Centre for International
Governance Innovation

CIGI Papers No. 227 – October 2019

Digital Trade at the WTO

The CPTPP and CUSMA Pose Challenges to Canadian Data Regulation

Patrick Leblond

Centre for International
Governance Innovation

CIGI Papers No. 227 — October 2019

Digital Trade at the WTO

The CPTPP and CUSMA Pose Challenges to Canadian Data Regulation

Patrick Leblond

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 Author

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.

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

AI	artificial intelligence
CETA	Comprehensive Economic and Trade Agreement
CPTTP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
CUSMA	Canada-United States-Mexico Agreement
FTA	free trade agreement
G20	Group of Twenty
GATS	General Agreement on Trade in Services
NAFTA	North American Free Trade Agreement
OPC	Office of the Privacy Commissioner of Canada
PIPEDA	Personal Information Protection and Electronic Documents Act
TPP	Trans-Pacific Partnership
USMCA	United States-Mexico-Canada Agreement
WTO	World Trade Organization

Executive Summary

On the margins of the Group of Twenty (G20) leaders' meeting in Osaka, Japan on June 28-29, 2019, Canada and 23 others signed the Osaka Declaration on the Digital Economy. This declaration launched the "Osaka Track," which reinforces the signatories' commitment to the World Trade Organization (WTO) negotiations on "trade-related aspects of electronic commerce." In this context, unlike its main economic partners (China, the European Union and the United States), Canada has yet to decide its position. The purpose of this paper is thus to help Canada define its position in those negotiations. To do so, it offers a detailed analysis of the e-commerce/digital trade chapters found in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Canada-United States-Mexico Agreement (CUSMA), the North American Free Trade Agreement's (NAFTA's) replacement, in order to identify the potential constraints that these agreements could impose on the federal government's ability to regulate data nationally as it seeks to establish a trusting digital environment for consumers and businesses. The analysis leads to the conclusion that Canada's CPTPP and CUSMA commitments could ultimately negate the effectiveness of future data protection policies that the federal government might want to adopt to create trust in the data-driven economy. As a result, Canada should not follow the United States' position in the WTO negotiations. Instead, the best thing that Canada could do is to push for a distinct international regime (i.e., separate from the WTO) to govern data and its cross-border flows.

Introduction

On the margins of the G20 leaders' meeting held in Osaka in June, Canada and its partners signed the Osaka Declaration on the Digital Economy.[1] The declaration states that the signatories, "standing together with other WTO Members that participate in the Joint Statement on Electronic Commerce issued in Davos on 25 January 2019, in which 78 WTO Members are on board, hereby declare the launch of the 'Osaka Track,' a process which demonstrates our commitment to promote international policy discussions." The January 2019 Joint Statement, issued during the World Economic Forum's annual meeting in Davos, Switzerland confirms the members' "intention to commence WTO negotiations on trade-related aspects of electronic commerce."[2] This Joint Statement is a restatement of a previous joint statement issued at the WTO's eleventh ministerial conference in Buenos Aires, Argentina in December 2017, where some 75 members, including Canada, "recognize[d] the important role of the WTO in promoting open, transparent, non-discriminatory and predictable regulatory environments in facilitating electronic commerce."[3] The Buenos Aires Joint Statement indicated that the signatories would begin exploratory work toward "future WTO negotiations on trade-related aspects of electronic commerce."[4]

A number of discussion rounds took place in 2018 and 2019 in Geneva, Switzerland in order to delimit the scope of potential plurilateral negotiations on electronic commerce/digital trade. At the end of April 2019, the key players in the negotiations, China, the European Union and the United States, issued their proposals.[5] The Chinese proposal is focused on principles without specific provisions, reflecting the country's desire to protect its walled-off digital realm (Aaronson and Leblond 2018). The European Union's proposal is much more detailed, offering specific provisions that support unrestricted cross-border data flows, although it also calls for "the adoption and application of rules for the cross-border transfer of personal data."

