European University Institute
ROBERT SCHUMAN CENTRE FOR ADVANCED STUDIES

WORKING PAPERS

RSCAS 2018/27
Robert Schuman Centre for Advanced Studies
Global Governance Programme-305

Learning about digital trade:
Privacy and e-commerce in CETA and TPP

Robert Wolfe

European University Institute

Robert Schuman Centre for Advanced Studies

Global Governance Programme

Learning about digital trade: Privacy and e-commerce in CETA and TPP

Robert Wolfe

EUI Working Paper **RSCAS** 2018/27

ISSN 1028-3625

Printed in Italy, May 2018
European University Institute
Badia Fiesolana
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu/RSCAS/Publications/
www.eui.eu
cadmus.eui.eu

Robert Schuman Centre for Advanced Studies

The Robert Schuman Centre for Advanced Studies (RSCAS), created in 1992 and directed by Professor Brigid Laffan, aims to develop inter-disciplinary and comparative research and to promote work on the major issues facing the process of integration and European society.

The Centre is home to a large post-doctoral programme and hosts major research programmes and projects, and a range of working groups and *ad hoc* initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration and the expanding membership of the European Union.

Details of the research of the Centre can be found on:
http://www.eui.eu/RSCAS/Research/

Research publications take the form of Working Papers, Policy Papers, Policy Briefs, Distinguished Lectures, Research Project Reports and Books.

Most of these are also available on the RSCAS website:
http://www.eui.eu/RSCAS/Publications/

The Global Governance Programme at the EUI

The Global Governance Programme is one of the flagship programmes of the Robert Schuman Centre for Advanced Studies at the European University Institute (EUI). It aims to: build a community of outstanding professors and scholars, produce high quality research and, engage with the world of practice through policy dialogue. At the Global Governance Programme, established and early career scholars research, write on and discuss, within and beyond academia, issues of global governance, focussing on four broad and interdisciplinary areas: European, Transnational and Global Governance; Global Economics; Europe in the World; and Cultural Pluralism.

The Programme also aims to contribute to the fostering of present and future generations of policy and decision makers through its unique executive training programme, the Academy of Global Governance, where theory and "real world" experience meet. At the Academy, executives, policy makers, diplomats, officials, private sector professionals and academics, have the opportunity to meet, share views and debate with leading academics, top-level officials, heads of international organisations and senior executives, on topical issues relating to governance.

For more information: http://globalgovernanceprogramme.eui.eu

Abstract

It is a truth universally acknowledged that every ambitious 21st century trade agreement is in want of a chapter on electronic commerce. One of the most politically sensitive and technically challenging issues is personal privacy, including cross-border transfer of information by electronic means, use and location of computing facilities, and personal information protection. States are learning to solve the problem of state responsibility for something that does not respect their borders while still allowing 21st century commerce to develop. A comparison of the Canada-European Union Comprehensive Economic and Trade Agreement (CETA) and the Trans-Pacific Partnership (TPP) allows us to see the evolution of the issues thought necessary for an e-commerce chapter, since both include Canada, and to see the differing priorities of the U.S. and the EU, since they are each signatory to one of the agreements, but not of the other. I conclude by seeking generalizations about why we see a mix of aspirational and obligatory provisions in free trade agreements. I suggest that the reasons are that governments are learning how to work with each other in a new domain, and learning about the trade implications of these issues.

Keywords

Digital trade; electronic commerce; trade agreements.

1. The problem[*]

It is a truth universally acknowledged that every ambitious 21st century trade agreement is in want of a chapter on electronic commerce.[1] Of the 275 regional/bilateral trade agreements (RTAs) currently in force that had been notified to the World Trade Organization (WTO) by May 2017, 75 have e-commerce provisions, and such provisions are included in more than 60% of the RTAs that entered into force between 2014 and 2016 (Monteiro and Teh, 2017, 6).[2] While these chapters are called "e-commerce", they include things that go beyond the WTO definition of "the production, distribution, marketing, sale or delivery of goods and services by electronic means." One of the most politically sensitive and technically challenging issues is the privacy of personal information. Among the more than two dozen main types of provisions related to e-commerce in RTAs, three matter for privacy: cross-border transfer of information by electronic means, found in 19 agreements; use and location of computing facilities in 2; and personal information protection in 44 (Monteiro and Teh, 2017, 14). The diversity of approaches, even of definitions of "e-commerce", shows that states are still learning how to regulate in this domain.

Digital trade is deeply challenging for a territorial conception of states and their jurisdiction, because the internet is not physical. This is not the place for a theory of territoriality (Ruggie, 1993) nor of changing conceptions of the role of the state in 21st century governance (Macdonald and Wolfe, 2009), but we should recognize two things: first, citizens still look to the state for protection, including of their privacy; and second, the default setting of the state is to attempt to exert territorial control. An example of this difficulty is efforts to ensure privacy by demanding that computer servers be located at home. The digital trade story is about how states are learning to solve the problem of state responsibility for something that does not respect their borders while still allowing 21st century commerce to develop.

I explore this problem in a comparison of two recent trade agreements, the Canada-European Union Comprehensive Economic and Trade Agreement (CETA) and the Trans-Pacific Partnership (TPP). CETA was signed in October 2016 and was provisionally in force as of September 21, 2017, but the e-commerce chapter was substantially complete in 2012. The TPP text was released in January 2016, four years later than the completion of the CETA e-commerce chapter, but remains unratified after the U.S. pulled out in January 2017.[3]

Canada is caught between the EU—the most comprehensive privacy regime in the world—and the U.S., home of the largest digital players. A comparison of CETA and TPP allows us to see the evolution of the issues thought necessary for an e-commerce chapter, since both include Canada, and we see the differing priorities of the U.S. and the EU, since they are each signatory to one of the agreements, but not of the other. The two chapters differ from each other even on something as simple as the definitions of their domain, in CETA 16.1 and TPP 14.1. Although a snapshot of two moments in time in a rapidly evolving area, the comparison therefore sheds light on the difficulties that may be faced in future trade negotiations involving the EU and the U.S., including the exploratory work

---

[*] An earlier version of this paper was presented at the Columbia Law School Trade Seminar Series on November 6, 2017. I am grateful for insightful comments from Susan Ariel Aaronson, Henry Gao, Bernard Hoekman, Petros C. Mavroidis and Roy Santana, for the able research assistance of Grace Tahan, Sifat Syeda, and Maria Bridgemohan; and for confidential interviews in Geneva and Ottawa.

1 With apologies to Jane Austen.

2 Note that this important study did not include CETA and TPP.

3 TPP included Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, USA, and Vietnam. The remaining 11 parties signed the Comprehensive and Progressive TPP (CPTPP) on March 8, 2018; it is likely to be ratified by enough countries to enter into force by early 2019. The differences between CPTPP and TPP do not affect the provisions relevant to this article.

launched at the WTO's 2017 Buenos Aires ministerial (WTO, 2017), and a possible resumption of the negotiations for a Trade in Services Agreement (TiSA) and the Transatlantic Trade and Investment Partnership (TTIP).

