdpr-one-year.pdf.

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

CIGI-Ipsos. 2018. "2018 CIGI-Ipsos Global Survey on Internet Security and Trust." www.cigionline.org/internet-survey-2018.

———. 2019. "2019 CIGI-Ipsos Global Survey on Internet Security and Trust." www.cigionline.org/internet-survey-2019.

Ciuriak, Dan. 2018a. *Rethinking Industrial Policy for the Data-driven Economy.* CIGI Paper No. 192. Waterloo, ON: CIGI. www.cigionline.org/publications/rethinking-industrial-policy-data-driven-economy.

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

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

Ciuriak, Dan and Maria Ptashkina. 2018. "The Digital Transformation and the Transformation of International Trade." RTA Exchange, Issue Paper, January. New York and Geneva: Inter-American Development Bank and International Centre for Trade and Sustainable Development. e15initiative.org/wp-content/uploads/2015/09/RTA-Exchange-Digital-Trade-Ciuriak-and-Ptashkina-Final.pdf.

Cory, Nigel. 2017. "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" May 1. Washington, DC: Information Technology & Innovation Foundation. https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

———. 2019. "Why China Should Be Disqualified From Participating in WTO Negotiations on Digital Trade Rules." ITIF Policy Brief, May. Washington, DC: Information Technology & Innovation Foundation. https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital.

Cory, Nigel, Robert D. Atkinson and Daniel Castro. 2019. "Principles and Policies for 'Data Free Flow With Trust.'" May. Washington, DC: Information Technology & Innovation Foundation. https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust.

Evans, Hayley and Shannon Togawa Mercer. 2018. "Privacy Shield on Shaky Ground: What's Up With EU-U.S. Data Privacy Regulations Lawfare." *Lawfare* (blog), September 2. www.lawfareblog.com/privacy-shield-shaky-ground-whats-eu-us-data-privacy-regulations.

Farrell, Henry (with Abraham Newman). 2019. "Facebook finally learns to love privacy rules." *Financial Times* (US edition), April 5, 9.

Fay, Robert. 2019. "The world faces a turning point on data and AI. Will we learn from the financial crisis?" *The Globe and Mail*, May 28. www.theglobeandmail.com/opinion/article-the-world-faces-a-turning-point-on-data-and-ai-will-we-learn-from-the/.

Fefer, Rachel F. 2019. "Data Flows, Online Privacy, and Trade Policy." CRS Report R45584, March 11. Washington, DC: Congressional Research Service. crsreports.congress.gov/product/pdf/R/R45584.

Ferracane, Martina Francesca, Janez Kren and Erik van der Marel. 2019. "Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?" EUI Working Paper RSCAS 2019/28, Global Governance Programme-341. Florence: European University Institute, Robert Schuman Centre for Advanced Studies. https://cadmus.eui.eu/handle/1814/62324.

Ferracane, Martina Francesca and Erik van der Marel. 2019. "Do Data Policy Restrictions Inhibit Trade in Services?" EUI Working Paper RSCAS 2019/29, Global Governance Programme-342. Florence: European University Institute, Robert Schuman Centre for Advanced Studies. https://cadmus.eui.eu/handle/1814/62325.

Fortnam, Brett. 2018. "Divisions emerge as some WTO members push for e-commerce plurilateral." Inside U.S. Trade's *World Trade Online*, July 20. https://insidetrade.com/daily-news/divisions-emerge-some-wto-members-push-e-commerce-plurilateral.

Ghosh, Dipayan. 2018. "What You Need to Know About California's New Data Privacy Law." *Harvard Business Review*, July 11. https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law.

Girard, Michel. 2019. *Big Data Analytics Need Standards to Thrive: What Standards Are and Why They Matter.* CIGI Papers No. 209. Waterloo, ON: CIGI. www.cigionline.org/publications/big-data-analytics-need-standards-thrive-what-standards-are-and-why-they-matter.

Goldfarb, Avi and Daniel Trefler. 2018. "AI and International Trade." NBER Working Paper 24254, January. Cambridge, MA: National Bureau of Economic Research. www.nber.org/papers/w24254.

Grant, Kelli B. 2017. "Identity theft, fraud cost consumers more than $16 billion." *CNBC*, February 1. www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html.