The US proposal, for its part, goes further than the European Union as it follows closely the digital trade chapter found in CUSMA[6] (see

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

2 See http://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157643.pdf.

3 See www.mofa.go.jp/mofaj/files/000355907.pdf.

4 Ibid.

5 For China's proposal, see https://docs.wto.org/dol2fe/Pages/FE_Search/ExportFile.aspx?id=253560&filename=q/INF/ECOM/19.pdf. For the European Union's proposal, see http://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf. For the US proposal, see https://drive.google.com/file/d/1mPHx-0nCevixcoobZXKMwWBcgaLDpFJf/view.

6 It is important to note that the agreement is known as the United States-Mexico-Canada Agreement (USMCA) in the United States. It was signed by all three parties on November 30, 2018, and ratified in Canada and Mexico in the spring of 2019. Ratification is still pending in the United States.

Baschuk 2019; Manak 2019). CUSMA was itself built on the Trans-Pacific Partnership's (TPP's)[7] electronic commerce (e-commerce) chapter.

Having signed two trade agreements containing extensive e-commerce/digital trade chapters with the United States (the TPP and CUSMA) suggests that Canada would support the US proposal; however, Canada has yet to make its position on the WTO negotiations known. In January 2019, the Government of Canada, under Global Affairs Canada's responsibility, launched a public consultation related to Canada's digital trade policies: "Canada's Future World Trade Organization (WTO) Negotiations on E-Commerce."[8] In addition to traditional trade issues such as customs duties, trade facilitation and market access (for goods and services), the consultation's backgrounder document indicates that the following themes also matter for the WTO negotiations: flow of information (data) across borders, access (to data) and non-discrimination, business trust, consumer trust, intellectual property, transparency and so on.[9] The consultation closed at the end of April 2019; however, the Government of Canada has not yet made its WTO negotiating position public, if it has defined it at all.

The purpose of this paper is to help Canada define its position in the WTO negotiations on trade-related aspects of e-commerce. To do so, it offers a detailed analysis of the e-commerce/digital trade chapters found in the CPTPP and CUSMA in order to identify the potential constraints that these agreements could impose on the federal government's ability to regulate data nationally as it seeks to establish a trusting digital environment for consumers and businesses.[10]

The analysis leads to the conclusion that Canada's CPTPP and CUSMA commitments could ultimately negate the effectiveness of future data protection policies that the federal government might want to adopt to achieve its "trust in the digital age" objective. As a result, Canada should not follow the United States' position in the WTO negotiations.[11]

The European Union's position, which puts more emphasis on protecting personal data and privacy, might therefore be a better approach for Canada to support, if it wishes to preserve for itself sufficient room to manoeuvre in terms of regulating data in the future.[12]

The best thing that Canada should do, however, is seek to remove issues related to data regulation from the "trade-related aspects of electronic commerce" negotiations and push for a separate international regime to govern data and its cross-border flows (see Leblond and Aaronson 2019). Just like capital (or financial) flows are not part of the WTO's framework,[13] which limits itself to rules on financial services, so too should data flows be excluded from an eventual agreement on trade-related aspects of e-commerce, which should focus its attention solely on digital goods and services.

The CPTPP, CUSMA and Data Regulation

International trade agreements regulate data flows through provisions aiming to facilitate the cross-border trade of goods and services built on data, such as data processing and other computing services (Aaronson 2018; Burri 2017). This section analyses the e-commerce/digital trade chapters included in the CPTPP and CUSMA in order to determine how they may affect data regulation in

7 The United States abandoned the TPP in January 2017 when President Donald Trump took office. The remaining 11 members, including Canada, signed the CPTPP in March 2018. The agreement entered into force on December 30, 2018, between Australia, Canada, Japan, Mexico, New Zealand and Singapore. The CPTPP entered into force in Vietnam on January 14, 2019. The agreement has yet to apply in Brunei, Chile, Malaysia and Peru.

8 See www.international.gc.ca/trade-commerce/consultations/wto-omc/index.aspx?lang=eng.

9 See www.international.gc.ca/trade-commerce/consultations/wto-omc/background-information.aspx?lang=eng.

10 On May 21, 2019, the Government of Canada published its Digital Charter, which is a set of 10 principles that are "the building blocks of a foundation of trust for this digital age" (see www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html).