In the next section I briefly address why we have trade agreements in general, and why ambitious ones now include chapters on e-commerce; and then in the following section I show how the EU, Canada and the U.S. can be arrayed along a privacy continuum. I next explore the difference between CETA and TPP with respect to privacy, data flows, location of computing facilities, and institutional provisions. I conclude by seeking generalizations about why we see a mix of aspirational and obligatory provisions in free trade agreements. I suggest that the reasons are that governments are learning how to work with each other in a new domain, and learning about the trade implications of these issues.

2. Why have a trade agreement?

The major reason to have a trade agreement, especially one that covers behind-the-border policies, is to reduce uncertainty for governments and firms, which is not the same as creating certainty, nor is it the same as the standard terms of trade argument.[4] Three factors influence the timing and content of attempts to reduce uncertainty in the domain of e-commerce. The first is technological and economic change. The digital world is changing fast—digital flows globally are said to have been 45 times larger in 2014 than 2004 (Manyika, Lund, Bughin, et al., 2016), and the rate of increase is not slowing. Restrictions on these flows are not new, but they too have increased in the last decade (Ferracane, 2017, Figure 1).

Second, as governments attempt to deal with these changes, they discover that differences in their regulatory frameworks create an interface issue, which alters their view of the need for some form of international regulatory cooperation—so called "interoperability" is one response, in addition to the usual alternatives of alignment, harmonization, and mutual recognition. While the U.S., the EU and Canada all say they want to facilitate e-commerce, that does not mean that their interests coincide, or that they are equally responsive to business demands. The issues placed by the USTR on the TPP negotiating agenda primarily reflect concerns that American companies had been facing in foreign markets (Mishra, 2017, 33), but Canadian negotiators were also hearing more and more from business about their needs.

Finally, as personal information flows more freely than ever before, making it harder for individuals to guard their privacy, high profile data breaches and cyber-attacks, along with things like the Facebook controversy of early 2018, lead to public demands for governments to act. But since data flows everywhere, governments cannot act at home without some sort of international coordination, which for the moment leads to trade agreements. Although here as in other domains, a trade agreement might not be the best vehicle for regulatory cooperation (Wolfe, 2017, 29), if the objective is some form of equivalence.

While a coherent global data protection and privacy regime may be desirable, what the world has now is highly fragmented. Aaronson and Leblond suggest that digital realms are emerging in the EU, the U.S., and China. Their view is that small countries have to pick one or the other realm, which they helpfully describe in considerable detail (Aaronson and Leblond, forthcoming). While research making this claim about China is novel, although it reflects a common worry sparked by China's Belt and Road initiative (Chaisse and Matsushita, 2018), we know that the EU and the U.S. tend to favour their own template for RTAs. Many analysts have observed that TPP draws on past U.S. RTAs, notably the e-commerce provisions (Gao, 2018), and Chapter 2 builds on both WTO, and past U.S. RTAs (Santana, in press).

[4] For a more extensive discussion of this claim, see (Wolfe, 2017).

Others have observed that both the U.S. and the EU try to use negotiation of their RTAs to transfer their regulatory regimes to other countries (Horn, Mavroidis and Sapir, 2010). Hence when I come to the textual comparison in section 4, I will be especially interested in the sources of the language of the e-commerce chapters. But first, I consider the differences in the privacy regimes of the parties.

3. The privacy continuum

The privacy aspects of e-commerce chapters may be the most puzzling for trade people. Some scholars see all such policies as trade restrictions (Ferracane, Lee-Makiyama and Van Der Marel, 2018). Others are critical of efforts (especially by the U.S.) to use trade agreement to undermine privacy law (Greenleaf, 2016a). The problem is familiar: parties have to find a way to reconcile differing regulatory approaches. But the reason to regulate "privacy", and the way to do it, is rooted in culture, legal evolution, and especially constitutional norms. National conceptions of privacy will inform trade agreements and national conceptions can meaningfully be enforced only within national jurisdictions. The poles are illustrated by Europeans who are more worried about rapacious firms, and Americans who worry more about an intrusive government. Canadians are caught in the middle. TPP and CETA are especially interesting, therefore, because they are at the poles, and yet both have privacy provisions acceptable to Canada.

EU privacy

Privacy rules promulgated by the EU Commission are secondary law, derived from the principles and objectives set out notably in the *Treaty on the Functioning of the European Union* (TFEU) and the *Charter of Fundamental Rights of the European Union*. Articles 7 and 8 of the Charter guarantee both the right to privacy and an independent right to the protection of personal data (Yakovleva, forthcoming, 10). Implementing such rights in legislation requires some acceptable compromise among the Member States.

The European Data Protection Directive of 1995 was intended to harmonize the privacy standards of the Member States to ensure the protection of personal data of EU citizens, including when such data is transferred outside the EU. Under Article 288 of the TFEU, "directives" leave national authorities free to choose the form and method of implementation, while a "regulation" is directly applicable in all Member States. As part of the current plan to create a Digital Single Market for Europe (EU, 2017b), complementing the single market for goods and services that is one of the foundations of the EU, the Commission decided to transform the data directive into a regulation.

The General Data Protection Regulation (GDPR) is intended to offer businesses simplified rules, and new opportunities while encouraging innovation. The GDPR (Regulation (EU) 2016/679) is a complex set of rules that place a heavy onus on firms to protect personal data. My interest is in how the Commission deals with the problem of differing regulations in other countries. The CETA e-commerce chapter was negotiated while the EU legal regime was still the Data Protection Directive, but the Commission had already started the process which led to the adoption of the GDPR after the CETA text was complete, hence the GDPR is my reference point.

In the Preamble to the GDPR, (103) the Commission may decide that a third country "offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union…. In such cases, transfers of personal data to that third country … may take place without the need to obtain any further authorisation." In reaching such an adequacy decision, (104) "The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union..." and one indicator of such equivalency (105) could the third country's accession to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (also known as Convention 108). Only a handful of countries

outside the Council of Europe have ratified Convention 108, but others are in process.[5] Whether that will lead to standards seen as adequate by the EU is not clear (Greenleaf, 2016b; Greenleaf, 2017a).

The Commission is clear: the EU data protection rules cannot be the subject of negotiations in a free trade agreement. Privacy they say is not a commodity to be traded (EU, 2017a), but horizontal provisions for cross-border data flows and personal data protection in trade negotiations can aim at reducing protection barriers in other countries (EU, 2018). Free traders in Europe worry that the EU position tilts too far towards protecting privacy, and not enough towards facilitating digital trade. Some scholars think such a mandate in trade agreements is essential to balance interests protected by trade law and those protected by human rights law (Yakovleva, forthcoming). The Commission (EU, 2017a, 6) argues that an

> An adequacy finding allows the free flow of personal data from the EU without the EU data exporter having to implement any additional safeguards or being subject to further conditions. In finding that its legal order provides an adequate level of protection, the decision recognises that the country's system approximates that of the EU Member States. As a result, transfers to the country in question will be assimilated to intra-EU transmissions of data, thereby providing privileged access to the EU single market, while opening up commercial channels for EU operators.