Herrle, Jeanette and Jesse Hirsh. 2019. "The Peril and Potential of the GDPR." Opinion, July 9. Waterloo, ON: CIGI. www.cigionline.org/articles/peril-and-potential-gdpr.

Hirsh, Jesse. 2019. "Could Banking Regulation Rein in Social Media Giants?" Opinion, February 22. Waterloo, ON: CIGI. www.cigionline.org/articles/could-banking-regulation-rein-social-media-giants.

Hornby, Lucy. 2018. "Cash colours Chinese curbs on corporate internet access." *Financial Times* (US edition), January 23, 4.

Ipsos. 2018. "Four in Ten (39%) Canadians Changed Their Social Media Behaviour (28%) or Stopped Using some Platforms (11%) Over Data Privacy Concerns." Press release, April 10. www.ipsos.com/en-ca/news-polls/Global-News-Data-Privacy-and-Social-Media-Poll-April-2018.

Jardine, Eric. 2019. "Beware Fake News: How Influence Operations Challenge Liberal Democratic Governments." In *Governing Cyberspace during a Crisis in Trust.* Waterloo, ON: CIGI. www.cigionline.org/publications/governing-cyberspace-during-crisis-trust.

Jourová, Věra. 2019. "What next for European and global data privacy?" Speech at the 9th Annual European Data Protection and Privacy Conference. Brussels, Belgium, March 20. https://europa.eu/rapid/press-release_SPEECH-19-1776_en.htm.

Judge, Elizabeth F. and Michael Pal. 2019. "Election Cyber Security Challenges for Canada." In *Governing Cyberspace during a Crisis in Trust.* Waterloo, ON: CIGI. www.cigionline.org/publications/governing-cyberspace-during-crisis-trust.

Keohane, Robert O. 1986. "Reciprocity in international relations." *International Organization* 40 (1): 1–27.

Kerry, Cameron F. 2019. "Will this new Congress be the one to pass data privacy legislation?" January 7. Washington, DC: Brookings Institution. www.brookings.edu/blog/techtank/2019/01/07/will-this-new-congress-be-the-one-to-pass-data-privacy-legislation/.

Leblond, Patrick. Forthcoming 2019. *Digital Trade Negotiations at the WTO: Let's Not Ignore the Challenges the CPTPP and the CUSMA Pose to Canadian Data Regulation*. CIGI Paper No. 227. Waterloo, ON: CIGI.

Maldoff, Gabe. 2016. "Top 10 operational impacts of the GDPR: Part 3 – consent." The Privacy Advisor, January 12. The International Association of Privacy Practitioners. https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/.

McDonald, Sean. 2019. "What Is Stalling Better Data Governance?" Opinion, June 7. Waterloo, ON: CIGI. www.cigionline.org/articles/what-stalling-better-data-governance.

Meltzer, Joshua P. 2019. "Governing Digital Trade." *World Trade Review* 18 (S1): 523–48.

Moody, Andrew and Cheng Yu. 2017. "'Digital silk road' expected to link world." *China Daily*, December 8. africa.chinadaily.com.cn/weekly/2017-12/08/content_35257746.htm.

Munro, Daniel. 2019. "Governing AI: Navigating Risks, Rewards and Uncertainty." Public Policy Forum, January 11. https://ppforum.ca/wp-content/uploads/2019/01/Governing-AI-PPF-Jan2019-EN.pdf.

O'Connor, Nuala. 2018. "Reforming the U.S. Approach to Data Protection and Privacy." Digital and Cyberspace Policy Program, January 30. New York, NY: Council on Foreign Relations. www.cfr.org/report/reforming-us-approach-data-protection.

Office of the Privacy Commissioner of Canada. 2019. "2018-19 Survey of Canadians on Privacy." Ottawa, ON: Office of the Privacy Commissioner of Canada. www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/.

Orol, Ronald. 2018. "The IMF Should Spark a Bretton Woods Moment for the Digital Age, Says Balsillie." Opinion, November 22. Waterloo, ON: CIGI. www.cigionline.org/articles/imf-should-spark-bretton-woods-moment-digital-age-says-balsillie.