11 As such, it might be another reason for CUSMA to be abandoned. According to Dan Ciuriak, Ali Dadkhah and Jingliang Xiao (2019), CUSMA's expected economic benefits for Canada are, on the whole, negative. Jeffrey Schott (2019) also concludes that the United States should not ratify the USMCA's version.

12 Besides data-related issues, Ciuriak (2019) identifies a number of other important issues related to trade in digital goods and services that the WTO negotiations should address.

13 The Financial Stability Board oversees and coordinates the various international bodies that set the standards that govern finance.

Canada.[14] Since the CPTPP's e-commerce chapter provided the basis for CUSMA's digital trade chapter, the analysis focuses first on the CPTPP.

The CPTPP

The CPTPP contains several provisions in its Chapter 14 (on e-commerce) that concern data.[15] Chapter 14 does not specify what types of data are covered, except to say those that are necessary for business purposes. It also preserves member states' ability to limit the free flow of data held by government entities. The CPTPP also encourages interoperability between data privacy regimes and encourages cooperation between consumer protection authorities.

Here are the CPTPP's main provisions relating to data:

- Consistent with the WTO's waiver on customs duties on electronic commerce, article 14.3 prohibits the imposition of customs duties on electronic transmissions; however, it allows "internal taxes, fees or other charges" as long as they are not discriminatory (i.e., applied equally to national as well as foreign entities).[16] As such, the CPTPP does not discriminate among various types or sources of data.
- Article 14.8 mandates a personal data protection floor; it ensures that member states have laws and regulations that provide a minimum level of personal information protection, but it is flexible as it accommodates different national approaches.[17]
- Article 14.11 protects the free flow of cross-border data for business purposes,[18] although it allows restrictions on such flows in order to achieve a "legitimate public policy objective."[19]
- Article 14.13 prohibits the obligation for a business to locate specific computing facilities in exchange for market access.[20] In other words, it prohibits member states from imposing data localization requirements. However, the "legitimate public policy objective" exception also applies in this case.
- Article 14.17 prohibits requirements that source code be transferred or accessed as a condition of import.[21] The prohibition is, however, limited to mass-market software, but not when it is used in critical infrastructure.[22] The prohibition also does not apply to requests for source code modification to comply with domestic laws of regulations, as long as the latter are not inconsistent with the CPTPP (i.e., they

14 Canada's other major recent free trade agreement (FTA), the Comprehensive Economic and Trade Agreement (CETA) with the European Union has a specific chapter on e-commerce (Chapter 16). Unlike the CPTPP and CUSMA, it does not address the cross-border transfer of data. The chapter follows long-standing WTO language that governments should prohibit custom duties (tariffs) on goods purchased online. CETA's other e-commerce provisions (for example, electronic signatures, spam, and fraudulent and deceptive commercial practices) are considered "best endeavours or too vague to be enforceable" (Wolfe 2018, 7). In terms of privacy protection, CETA's article 16.4 encourages but does not require the protection of personal information. Only when it comes to public telecommunications services, does CETA (in article 15.3, paragraph 4) require that the parties adopt measures to protect the privacy of the services' users (ibid., 9).

15 See http://international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/14.aspx?lang=eng.

16 Article 14.3: "1. No Party shall impose customs duties on electronic transmissions, including content transmitted electronically, between a person of one Party and a person of another Party. 2. For greater certainty, paragraph 1 shall not preclude a Party from imposing internal taxes, fees or other charges on content transmitted electronically, provided that such taxes, fees or charges are imposed in a manner consistent with this Agreement."

17 Article 14.8: "2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies. 3. Each Party shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction."

18 Article 14.11, paragraph 2: "Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person."

19 Article 14.11, paragraph 3: "Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are required to achieve the objective."

