7

Digital Trade

New Design Elements in Preferential Trade Agreements

*Mira Burri**

7.1 INTRODUCTION

'Digital trade'[1] can be said to be a relatively well-established topic in international economic rulemaking, if one considers that soon after the completion of the Uruguay Round, the Information Technology Agreement (ITA) (WTO 1996)[2] as a plurilateral arrangement aiming at zero tariffs for information technology (IT) products was adopted in 1996 and two years later the membership of the World Trade Organization (WTO) launched the Work Programme on Electronic Commerce (WTO 1998). The latter initiative sought to address the implications of the Internet that could potentially lead to adjustments in the existing rules for trade in goods, trade in services, and intellectual property (IP) rights protection. Interestingly, for those wishing to understand the broader context of emerging Internet governance, this was also the time when John Perry Barlow penned his declaration on the independence of cyberspace, claiming, in essence, that neither states nor companies will be able to control this new space of freedom (Barlow 1996). Since then, the perception that states should and can regulate online activities became a reality, and a flurry of regulations were adopted around the

* The support of the European Research Council under Consolidator Grant 101003216 is gratefully acknowledged.

[1] The Organisation for Economic Co-operation and Development (OECD) has pointed out that, while there is no single recognised and accepted definition of digital trade, there is a growing consensus that it encompasses digitally enabled transactions of trade in goods and services that can either be digitally or physically delivered and that involve consumers, firms, and governments. Critical is that the movement of data underpins contemporary digital trade and can also itself be traded as an asset and a means through which global value chains (GVCs) are organised and services delivered (López González and Jouanjean 2017; López-González et al. 2022).

[2] On the negotiating history of the ITA, see Fliess and Sauvé (1998). On the relevance of the ITA in regulatory landscape of digital trade, see Burri (2015).

world that targeted commercial transactions, personal data protection, online gambling, and other types of illegal activity online.[3] The WTO Work Programme on Electronic Commerce could not keep up with these developments and stalled for a variety of reasons, ultimately rendering WTO law dated in many aspects (Wunsch-Vincent and Hold 2012).

In the meantime, digital trade as practice and as a subject of regulation did substantially transform. On the one hand, this has been spurred by the progressively advancing digitisation of economies and societies as a whole with a number of palpable new trends in trade, such as the emergence of global value chains (GVCs) and increased servicification (Burri 2019; WTO 2019c), as well as by the more recently emerged critical importance of data (Manyika et al. 2011; Mayer-Schönberger and Cukier 2013; Henke et al. 2016; WTO 2018). On the other hand, the surge in digital trade rulemaking, which in this chapter covers both hard and soft rules creation (Abbott and Snidal 2000: 421–456; Shaffer and Pollack 2010), can be linked to the multiple new issues that the data-driven economy has raised. Some of them, such as those in the area of personal data protection, demand urgent regulatory responses (Burri 2021a; Chander and Schwartz 2023).

The chapter is set against this background and seeks to provide a better understanding and contextualisation of the highly dynamic field of digital trade rulemaking driven by preferential trade agreements (PTAs). The new rules found in bilateral and regional PTAs not only compensate for the lack of developments in the multilateral forum of the WTO (at least so far)[4] but effectively create a comprehensive, albeit fragmented, governance framework for the data-driven economy. The chapter's analytical lens is directed in particular towards the more recent and advanced models of digital trade rulemaking, such as those under the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the United States (US)–Mexico–Canada Agreement (USMCA), as well as those endorsed by dedicated digital economy agreements (DEAs). The chapter then covers the European Union's (EU) new generation of trade deals, particularly the post-Brexit Agreement with the United Kingdom (UK), the agreement with New Zealand, and the currently negotiated deals with Australia and Tunisia. It looks at the Regional Comprehensive Economic Partnership (RCEP), as the first agreement with digital trade provisions that includes China, to give a sense of the dynamic governance environment on digital trade issues.

With the help of these enquiries, it is the chapter's objective to identify new design elements found in PTAs and to trace how these have diffused, especially in recent years, and to what extent one can observe convergence or divergence across regulatory templates and issues in the digital trade domain.

[3] For a great review of the theories on cyberspace regulation, their evolution over time, and review of the literature, see Eichensehr (2015: 313–334).

[4] For an analysis of the WTO relevance to digital trade, see Burri and Cottier (2012); Burri (2015).

7.2 THE PTA LANDSCAPE OF DIGITAL TRADE RULEMAKING

7.2.1 *Overview*

As earlier noted, since the WTO law did not undergo any adaptation in the past two decades, the regulatory environment for digital trade has been shaped exclusively by developments in PTAs. Out of the 432 PTAs entered into between 2000 and 2023, 214 contain provisions relevant to digital trade and 122 have dedicated electronic commerce chapters.[5] While it is true that the pertinent rules are very heterogeneous and differ as to issues covered, the scope and level of commitments, and their binding nature, it is apparent that the trend towards more detailed provisions on digital trade has intensified significantly over the years.[6] This regulatory push in the digital trade domain can be explained by the increased importance of the issue over the years, as noted earlier, and the role played by the US as a legal entrepreneur (Elsig and Klotz 2021).