An adequacy decision under Article 45 of the GDPR by the Commission is therefore unilateral, but can follow consultations with the other country, as is the case with Canada, and the Privacy Shield discussed below rests on an EU-U.S. agreement about the rules applicable to U.S. firms. The collaborative process gets the EU to a position of determining that rules offer equivalent protection.

Canadian law

Canada's *Charter of Rights and Freedoms*, part of the *Constitution Act, 1982*, "is almost exclusively a compendium of negative rights running against only the government itself, not positive rights that the state has a duty to secure more broadly within society (Krotoszynski, 2016, 59)." In consequence, the European idea of a positive duty to secure privacy rights has no basis in Canadian constitutional law.

Canada has two federal laws that govern the protection of personal information; the *Privacy Act*, which covers the personal information-handling practices of federal government departments and agencies, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the federal private-sector privacy law (Power, 2017). PIPEDA is horizontal: it sets out the ground rules for how all private-sector organizations collect, use or disclose personal information in the course of commercial activities (Canada, 2009, Principle 4.1.3 of Schedule 1).

PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing, and its rules governing such transfers do not require a particular legal framework for protection in a foreign jurisdiction. Rather, the transferring organization is accountable for the information in the hands of the organization to which it has been transferred, subject to oversight by the Privacy Commissioner of Canada. Organizations must be transparent about their personal information handling practices. This includes advising customers that their personal information may be sent to another jurisdiction for processing and that while the information is in another jurisdiction it may be accessed by the courts, law enforcement and national security authorities.

Officials say that Canada recognizes that growth in international trade and competitiveness in the digital economy depends on seamless and uninterrupted flows of information across borders, but individuals must have confidence that their personal information is protected wherever it travels.

[5] https://www.coe.int/en/web/data-protection/convention108/parties. All EU countries are members of the CoE; Canada is an observer.

Business recognizes that concern, but it is only one of many issues they think should be addressed in e-commerce policy (Canada, 2018a).

PIPEDA, first proposed in 2000 but since amended, most recently in 2015 by the *Digital Privacy Act*, was motivated the EU Data Protection Directive of 1995 (Soma and Rynerson, 2008). In 2001, the EU formally recognized PIPEDA as providing an "adequate" level of data protection for the purposes of the Directive, thereby permitting transfers of personal data from the EU to Canada without the need for additional safeguards or the need for foreign firms to individually show compliance with EU privacy laws. PIPEDA was again under review at the time of writing, with a House of Commons report recommending changes including stronger enforcement powers for the Privacy Commissioner (Canada, 2018b). The EU has apparently signaled that the current adequacy finding only covers PIPEDA. Given the stronger protections envisaged in the GDPR, future adequacy decisions will involve a comprehensive assessment of a country's privacy regime, including access to personal data by public authorities for law enforcement, national security, and other public interest purposes (Canada, 2018b, 65).

U.S. privacy law

U.S. privacy law is less protective of individual privacy than Canadian law (Krotoszynski, 2016, 59)—Americans worry more about an intrusive government and are traditionally trusting of business. State constitutions often provide more protection for individual privacy than the U.S, constitution. At least 10 state constitutions contain explicit right to privacy clauses and others have some form of a right to privacy through court interpretations of their state constitutions (Soma and Rynerson, 2008).

In the absence of general legislation, U.S. privacy law is a confusing patchwork. The main federal legislation is the *Federal Trade Commission Act*, which prohibits "unfair" and "deceptive" acts or practices in or affecting commerce. The Federal Trade Commission (FTC) also enforces targeted (or vertical) statutes that protect information relating to health, credit and other financial matters, as well as children's online information. Exceptions to FTC jurisdiction include banks, airlines, insurance, and common carrier activities of telecommunications service providers where a mix of legislation and self-regulation allows companies and industry bodies to establish codes of practice (Soma and Rynerson, 2008) on the assumption that the market will do a better job at reaching a balance between commercial needs and privacy interests (Cockfield, 2010). The FTC has enforcement powers over privacy-related contractual provisions, such as the power to issue orders and seek consumer redress in certain circumstances, but federal law does not stipulate what those provisions should be (Branstetter, 2016, 79).

This system makes it difficult for U.S. firms to show that they follow EU rules, because there is no comprehensive legal regime that can be shown to be adequate. The first attempt to bridge this divide, called Safe Harbor, collapsed after a legal challenge. The replacement EU-U.S. agreement, called Privacy Shield, relies on commitments by participating companies to apply the high data protection standards of the agreement that are in turn enforceable under U.S. law by the FTC (EU, 2017a, 7). EU regulators in their first annual review were not convinced that the system is working.[6] Privacy Shield is unlikely to be the last word on finding ways to ensure that U.S. practices are deemed adequate under the GDPR.

The Atlantic divide

These differing conceptions of privacy rest on constitutional foundations on both sides of this Atlantic, even if the divide manifests itself as a difference over the priority to be assigned to commercial or rights considerations (Watanabe, 2017, 1115). The EU insists on adequate protection, the U.S. worries

[6] https://iapp.org/media/pdf/resource_center/Privacy_Shield_Report-WP29pdf.pdf

that data protection is a trade barrier that could serve as a camouflage for protectionism (Berka, 2017). Policies designed to privilege human rights will seem to restrain trade more than policies designed to preserve trust in online commerce (Yakovleva, forthcoming).

U.S. experts and former practitioners lament the fragmented implementation of U.S. privacy law, not least because it cedes a lead role to the EU (Hyman and Kovacic, 2018). This puts U.S. companies at a disadvantage globally as emerging economies adopt simpler, and often more EU-style, comprehensive approaches (O'connor, 2018). The Obama Administration proposal for a Consumer Privacy Bill of Rights Act went nowhere, but in light of the Facebook controversy, some Americans think it is time the U.S. had a horizontal privacy law with similar objectives to the GDPR.

In the meantime, foreign data companies need to comply with the GDPR to do business with Europeans. Many will simply adopt European standards globally rather than have to meet multiple sets of privacy regulations, although the EU does not require firms to apply the GDPR rules to non-European data held outside the EU. Indeed in response to the scandal over use of its data in early 2018, Facebook said it would apply the EU privacy standards, but not other regulatory requirements, around the world, with appropriate adaptation to local laws (Scott, 2018). As I was finishing my research on the GDPR, I received an email in Canada from the maker of my wireless home sound system telling me that they were updating their privacy statement. The company's FAQ states "We now meet the high standard required by the European Union's General Data Protection Regulation (GDPR)…. And because we believe that all our customers can benefit from its mandates, we're implementing it globally."[7] The GDPR may become the de facto global standard in the absence of a coherent U.S. approach, and the current global standard for data privacy laws seems closer to the EU standards than those of the OECD (Greenleaf, 2017b). Canadian law is evolving towards greater compatibility with the EU approach.