20 Article 14.13, paragraph 2: "No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."

21 Article 14.17, paragraph 1: "No Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory."

22 Article 14.17, paragraph 2: "For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure."

are not discriminatory in nature; they apply equally to domestic and foreign firms).[23]

CPTPP's article 14.2, paragraph 3 stipulates that "this Chapter shall not apply to: (a) government procurement; or (b) information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection." This means that prohibitions on data transfer restrictions and data localization found in articles 14.11 and 14.13 do not apply to governments. Therefore, the requirements imposed by the federal and some provincial governments that personal information held by public bodies be kept and processed in Canada are exempted under the CPTPP. This exception is potentially important if Canadian governments wish to make more publicly collected data available for analysis (for example, for artificial intelligence [AI] training purposes), but want to ensure that they retain control over them to protect individuals as well as the state.

The scope of application of article 14.2, paragraph 3 is, however, somewhat ambiguous when it comes to subnational governments, especially part (b). This is because article 1.3 defines "Party" as "any State or separate customs territory for which this Agreement is in force." As such, it would exclude subnational governments at the provincial and municipal levels, especially since "regional level of government" is defined separately in article 1.3.[24] The term "government procurement" in part (a) is less ambiguous. Article 15.2, paragraph 2 establishes the scope of application of government procurement: "For the purposes of this Chapter, covered procurement means government procurement: (a) of a good, service or any combination thereof as specified in each Party's Schedule to Annex 15-A." In Canada's schedule in Annex 15-A, Section B deals with sub-central government entities.[25] Government procurement provisions do not apply to schools, universities, hospitals and Crown corporations for all provinces and territories except Ontario and Quebec.[26] This means that only in Ontario and Quebec (the excluded provinces) could such public entities impose localization restrictions of data storage and processing in their procurement contracts.

The CPTPP's articles 14.11 and 14.13 — on the prohibition of, respectively, restrictions on cross-border data transfers for business purposes and requirements to localize the storage of data domestically — both contain an exception for a "legitimate public policy objective." This means that CPTPP member states such as Canada can restrict the in-and-out flow of data in order to pursue such an objective. The big question, however, is: what is a "legitimate" objective? Article 14.11, paragraph 3 states that a measure restricting cross-border data transfers cannot: be "applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade;" and "impose restrictions on transfers of information greater than are required to achieve the objective." Article 14.13, paragraph 3 offers the same limitation on the "legitimate public policy objective" (also called general) exception: "Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective."

Michael Geist (2018) questions whether privacy protection would qualify under the above-mentioned exception. He seems doubtful when he writes: "the [CPTPP] restriction on the use of data localization requirements may pose an insurmountable barrier." The same conclusion would apply to article 14.11 on data transfers. For instance, in early April 2019, the Office of the Privacy Commissioner of Canada (OPC) released a consultation paper on transborder data flows in which it indicates that it would require a company

23 Article 14.17, paragraph 3(b): "Nothing in this Article shall preclude: a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement."

24 According to law professor Debra Steger (2018), a state refers to a nation-state and does not cover subnational governments (separate customs territory refers to customs union such as the European Union).

25 See http://international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/15-a3.aspx?lang=eng.

26 Note 5 to Section B in Canada's schedule in Annex 15-A says: "For those provinces and territories marked by an obelisk (†), Chapter 15 (Government Procurement) shall not cover the procurement of goods, services or construction services purchased for the benefit of, or which is to be transferred to the authority of, school boards or their functional equivalents, publicly-funded academic institutions, social services entities or hospitals." Note 6 to Section B applies to Crown corporations.

to obtain prior consent from individuals before moving their personal data outside of Canada.[27] According to Geist (2019), this new approach "is a significant reversal of longstanding policy that relied upon the accountability principle to ensure that organizations transferring personal information to third parties are ultimately responsible for safeguarding that information."[28] The OPC stated that this new approach would be consistent with Canada's international trade obligations. Geist (ibid.) is not so sure, however: "The imposition of consent requirements for cross-border data transfers could be regarded as imposing restrictions greater than required to achieve the objective of privacy protection, given that PIPEDA [Personal Information Protection and Electronic Documents Act] has long been said to provide such protections through accountability without the need for this additional consent regime."[29]