Pfeifle, Sam. 2018. "US federal privacy law? Apple, Google, Facebook, Microsoft all hope so." The International Association of Privacy Professionals, October 25. https://iapp.org/news/a/us-federal-privacy-law-apple-google-facebook-microsoft-all-hope-so/.

Pichai, Sundar. 2019. "Google's Sundar Pichai: Privacy Should Not Be a Luxury Good." *The New York Times*, May 7. www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html.

Politi, James and Tom Mitchell. 2019. "Digital trade remains a stumbling block in US-China trade talks." *Financial Times*, March 23. www.ft.com/content/ffd51efe-4d9d-11e9-b401-8d9ef1626294.

Rentzhog, Magnus. 2015. "No Transfer, No Production — a Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods." Kommerskollegium 2015:1. Stockholm: National Board of Trade. www.kommers.se/In-English/Publications/2015/No-Transfer-No-Production/.

Rentzhog, Magnus and Henrik Jonströmer. 2014. "No Transfer, No Trade — the Importance of Cross-Border Data Transfers for Companies Based in Sweden." Kommerskollegium 2014:1. Stockholm: National Board of Trade. www.kommers.se/Documents/dokumentarkiv/publikationer/2014/No_Transfer_No_Trade_webb.pdf.

Scassa, Teresa. 2018. "Enforcement powers key to PIPEDA reform." *Policy Options*, June 7. policyoptions.irpp.org/magazines/june-2018/enforcement-powers-key-pipeda-reform/.

———. 2019. "Why Canada needs a national data strategy." *Policy Options*, January 15. policyoptions.irpp.org/magazines/january-2019/why-canada-needs-a-national-data-strategy/.

Scott, Mark. 2019. "Facebook's Clegg: Politicians must regulate to avoid 'Balkanized' internet." *Politico*, March 31. www.politico.eu/article/facebook-mark-zuckerberg-regulation-tech-europe-privacy-data-protection-washington-nick-clegg/.

Seddon, Max and Henry Foy. 2019. "Russian technology: can the Kremlin control the net?" *Financial Times*, June 5. www.ft.com/content/93be9242-85e0-11e9-a028-86cea8523dc2.

Serrato, Jeewon Kim, Chris Cwalina, Anna Rudawski, Tristan Coughlin and Katey Fardelmann. 2018. "US states pass data protection laws on the heels of the GDPR." Data Protection Report, July 9. Norton Rose Fulbright. www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/.

Shankar, Venkatesh, Glen L. Urban and Fareena Sultan. 2002. "Online trust: a stakeholder perspective, concepts, implications, and future directions." *Journal of Strategic Information Systems* 11 (3-4): 325–44.

Silberg, Jake and James Manyika. 2019. "Notes from the AI frontier: Tackling bias in AI (and in humans)." McKinsey Global Institute, June. www.mckinsey.com/featured-insights/artificial-intelligence/tackling-bias-in-artificial-intelligence-and-in-humans.

The Editorial Board. 2019. "Global Standards on Big Tech are sorely needed." *Financial Times*, April 1. www.ft.com/content/9945cb7e-5488-11e9-a3db-1fe89bedc16e.

Vallée, Paul. 2019. "Trust and Data: How Changes to the Privacy Landscape Can Bolster Innovation in Canada." In *Governing Cyberspace during a Crisis in Trust.* Waterloo, ON: CIGI. www.cigionline.org/articles/trust-and-data-how-changes-privacy-landscape-can-bolster-innovation-canada.

Wolfe, David A. 2019. "A Digital Strategy for Canada: The Current Challenge." IRPP Insight No. 25, February. Montreal, QC: Institute for Research on Public Policy. http://irpp.org/research-studies/a-digital-strategy-for-canada/.

WTO. 2017. "Joint Statement on Electronic Commerce." WT/MIN(17)/60, December 13. www.mofa.go.jp/mofaj/files/000355907.pdf.

———. 2019. "Joint Statement on Electronic Commerce." WT/L/1056, January 25. http://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157643.pdf.

Zuckerberg, Mark. 2019. "Mark Zuckerberg: The Internet needs new rules. Let's start in these four areas." *The Washington Post,* March 30. www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?noredirect=on.

Centre for International
Governance Innovation

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

@cigionline