4. Textual comparison of the CETA and TPP e-commerce chapters

The e-commerce chapter in TPP is perhaps the most ambitious yet seen in an RTA. The difference with CETA is because it is more recent, but also because of the differing parties in the negotiations. The chapters may also differ for other reasons. I do not consider the chapters as part of a bargain in the overall agreement, nor do I consider the chapters as bargains in themselves, with trade-offs among the various provisions, other than the privacy-related provisions that are the focus of this article. And with respect to TPP, I only consider Canada and he U.S., without asking if the U.S. included certain provisions to try to change domestic policy in the ten other parties, or if those others influenced an outcome that was obviously acceptable to the U.S. and Canada.

The comparison of CETA and TPP is sketched in Box 1, where the topics of each article are grouped according to whether the language is aspirational or obligatory.[8] In a now classic analytic framework for RTAs, the covered subjects are divided into 'WTO-plus' (WTO+), corresponding to topics where bilateral commitments go beyond multilateral obligations; and 'WTO-extra' (WTO-X) where the topics are not currently covered by WTO disciplines (Horn, Mavroidis and Sapir, 2010, 1567). While a great many WTO-X provisions, the ones where they are trying to export their regulatory regimes, are included in EU and U.S. RTAs, few are enforceable. Enforceability here simply means whether the provision is drafted in terms of aspiration or obligation, hence whether it could be invoked before a regional or domestic court, not whether the institutional means of

[7] https://www.sonos.com/en-ca/legal/privacy?utm_source=owners&utm_medium=email&utm_content=learnbutton-EN-CA&utm_campaign=GDPR#faq last accessed April 24, 2018.

[8] For a detailed comparison of the provisions of CETA, TPP, and RCEP see (Ciuriak and Ptashkina, 2018, Annex 2). While my focus is Chapter 14 on e-commerce, a USTR information sheet identified 24 aspects of TPP spread across numerous chapters designed to promote the digital economy. https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2016/digital-2-dozen

enforcement envisaged by the agreement are either practical, or used (Horn, Mavroidis and Sapir, 2010, 1572).

Box 1 Texts of e-commerce chapters compared

This is a list of all the topics covered in the e-commerce chapters, with an [indication] of related topics in other chapters. The starred items (*) are relevant to privacy.

Legally enforceable (obligatory language)

CETA Chapter 16

Permanent prohibition on customs duties
[Transfer and processing of financial information 13.15]
*[Privacy of users of public telecommunications transport services 15.3.4]

TPP Chapter 14

Permanent prohibition on customs duties
Non-Discriminatory Treatment of Digital Products
Electronic Authentication and Electronic Signatures
*Cross-Border Transfer of Information by Electronic Means
*Location of Computing Facilities
Source Code

Best endeavours or too vague to be enforceable, or dialogue/cooperation

CETA Chapter 16

*Trust and confidence in electronic commerce
General Provisions
Electronic signatures
Liability of intermediary service suppliers;
Spam
Fraudulent and deceptive commercial practices

TPP Chapter 14

*Personal Information Protection
Domestic Electronic Transactions Framework
Online Consumer Protection
Paperless Trading
Principles on Access to Internet
Internet Interconnection Charge Sharing
Spam
Security in electronic communications
Authentication
*[Privacy of personal data of end-users of public telecommunications networks 13.4.4]

So what do we find? First, the definitions in TPP 14.1, the more recent agreement, cover more concepts than in CETA 16.1. Indeed TPP generally covers more issues, including in the Scope article (14.2), with more concrete language.

Second, both agreements say the objective is to promote the development of e-commerce for economic reasons (CETA 16.2; TPP 14.2), and both make permanent the WTO moratorium on customs duties, an easy and longstanding obligation. The chapters themselves are not otherwise about market access, though tradeoffs between the rules here and access in another chapter may not be incidental.

Third, negotiations on both agreements started well after the entry into force of the General Agreement on Trade in Services (GATS) in 1995, and the 1998 WTO ministerial Declaration on

Electronic Commerce (WTO, 1998). With the exception of a ban on customs duties, most e-commerce provisions in CETA and TPP are WTO-X. CETA confirms the applicability of WTO rules (16.2), and both agreements explicitly acknowledge the general exceptions and horizontal necessity test in GATS Article XIV.[9] This test does not prevent regulations that "are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services…" especially if they are necessary for "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."

Fourth, both agreements are a mix of aspirational and obligatory commitments, which may be just as well, because both have weak institutional provisions, as discussed below. How do I decide that some provisions are aspirational? Here is an example. TPP Article 14.5 requires parties to have a legal framework governing electronic transactions, without specifying its content, and they "shall endeavor" to ensure that it does not create an unnecessary regulatory burden.

Finally, the source of the e-commerce language in TPP is often other U.S. agreements (Alschner, Seiermann and Skougarevskiy, 2017), but Canada had more influence on the CETA chapter (Allee, Elsig and Lugg, 2017, 249 and Table 2), and Canada played the key role on privacy in TPP.

In the rest of this section I conduct a more detailed comparison of the privacy provisions, then data flow and data localization, and finally the institutional provisions.

Privacy protection

The key privacy provision in CETA is Article 16.4 on Trust and confidence in electronic commerce:

> Each Party should adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce and, when doing so, shall take into due consideration international standards of data protection of relevant international organizations of which both Parties are a member.

This commitment is not obligatory—it simply recognizes that the CETA parties have dealt with privacy in another forum through the adequacy finding (section 3 above). This text has a clear origin in Article 13.4 of Canada's RTA with Korea of 2015 (work started years earlier), and Article 1507 of its 2009 RTA with Peru.

In TPP Article 14.8.2 on Personal Information Protection provides that "each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce." This language came from past Canadian agreements, although the "should" in CETA 16.4 is replaced by "shall" in TPP. The key though is footnote 6 on this sentence, which reads

> For greater certainty, a Party may comply with the obligation in this paragraph by [A] adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, [B] sector-specific laws covering privacy, or [C] laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.

The language at [A] refers to PIPEDA; at [B] it takes account of the U.S. patchwork; and at [C] it covers the Privacy Shield approach. TPP accommodates the privacy regimes of Canada and the U.S. without requiring any domestic policy change.

TPP also provides in Article 14.8.4 that

> Each Party should publish information on the personal information protections it provides to users of electronic commerce, including how:

[9] TPP Article 29.1.3 explicitly makes GATS XIV part of Chapter 14; CETA Article 28.3 c) ii) does not mention GATS, but uses identical language.

(a) individuals can pursue remedies; and

(b) business can comply with any legal requirements.

Publication at home is a basic transparency norm, but as noted below TPP does not go to the next step of notification to trading partners. Clause (a) is consistent with the complaints-based enforcement system of the U.S. FTC—parties are only required to have reactive enforcement. The only cause for dispute under this chapter would be if a party has no privacy legislation, which might require change in the domestic policies of some CPTPP parties. Clause (b) is fundamental administrative law: economic actors need to know the rules with which they are expected to comply. This language was first used in Article 1504 of Canada-Peru. The rest of Article 14.8 is best endeavours, including 14.8.5 on the development of mechanisms to promote compatibility between the different regimes of the parties.