Andrew D. Mitchell and Neha Mishra (2018), for their part, also point out that there is the potential for conflict between e-commerce or digital trade chapters in FTAs and WTO agreements such as the General Agreement on Trade in Services (GATS). They write that GATS article XIV provides the basis for the general exception found in FTA provisions such as the CPTPP's articles 14.11 and 14.13; however, they also note that "these exceptions may be unable to address all aspects of data flow restrictions" (ibid., 1095). In addition, Mitchell and Mishra mention that "strict scrutiny of these measures [restricting data flows] under international trade law may lead to unsatisfactory outcomes because GATS Articles XIV are limited in scope and do not facilitate consideration of Internet trust issues holistically" (ibid.). The above implies that general exceptions on data transfers and data localization found in the CPTPP may not offer as much policy flexibility as originally thought with respect to future laws and regulations that Canadian governments might want to put into place to govern data in order to ensure trust as well as stimulate innovation.

Given that algorithms "drive what news content and advertising each of us sees online [and] will be used by governments to decide who receives or is denied benefits" (Scassa 2018), it is reassuring that the CPTPP's article 14.17 does not prevent governments from regulating and supervising source codes, as long as it is not done in a protectionist way against foreign producers. Teresa Scassa (ibid.) notes that it is necessary to be able to access the source code of an app, software or AI in order to evaluate algorithms' performance and potential biases. Such enquiries are important if the government wants to protect consumers, workers and businesses from suffering the negative consequences associated with, for example, fraud or discrimination.

CUSMA

CUSMA, unlike NAFTA, which it is supposed to replace, contains a chapter (19) on "digital trade" (not "e-commerce," in order to signify its broader scope) that builds on the CPTPP's Chapter 14.[30] As such, CUSMA introduces a number of differences from the CPTPP. The following analysis focuses on these differences.

One significant difference with the CPTPP concerns the requirement for CUSMA member states to "adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade" (article 19.8, paragraph 2). While CUSMA does not prescribe specific rules or measures that a party must take to protect privacy, it goes further than the CPTPP by providing more guidance to inform a country's privacy regime. In particular, CUSMA refers explicitly to the APEC [Asia-Pacific Economic Cooperation] Privacy Framework and

27 See www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transborder-dataflows/.

28 In light of the government's publication of the Digital Charter, the OPC reframed its consultation in June 2019, putting less emphasis on its interest in requiring businesses to obtain prior consent from individuals before transferring their data abroad (see www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transfers-for-processing/).

29 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 OPC, 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.

30 See https://international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/text-texte/toc-tdm.aspx?lang=eng.

OECD [Organisation for Economic Co-operation and Development] Guidelines as relevant "principles and guidelines" when developing a legal framework for protecting personal information.[31] Unlike the CPTPP, CUSMA also mentions key principles that member states should follow as they develop their legal framework.[32]

In addition, CUSMA stipulates that the parties "recognize the importance of…ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented" (article 19.8, paragraph 3), thereby providing some limit on the extent to which data protection legislation or regulation can constrain cross-border personal data flows. Such a standard for potentially restricting data flows in order to protect personal information is not present in the CPTPP's article 14.8, paragraph 2. As such, it provides some guidance, albeit vague, to future panel arbitrators in interpreting the "legitimate public policy objective" exception in the case of a dispute involving limits imposed on cross-border data flows by one of the CUSMA parties. The big issue in this case is what does "necessary and proportionate" mean in the context of protecting personal information? For instance, would a requirement for organizations in Canada to obtain explicit consent from individuals before the latter's data are transferred across the border to the United States be deemed necessary and proportionate?

What is probably the most important difference between CUSMA and the CPTPP is the former's article 19.17 on Interactive Computer Services, which has no equivalent in the CPTPP. According to this article, internet service providers, social media platforms and search engines cannot be treated as information content providers for liability purposes, which means "immunity from legal consequences for content generated by users" (Israel and Tribe 2018).[33] However, Annex 19-A, paragraph 4 states: "For greater certainty, Article 19.17 (Interactive Computer Services) is subject to Article 32.1 (General Exceptions), which, among other things, provides that, for purposes of Chapter 19, the exception for measures necessary to protect public morals pursuant to paragraph (a) of Article XIV of GATS is incorporated into and made part of this Agreement, *mutatis mutandis*." This paragraph opens the door for potential limits on the article's scope and application but, as mentioned above, there is a lot of uncertainty with respect to the general exception's reach. In any case, CUSMA's article 19.17 will likely make it harder for Canadian governments to develop measures to protect individuals and consumers of social media, search engines and other user-generated content providers from the consequences of disinformation (for example, "fake news").