Finally, an important privacy-related provision is found in the telecommunications chapters of both agreements—parties "shall" (CETA 15.3.4) or "may" (TPP 13.4.4) take measures to ensure the privacy of users of public telecommunications services, subject to standard necessity test language on not being a disguised restriction on trade. The CETA language is consistent with the EU ePrivacy Directive (soon to be a Regulation), and PIPEDA.

Data localization and data flows

Two other issues in these agreements are related to privacy. An example illustrates the problem to be solved. Iceland is apparently emerging as a prime location for server farms (Gudjonsson, 2018). Why? Server farms are prodigious users of electricity and cooling, both of which the country has in abundance. Should other countries prevent their citizens' data from being held on servers in Iceland in the interest of protecting their privacy? Should governments restrict the cross-border flow of data to and from Iceland? And in either case would any restrictions be designed to protect jobs at home rather than privacy?

Who has physical control of the server is not the same as who has control of the data. In PIPEDA terms, a Canadian entity can be accountable for control of the data held on a server in Iceland. A different concern arises if a foreign government attempts to gain access to data for security reasons, and the controller of the data has no means to resist. The issue applies largely to the U.S., a government that tries to gain access wherever the server is located, although the EU is moving in that direction. Hence the more certainty of privacy or access is desired—e.g. for security reasons—the more physical location matters because the state has more confidence in its control of the controllers.

Neither of these issues were addressed in CETA—Canadian officials had only just begun to hear about them when the e-commerce chapter was completed in 2012. CETA has a weak provision in the financial services chapter: Article 13.15 requires a party to permit the transfer of information for data processing if required in the ordinary course of business, subject to the privacy framework of the originating country and to certain other limitations in Article 13.17. A separate EU initiative seeks to establish the same free movement for non-personal data as the GDPR does for personal data as a way to prevent requirements hampering data flows within the EU itself.

Americans believe that the choice of technology and server location should be dictated by business considerations and not rules on data storage. Hence their trade agreements have increasingly included rules to ensure that such domestic measures are not an unnecessary burden on trade. TPP therefore has two obligatory provisions, derived from past U.S. practice, requiring parties to allow cross-border transfer for the conduct of the business of a covered person and prohibiting a requirement to locate computing facilities in that Party's territory as a condition for conducting business in that territory (14.13). This language is harder than that found in the Korea-U.S. RTA (Burri, 2017, 433). Both articles recognize that parties may have regulatory requirements for security and privacy, and both say

that parties may maintain restrictions for legitimate public policy purposes, subject to a necessity test, although some observers worry that the exceptions language is too weak (Geist, 2018).

The TPP data flow and localization obligations do not apply to government data. The scope article specifies (14.2.3) that the e-commerce chapter shall not apply to government procurement, or information held or processed by or on behalf of a Party, and the government procurement chapter (Article 19.2.3) specifies that it does not apply to data held by a government. Canada's federal *Privacy Act* and the tough data rules in the provinces of British Columbia and Nova Scotia are not affected by TPP.

Financial services is a special case. The definitions in TPP 14.1 exclude a "financial institution" and a "cross-border financial service supplier of a Party" from the e-commerce chapter. The U.S. financial services industry was not happy with this carve out, which was included due to pressure from the U.S. Treasury (Dawson, 2018, 8). The industry is lobbying for a blanket ban on data localization in the renegotiation of NAFTA underway at the time of writing, but Canada and Mexico remain cautious. The three countries reached an accommodation in the TPP negotiations, and so far as we know, the TPP chapter is the basis for the NAFTA negotiations. I presume that Canada and Mexico would have no difficulty with the TPP language in Article 14.8.2, and that the Americans, Facebook's troubles notwithstanding, are unlikely to want to make footnote 6 in that article any harder.

Institutional weakness limits enforceability, and learning

A final basis for comparison is institutional. Once the parties have an agreement on paper, they have to bring it to life, which depends on effective institutional design. Reciprocal obligations, the basis of any trade agreement, depend on opportunities for the constant development and affirmation of shared understanding of what the obligations mean (Wolfe, 2015). Such opportunities require transparency; and accountability to partners. No much can be expected from the weak institutional provisions in both chapters.

First, both chapters are deficient in generating information, an essential step in learning. Many other CETA and TPP chapters indicate that compliance with the relevant WTO notification obligation would meet the requirements of the agreement. The absence of a notification requirement in the e-commerce chapters is telling. WTO Members have so far failed to agree on how the rules apply. In consequence, WTO has no explicit notification requirements for anything to do with e-commerce. Not that it would be easy to decide what should be notified—countries are still at an early stage in elaborating e-commerce disciplines. So in the case of the various exceptions clauses in TPP, parties are not required to notify the limitations they place on the location of computing facilities or restrictions they place on data flows. Nor are they required to explain implementation of their privacy rules in a way that could be discussed in a committee established under the agreement,

Second, the lack of notifications hardly matters because neither agreement creates a dedicated committee for e-commerce.[10] This omission is perhaps not surprising—only 16 RTAs establish specific institutional arrangements related to e-commerce (Monteiro and Teh, 2017). Both chapters have a large regulatory cooperation component, but such cooperation is hard to do without a means for the regulators to talk to each other.

Finally, the handful of articles cast in obligatory terms are potentially justiciable, though skepticism is warranted about whether the dispute settlement mechanisms in these two agreements will be used any more than the dispute settlement provisions in other RTAs (Wolfe, 2017).

[10] The CETA Parties might also make use of the Committee on Services and Investment—Article 26.2 mentions e-commerce.

Summing up the comparison

The e-commerce chapters of CETA and TPP address a regulatory cooperation problem, but the provisions on e-commerce are not mutual recognition agreements, and are not part of the regulatory cooperation process in CETA Chapter 21 or TPP Chapter 25. Regulatory equivalence as a concept in EU practice is similar, but in these chapters there is no joint determination of what standards should be, let alone any appeal to the standards of a multilateral regime. Both chapters have similarities to a Reference Paper on the model of the 1997 WTO agreement on trade in basic telecommunications services: both chapters with principles, not common regulations or harmonization, and neither deal with market access, which is covered in other chapters.

Interoperability of government measures, and accountability assigned to firms, represent an inherently decentralized approach, while being consistent with the post-war compromise of embedded liberalism (Ruggie, 1982)—do what you must to allow trade liberalization, while protecting national regulatory space. The principles cover issues that might be specific to digital trade. There are *commitments* that facilitate consumer trust by ensuring countries have measures in place to protect their information, and prevent fraudulent practices online. There is *cooperation* on things that are international in scope, like spam, where little can be done domestically when the unsolicited email is coming from abroad.[11]

On personal privacy, the expectation of both CETA and TPP is that parties will have a domestic regime. The EU requires proof that the regime is adequate, Canada holds firms accountable for following its rules wherever data is transferred, and the U.S. provides individuals a right to complain. Parties can claim an exemption if restrictions are necessary, but the default is no restriction on data flows and processing. Some critics think that the balance between privacy and data flow falls in the wrong place (Greenleaf, 2016a, 3, 6). The EU says personal data may be transferred only to countries with an "adequate level of protection" of privacy. The U.S. thinks barriers to the flow of data harm legitimate business interests involved in cross-border trade, and hence are a camouflage for protectionism. Canada and Europe have horizontal privacy law, but Americans have vertical and sectoral privacy law, so Americans cannot agree to horizontal obligations.