Another noteworthy difference between CUSMA and the CPTPP concerns source code and algorithms. First, CUSMA's article 19.16 gets rid of the CPTPP's article 14.17, paragraph 2.[34] This implies that all types of source code are covered by CUSMA, without exception. As Scassa (2018) notes: "This may raise some interesting concerns given the growing government use of software and algorithms in key systems and processes." CUSMA also does not contain the CPTPP's provision on allowing requests for source code modification.[35] Instead, it offers article 19.16, paragraph 2, which does not exist in the CPTPP: "This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination, enforcement

31 The CPTPP's article 14.8, paragraph 3 states only that "each Party should take into account principles and guidelines of relevant international bodies" (it does not mention any particular international body, however).

32 CUSMA's article 19.8, paragraph 3 states: "The Parties recognize that pursuant to paragraph 2, key principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability."

33 CUSMA's article 19.17, paragraph 3 states: "No Party shall impose liability on a supplier or user of an interactive computer service on account of: (a) any action voluntarily taken in good faith by the supplier or user to restrict access to or availability of material that is accessible or available through its supply or use of the interactive computer services and that the supplier or user considers to be harmful or objectionable; or (b) any action taken to enable or make available the technical means that enable an information content provider or other persons to restrict access to material that it considers to be harmful or objectionable."

34 The CPTPP's article 14.17, paragraph 2 states: "For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure."

35 The CPTPP's article 14.17, paragraph 3(b) states: "Nothing in this Article shall preclude a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement."

action, or judicial proceeding, subject to safeguards against unauthorized disclosure." Scassa (ibid.) says that the difference between CUSMA and the CPTPP provisions is "important given that we are already facing context in which it is necessary to understand the algorithms that lead to certain decisions [for example, litigation involving autonomous vehicles]." So, CUSMA improves on the CPTPP in terms of source code transparency but it is also a step back when it comes to requesting modifications to algorithms, which could be found to be biased or causing harm to people, businesses or governments. In the latter case, a Canadian request for algorithmic modification could be challenged under CUSMA as a protectionist measure discriminating against the American or Mexican producer of the software or application.

The final difference between CUSMA and the CPTPP is with respect to the provisions on data localization ("Location of Computing Facilities"). In the CPTPP's article 14.13, "The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications" (paragraph 1) but "no Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory" (paragraph 2) unless it is for a "legitimate public policy objective" (paragraph 3).[36] For its part, CUSMA's article 19.12 only has one provision: "No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory." This means that, unlike the CPTPP, CUSMA does not allow its member states to invoke a "legitimate public policy objective" exception to impose a data localization requirement to firms from the other two parties as a condition for providing a digital good or service in the territory. The only exception possible here is for the specific case when a digital good or service is provided to a government, because CUSMA's Chapter 19 does not apply to "government procurement; or except for Article 19.18 (Open Government Data), to information held or processed by or on behalf of a Party, or measures related to that information, including measures related to its collection" (article 19.2, paragraph 3). Therefore, governments can only require organizations that collect, hold or process information to locate their computing facilities in the territory when these activities are undertaken for or on behalf of a government, which is in line with current practices. However, if, for example, data deemed critical for national security reasons were held by a private organization, then CUSMA would technically require a government to allow these data to be held and processed in the other two member states' territories. As a result, these data could become accessible to the other member-state governments (for example, through the USA PATRIOT Act in the United States).