It seems evident that the U.S. tried to use TPP to externalize its regulatory preferences for data flows and data localization, and the U.S. is still trying in the renegotiation of NAFTA to get its partners to agree to limits on intermediary liability for internet service providers. CETA called for dialogue on this issue, but TPP was silent. Canada and Mexico are resisting this attempt by the U.S. to embed its regulatory preferences in a trade agreement, not least because the circumstances that led to the passage of section 230 of the U.S. *Communications Decency Act* (Lomonte, 2018) rarely arise in Canada or Mexico.

My story confirms but does not develop work that analyzes the limits on the so-called "Brussels effect". Some scholars argue, using the example of digital trade among others, that the EU does not export its regulations through preferential trade agreements (Young, 2015). I think this claim is only true in the sense that the EU will not make commitments on the GDPR in a trade agreement. The CETA reference to privacy is framed in Canadian language, but the EU is a huge market, and Canada has clearly changed its policy to maintain its adequacy finding. EU rules on privacy create a first-mover advantage in the absence of comprehensive rules in the U.S. (Newman and Posner, 2015, 1323), but a unilateral rule is not the basis for a stable regime.

[11] Spam is covered by the ePrivacy Directive (Voss, 2017) and by Canada's Anti-Spam Legislation (https://crtc.gc.ca/eng/internet/anti.htm) but it seems only best endeavours language was wanted in CETA.

5. Seeking generalization

In lieu of a conclusion, in this section I seek to generalize from this comparison. The first question is, why do negotiators bother with vague provisions that are not enforceable? The brief answer is, because they are learning, and because reducing uncertainty does not require creating certainty.

Part of the process of learning is labeling—if you name something, it becomes more tractable for disciplines. Then you see that some aspects of the new area are affecting transaction flows in ways that are susceptible to analysis using trade concepts. Part of the process of learning is labeling—if you name something, it becomes more tractable for disciplines. Then you see that some aspects of the new area are affecting transaction flows in ways that are susceptible to analysis using trade concepts.

Countries arguably began learning about e-commerce in the 1970s beginning with the OECD work on what were then called transborder data flows, the precursor to discussions about "trade in services" (Drake and Nicolaïdis, 1992). The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980 inspired a number of national laws as well as the EU Data Protection Directive of 1995.[12] The EU Directive was also inspired by the 1981 Council of Europe Convention 108. The issue is still discussed at the OECD, for example in its evolving privacy guidelines (OECD, 2017).[13] Those Guidelines are designed to minimize restrictions, as does the APEC Privacy Framework, first elaborated in 2004, by making the data controller accountable regardless of where the data is located (Yakovleva, forthcoming, 8-9).

This work in international organizations notwithstanding, a multilateral regime has not yet emerged. There is no shared definition either of e-commerce, or of digital trade, as we see in RTA chapters (Monteiro and Teh, 2017, 17). The blurring of the terms is seen in TPP, where Article 14.2.2 provides that the e-commerce chapter "shall apply to measures adopted or maintained by a Party that affect trade by electronic means." WTO is blocked both by the transatlantic divide and by developing country nervousness, so RTAs are being used for learning. Or at least the negotiation process is a form of learning. The institutional weakness described above is compounded by the lack of a Secretariat that could draw on notifications and work in other international organizations to provide background papers for discussion. Perhaps the parties did not want to use a trade agreement in this way—TPP Article 14.15 provides that the Parties should "endeavor" to cooperate, without saying how. CETA article 16.6 calls for dialogue without being explicit about where. Creating a place to talk about e-commerce, a vital form of learning, should be part of the preparatory process now underway in the WTO (WTO, 2017).

I find it significant that neither the CETA not the TPP language is found in the new EU deal with Mexico announced in April 2018. The chapter on digital trade effectively says nothing on privacy (in effect carved out under "right to regulate" in Article. 1.2), or data localization, and discussion of data flows here and in the financial services chapter are deferred for at least three years.[14] For now e-commerce as a trade issue is far from being sufficiently well understood for consistent codification to be possible. Put differently, the lack of shared understanding at multilateral level leads to experiments in RTAs; and there the lack of shared understanding of causal relations hence of what agreements should even cover leads to aspirational rather than obligatory language. Trade lawyers may wonder why negotiators bother with the softer commitments, but informal law is valuable (Shaffer, Wolfe and Le, 2015) and trade agreements are necessarily incomplete, relational contracts. What matters is the effort to understand a new area and to express that understanding in language.

---

[12] For a concise history of the rapid evolution of privacy regimes, see (Stoddart, 2012).

[13] There was also a Ministerial Declaration on the Protection of Privacy on Global Networks (1998), now abrogated, and a Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007).

[14] http://trade.ec.europa.eu/doclib/docs/2018/april/tradoc_156811.pdf last accessed April 27, last accessed April 27, 2018.

What do trade people need to learn about privacy?

How should trade negotiators think about privacy? They are familiar with privacy for producers, which is customarily waived in trade in goods. For example, trade agreements ensure that consumers are able to hold producers liable for products that are in some way unsafe. Digital trade requires a similar relationship. The GDPR, for example, in effect creates new liabilities for producers, and limits their privacy. That is, in order to protect the privacy of the consumer, the data controller will have to have less privacy about its own actions. We observe that that countries do not use trade agreements to regulate privacy while trying to ensure that domestic privacy rules do not unduly interfere with trade. What trade analysts do not know is what the optimal trade rules should be in this rapidly changing area. For example, under what circumstances is it worth worrying about "disguised protection"?

Goldfarb and Trefler offer a novel argument looking at digital trade from the standpoint of Artificial Intelligence (AI), not e-commerce. Variation in regulations that affect access to data could help domestic AI firms and/or hurt foreign firms, especially if the regulations affect the ability of firms in small countries, like Canada, to access the huge amounts of data they need to build their predictive models, in comparison to firms in larger markets. In the case of the privacy of individuals, regulation involves policies on the collection and use of data, which can either limit or expand the ability of firms to use AI effectively. Goldfarb and Trefler say that "lax privacy policies may help domestic industry relative to countries with strict policies just as lax labor and environmental regulation may help the domestic industry." AI firms could be expected to move to the country with access to the most data and the least restrictions on its use. One might then expect that trade negotiations would try to prevent such a race to the bottom, by insisting on similar privacy laws in each partner (Goldfarb and Trefler, 2018, 20-2).

While that is not what we observe in the approach to privacy in CETA and TPP, which are permissive of variation in domestic privacy law, we also do not observe a necessity test applied to the privacy provisions, perhaps because the possibility of disguised protection in the case of strong privacy standards is not serious, since such rules do not help domestic firms at the expense of foreign firms.[15] As a consumer I cannot tell how well any firm will protect my information. If I start worrying about use of personal information, I may be inclined to use fewer services that ask for it. If in contrast I feel confident that government is ensuring strict protection, I will be more inclined to use more services and provide more information (Heidhues, Johnen and Koszegi, 2018). Hence trade agreements that promote strong privacy regulation might thereby promote more cross-border trade, rather than less.

In contrast, rules that limit data flows or require data to be kept at home might favour home firms. That is, we might expect privacy to be something a country ought to have, but transfer and localization, Goldfarb and Trefler suggest, could be expected to be characterized as trade restrictive and potentially as disguised protection. Hence we might expect such rules to be subject to a necessity test, a requirement that such restrictions be necessary for the achievement of a legitimate policy objective (Lim and De Meester, 2014, 348; Muller, 2015; Yakovleva, forthcoming, 21). And that is what we find: the "disguised restriction" language is explicit in the TPP articles on cross-border transfer (14.11) and data localization (14.13).

Finally, a standard reason for trade agreements is dealing with a market failure. What Hoekman and Mattoo call regulatory heterogeneity can be seen as a market failure when requirements in this domain vary across countries because of differences in institutions, and when regulators in the jurisdiction of the exporter do not adequately take into account consequences for consumers in the jurisdiction of the importer (Hoekman and Mattoo, 2017). The challenge is compounded because a

[15] Reviewing the work of other scholars, Greenleaf wonders if an adequacy decision could be challenged under GATS Article XIV, perhaps as discriminatory, or as an unjustifiable restriction (Greenleaf, 2016a, 4). Such a challenge seems unlikely.

change in domestic policy made for one partner is made for all—it is hard to design preferential privacy rules, ones that respect each country's domestic law. One solution suggested by Hoekman and Mattoo could be destination-based regulatory commitments by exporters to protect foreign consumer interests in return for market access commitments by importers. That is in effect what we see with the Privacy Shield, which requires U.S. regulators to discipline American digital exporters on behalf of European consumers, who are otherwise not the concern of U.S. regulators, in order to maintain market access. But no multilateral agreement is yet able to express such an approach in precise rules, and so there is no constraint on the inherent unilateralism of the EU approach to reaching an adequacy decision. Trade agreements may not be the best way to encourage agency to agency discussion among privacy regulators on how best to reconcile their domestic obligations with the free flow of data. In the absence of other consultative mechanisms, however, trade negotiators will keep learning through experimentation in RTAs.

References

Aaronson, Susan Ariel and Patrick Leblond, (forthcoming) 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO,' Journal of International Economic Law

Allee, Todd, Manfred Elsig and Andrew Lugg, (2017) 'Is the European Union Trade Deal with Canada New or Recycled? A Text-as-Data Approach,' Global Policy 8:2 246-52.

Alschner, Wolfgang, Julia Seiermann and Dmitriy Skougarevskiy, (2017) 'Text-as-Data Analysis of Preferential Trade Agreements: Mapping the PTA Landscape ' Ottawa Faculty of Law, Working Paper No. 2017-32, July 10, 2017.

Berka, Walter, (2017) 'CETA, TTIP, Tisa, and Data Protection,' in Griller, Stefan, Walter Obwexer and Erich Vranes, eds, Mega-Regional Trade Agreements: CETA, TTIP, and Tisa: New Orientations for EU External Economic Relations (Oxford: Oxford University Press),

Branstetter, Lee, (2016) 'TPP and Digital Trade,' in Schott, Jeffrey J. and Cathleen Cimino-Isaacs, eds, Assessing the Trans-Pacific Partnership, Volume 2: Innovations in Trading Rules (Washington: Peterson Institute for International Economics), 72-81.

Burri, Mira, (2017) 'The Regulation of Data Flows through Trade Agreements,' Georgetown Journal of International Law 48:2 (2017 Winter), 407-48.

Canada, (2009) 'Guidelines for Processing Personal Data across Borders,' Office of the Privacy Commissioner of Canada, January 2009, https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/ accessed April 1, 2018,

Canada, (2018a) 'E-Commerce: Certain Trade-Related Priorities of Canada's Firms—Report of the Standing Committee on International Trade,' House of Commons April 2018.

Canada, (2018b) 'Towards Privacy by Design: Review of the Personal Information Protection and Electronic Documents Act—Report of the Standing Committee on Access to Information, Privacy and Ethics,' House of Commons February 2018.

Chaisse, Julien and Mitsuo Matsushita, (2018) 'China's 'Belt and Road' Initiative: Mapping the World Trade Normative and Strategic Implications ' Journal of World Trade 52:1 (2018), 163-85.

Ciuriak, Dan and Maria Ptashkina, (2018) 'The Digital Transformation and the Transformation of International Trade,' RTA Exchange. International Centre for Trade and Sustainable Development and the Inter-American Development Bank, January 2018.

Dawson, Laura, (2018) 'Global Rules of Digital Trade: Can We Adapt Bordered Regulation for a Borderless World?,' Canadian Global Affairs Institute, February 2018.

Drake, William J. and Kalypso Nicolaïdis, (1992) 'Ideas, Interests, and Institutionalization: "Trade in Services" and the Uruguay Round,' International Organization 46:1 (Winter 1992), 37-100.

EU, (2017a) 'Exchanging and Protecting Personal Data in a Globalised World: Communication from the Commission to the European Parliament and the Council,' European Commission, COM(2017) 7, January 10, 2017.

EU, (2017b) 'A Connected Digital Single Market for All, Communication from the Commission on the Mid-Term Review on the Implementation of the Digital Single Market Strategy,' European Commission, COM/2017/228 final, 10.5.2017.

EU, (2018) 'European Commission Endorses Provisions for Data Flows and Data Protection in EU Trade Agreements,' European Commission, Daily News, http://europa.eu/rapid/press-release_MEX-18-546_en.htm, January 31, 2018.

Ferracane, Martina F., (2017) 'Restrictions on Cross-Border Data Flows: A Taxonomy,' European Centre for International Political Economy, ECIPE Working Paper No. 1/2017, 2017.

Ferracane, Martina Francesca, Hosuk Lee-Makiyama and Erik Van Der Marel, (2018) 'Digital Trade Restrictiveness Index,' European Center for International Political Economy, April 2018.

Gao, Henry, (2018) 'Regulation of Digital Trade in US Free Trade Agreements: From Trade Regulation to Digital Regulation,' Legal Issues of Economic Integration 47-70.

Geist, Michael, (2018) 'Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards,' Centre for International Governance Innovation, April 4, 2018.

Goldfarb, Avi and Daniel Trefler, (2018) 'Ai and International Trade,' National Bureau of Economic Research, Working Paper Series No. 24254, January 208.

Greenleaf, Graham, (2016a) 'Free Trade Agreements and Data Privacy: Future Perils of Faustian Bargains,' UNSW Law Research Paper, No. 2016-08, 30 November 2016.