Conclusion

With the CPTPP and CUSMA, which still needs to be ratified, Canada has adopted obligations that provide for the free flow across borders of data for business purposes while, in principle, protecting consumers, personal information (privacy) and government-related data. However, as analyzed above, these two trade agreements also pose potential obstacles to Canada's ability to effectively regulate data and provide a trustworthy environment for individuals, businesses and governments. The analysis herein shows that it is not at all clear how much policy flexibility the CPTPP and CUSMA will ultimately allow the federal and provincial governments in adopting new laws and regulations to, among various objectives, protect people's privacy, prevent algorithmic bias, protect critical infrastructure, ensure national security or promote domestic innovation. This means that Canada would err if it were to follow the United States' position in the negotiations for an agreement on "trade-related aspects of electronic commerce" at the WTO. To preserve its room for manoeuvre to regulate data in the future in order to provide a digital environment that individuals, firms and governments can trust, the Government of Canada would be better to follow the European Union's position. However, the best thing that Canada could do is to push for a distinct international regime (i.e., separate from the WTO) to govern data and its cross-border flows, as argued by Patrick Leblond and Susan Aaronson (2019).

36 The CPTPP's article 14.13, paragraph 3 states: "Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective."

Works Cited

Aaronson, Susan Ariel. 2018. "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.

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

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.

Burri, Mira. 2017. "The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation." *UC Davis Law Review* 51: 65–132.

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

Ciuriak, Dan, Ali Dadkhah and Jingliang Xiao. 2019. "Quantifying CUSMA: The Economic Consequences of the New North American Trade Regime." Working Paper July 25. Toronto, ON: C.D. Howe Institute. www.cdhowe.org/sites/default/files/attachments/research_papers/mixed/WorkingPaper_Ciuriak-Dadkhah-Xiao_2019.pdf.

Geist, Michael. 2018. "Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards." In *Data Governance in the Digital Age.* Waterloo, ON: CIGI. www.cigionline.org/publications/data-governance-digital-age.

———. 2019. "Canadian Privacy Commissioner Signals Major Shift in Approach on Cross-Border Data Transfer." April 10. www.michaelgeist.ca/2019/04/canadian-privacy-commissioner-signals-major-shift-in-approach-on-cross-border-data-transfers/.

Israel, Tamir and Laura Tribe. 2018. "Did NAFTA 2.0 sign away our digital future?" *Ottawa Citizen*, October 15. https://ottawacitizen.com/opinion/columnists/israel-and-tribe-did-nafta-2-0-sign-away-our-digital-future.

Leblond, Patrick and Susan Ariel Aaronson. 2019. *A Plurilateral "Single Data Area" Is the Solution to Canada's Data Trilemma.* CIGI Papers No. 226. Waterloo, ON: CIGI.

Manak, Inu. 2019. "U.S. WTO E-commerce Proposal Reads Like USMCA." *International Economic Law and Policy Blog*, May 8. https://worldtradelaw.typepad.com/ielpblog/2019/05/us-wto-e-commerce-proposal-reads-like-usmca.html.

Mitchell, Andrew D. and Neha Mishra. 2018. "Data at the Docks: Modernizing International Trade Law for the Digital Economy." *Vanderbilt Journal of Entertainment & Technology Law* 20: 1073–134.

Scassa, Teresa. 2018. "What Role for Trade Deals in an Era of Digital Transformation?" Opinion, October 4. Waterloo, ON: CIGI. www.cigionline.org/articles/what-role-trade-deals-era-digital-transformation.

Schott, Jeffrey J. 2019. "Just Say No to the New Nafta." *Bloomberg*, July 16. www.bloomberg.com/opinion/articles/2019-07-16/trump-s-nafta-alternative-is-a-bad-deal.

Steger, Debra (@DebraPS). 2018. "No. A State is a nation state. A separate customs territory like the EU can also be a Party to a CU or an FTA under Art XXIV GATT. University or hospital is a person or an enterprise." Twitter, August 4, 2018, 3:25 a.m. https://twitter.com/DebraPS/status/1025643907097350144.

Wolfe, Robert. 2018. "Learning about digital trade: Privacy and e-commerce in CETA and TPP." EUI Working Papers, RSCAS 2018/27, Florence, Italy: Global Governance Programme-305, Robert Schuman Centre for Advanced Studies, European University Institute. https://cadmus.eui.eu/handle/1814/55144.

Centre for International
Governance Innovation

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

@cigionline