Greenleaf, Graham, (2016b) 'International Data Privacy Agreements after the GDPR and Schrems,' Privacy Laws & Business International Report 139: (30 January 2016), 12-5.

Greenleaf, Graham, (2017a) 'Renewing Convention 108: The Coe's 'GDPR Lite' Initiatives,' Privacy Laws & Business International Report 142: (2017), 14-7.

Greenleaf, Graham, (2017b) ''European' Data Privacy Standards Implemented in Laws Outside Europe,' Privacy Laws & Business International Report 149: (September 3, 2017), 21-3.

Gudjonsson, Heidar, (2018) 'The Arctic, Where Cold Storage Comes Cheap for the Digital Age,' Financial Times (March 22, 2018),

Heidhues, Paul, Johannes Johnen and Botond Koszegi, (2018) 'Browsing Versus Studying: A Pro-Market Case for Regulation————————————,' unpublished ms, January 27, 2018.

Hoekman, Bernard and Aaditya Mattoo, (2017) 'Altered States: Populism and the Changing Political Economy of Trade Policy and Negotiations,' EUI and World Bank, September 2017.

Horn, Henrik, Petros C. Mavroidis and André Sapir, (2010) 'Beyond the WTO? An Anatomy of EU and US Preferential Trade Agreements,' The World Economy 33:11 (2010), 1565-88.

Hyman, David A. and William E. Kovacic, (2018) 'Implementing Privacy Policy: Who Should Do What?,' SSRN, February 2018.

Krotoszynski, Ronald J., (2016) 'Canada: Privacy in Canada: Taming a Notoriously Protean Legal Concept with a Coherent and Purposive Approach,' Privacy Revisited (New York: Oxford University Press),

Lim, Aik Hoe and Bart De Meester, (2014) 'Addressing the Domestic Regulation and Services Trade Interface: Reflections on the Way Ahead,' in Lim, Aik Hoe and Bart De Meester, eds, WTO Domestic Regulation and Services: Trade Putting Principles into Practice (Cambridge: Cambridge University Press), 332-51.

Lomonte, Frank, (2018) 'The Law That Made Facebook What It Is Today,' The Conversation (April 11, 2018),

Macdonald, Roderick A. and Robert Wolfe, (2009) 'Canada's Third National Policy: The Epiphenomenal or the Real Constitution?,' University of Toronto Law Journal 49:4 (October 2009), 469-523.

Manyika, James, Susan Lund, Jacques Bughin et al., (2016) 'Digital Globalization: The New Era of Global Flows,' McKinsey Global Institute, March 2016.

Mishra, Neha, (2017) 'The Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance?,' Journal of International Economic Law 20:1 (Mar 2017

2017-05-08), 31.

Monteiro, José-Antonio and Robert Teh, (2017) 'Provisions on Electronic Commerce in Regional Trade Agreements,' World Trade Organization, WTO Working Paper ERSD-2017-11, July 2017.

Muller, Gilles, (2015) 'The Necessity Test and Trade in Services: Unfinished Business?,' Journal of World Trade 49:6 (0), 951.

Newman, Abraham L. and Elliot Posner, (2015) 'Putting the EU in Its Place: Policy Strategies and the Global Regulatory Context,' Journal of European Public Policy 22:9 (2015), 1316-35.

O'connor, Nuala, (2018) 'Reforming the U.S. Approach to Data Protection and Privacy,' Council on Foreign Relations, Report January 30, 2018.

OECD, (2017) OECD Digital Economy Outlook 2017 (Paris: OECD Publishing).

Power, E. Michael, (2017) The Law of Privacy Second edition. (Toronto: LexisNexis).

Ruggie, J. G., (1982) 'International Regimes, Transactions, and Change - Embedded Liberalism in the Post-War Economic Order,' International Organization 36:2 (1982), 379-415.

Ruggie, John Gerard, (1993) 'Territoriality and Beyond: Problematizing Modernity in International Relations,' International Organization 47:1 (Winter 1993), 139-74.

Santana, Roy, (in press) 'Cross-Fertilization of International Trade Law: How Chapter 2 of the TPP Was Influenced by the WTO and Prior US Trade Deals ' in Gantz, David A. and Jorge Huerta Goldman, eds, The Trans Pacific Partnership Agreement: Its Substance and Impact on International Trade, NAFTA, and Other FTAs (Cambridge: Cambridge University Press),

Scott, Mark, (2018) 'Zuckerberg: Facebook Will Apply EU Data Privacy Standards Globally,' Politico (April 5, 2018),

Shaffer, Gregory, Robert Wolfe and Vinhcent Le, (2015) 'Can Informal Law Discipline Subsidies?,' Journal of International Economic Law 18:4 (December 2015), 711-41.

Soma and Stephen D. Rynerson, (2008) Privacy Law in a Nutshell (St. Paul, MN: Thomson/West).

Stoddart, Jennifer, (2012) 'International Privacy Standards: Development, Recent Events and Limitations,' Privacy Commissioner of Canada, Remarks at the 43rd Annual Study Session of the International Institute of Human Rights, https://www.priv.gc.ca/en/opc-news/speeches/2012/sp-d_20120709/ July 9, 2012.

Voss, W. Gregory, (2017) 'First the GDPR, Now the Proposed Eprivacy Regulation,' Journal of Internat Law (July 2017),

Watanabe, Paul J., (2017) 'An Ocean Apart: The Transatlantic Data Privacy Divide and the Right to Erasure,' Southern California Law Review 90:5 (July, 2017),

Wolfe, Robert, (2015) 'An Anatomy of Accountability at the WTO,' Global Policy 6:1 (2015), 13-23.

Wolfe, Robert, (2017) 'Canadian Trade Policy in a G-Zero World: Preferential Negotiations as a Natural Experiment,' in Assche, Ari Van, Stephen Tapp and Robert Wolfe, eds, Redesigning Canadian Trade Policies for New Global Realities (Montreal: Institute for Research on Public Policy), 323-63.

WTO, (1998) 'Declaration on Global Electronic Commerce, Adopted on 20 May 1998,' World Trade Organization, Ministerial Conference, Second Session, WT/MIN(98)/DEC/2, 25 May 1998.

WTO, (2017) 'Joint Statement on Electronic Commerce,' World Trade Organization, Ministerial Conference, Eleventh Session, WT/MIN(17)/60, 13 December 2017.

Yakovleva, Svetlana, (forthcoming) 'Should Fundamental Rights to Privacy and Data Protection Be a Part of the EU's International Trade "Deals"?,' World Trade Review

Young, Alasdair R., (2015) 'Liberalizing Trade, Not Exporting Rules: The Limits to Regulatory Co-Ordination in the EU' 'New Generation' Preferential Trade Agreements,' Journal of European Public Policy 22:9 (2015), 1253-75.

Author contacts:

Robert Wolfe

Professor Emeritus

School of Policy Studies

Queen's University

Kingston, Canada

K7L 3N6

Email: robert.wolfe@queensu.ca

Twitter @BobWolfeSPS