The US has, over the years, endorsed its 'Digital Agenda' (US Congress 2001; Wunsch-Vincent 2003; Gao 2018) through the PTA channel. The agreements reached since 2002 with Australia, Bahrain, Chile, Morocco, Oman, Peru, Singapore, the Central American countries,[7] Panama, Colombia, and South Korea all contain important, albeit with different depths of commitment, provisions in the broader field of digital trade. However, it should be highlighted that the US is not a sole actor any longer, as the dynamic of digital trade rulemaking has changed over time. On the one hand, it is noteworthy that the US template is not limited to US agreements (Elsig and Klotz 2021) and has been replicated in a number of other PTAs as well, such as Singapore–Australia, Thailand–Australia, New Zealand–Singapore, Japan–Singapore, and South Korea–Singapore. On the other hand, it ought to be pointed out that smaller countries, in particular Singapore and New Zealand, have become the most innovative and bold rule-makers in the area of digital trade (Burri, Vasquez Callo-Müller and Kugler 2024). Although reckoned as a major actor in international economic law and policy, the EU has been, in comparison, a latecomer into the digital trade rulemaking domain, as the chapter reveals below.

The relevant aspects of digital trade governance can be found in: (1) the specifically dedicated electronic commerce PTA chapters; (2) the chapters on cross-border supply of services (with particular relevance of the telecommunications, computer

[5] This analysis is based on a data set of all digital trade relevant norms in trade agreements (Trade Agreement Provisions on Electronic-commerce and Data, TAPED) (Burri and Polanco 2020; Burri, Vasquez Callo-Müller and Kugler 2024). For all data, as well as updates of the data set, see https://unilu.ch/taped.

[6] For an overview of the PTA developments, see Burri (2021b).

[7] Costa Rica, the Dominican Republic, El Salvador, Guatemala, Honduras, and Nicaragua as part of the Dominican Republic–Central America Free Trade Agreement (CAFTA-DR).

and related, audiovisual, and financial service sectors); and (3) the IP chapters.[8] This chapter focuses exclusively on the electronic commerce/digital trade chapters, as well as on the specific DEAs, which have become the critical source of new rulemaking in the area of digital trade and are also indicative of the novel legal design.

The electronic commerce/digital trade chapters play a dual role in terms of rule creation. For one, they represent an attempt to compensate for the lack of progress in the WTO and address many of the questions of the WTO Work Programme on Electronic Commerce that have been discussed but not resolved (Wunsch-Vincent 2006). For instance, a majority of the chapters recognise the applicability of WTO rules to electronic commerce (e.g. US–Singapore FTA, Article 14.1; US–Australia FTA, Article 16.1) and establish an express and permanent duty-free moratorium on electronic transmissions (e.g. US–Singapore FTA, Article 14.3, paragraph 1; US–Chile FTA, Article 15.3).[9] In most of the templates tailored along the US model, the chapters also include a definition of 'digital products', which treats products delivered offline as equally as those delivered online (e.g. US–Singapore FTA, Article 14.3; US–Australia FTA, Article 16.4), so that technological neutrality is ensured and some of the classification dilemmas under the General Agreement on Trade in Services (GATS) are cast aside (in particular when combined with negative committing for services).[10] In this context, one can observe some new design elements that essentially connect the multilateral discussions on e-commerce with actual rulemaking in the preferential forums. The level of legal certainty is increased for PTA partners even on some 'older' issues, such as the moratorium on customs duties on electronic transmissions, normally extended at the WTO Ministerial Conferences (MC), but the acceptance of which may be waning among WTO Members.[11]

The electronic commerce/digital trade chapters also include novel regulatory questions that have not been treated in the WTO context – the so-called 'WTO-extra' issues that have become increasingly important in the data-driven economy. One can group these rules into two categories: (1) rules that seek to facilitate digital trade, by tackling distinct issues, such as paperless trading, electronic contracts, and electronic authentication, as well as by increasing business and consumer trust; and (2) rules that address data governance, in particular cross-border data flows, and new data economy issues that can be of various natures. It should be noted that as to the

[8] For analysis of all relevant chapters, see Burri (2017).

[9] For a discussion of the variety of rules on the moratorium, see Burri and Polanco (2020).

[10] The negative committing is different from the conventional opt-in committing for service sectors under the GATS and covers all sectors except for those explicitly excluded (Horn et al. 2009; Adlung and Mamdouh 2013; Burri 2017).

[11] As the MC12 and MC13 proved. During these latest WTO Ministerial Conferences the scope and application of the moratorium were heavily contested, with, in particular, India and South Africa arguing against its extension (WTO 2021).

first cluster of issues on the facilitation of digital trade, the number of PTAs containing such rules is often substantial,[12] and one can observe some convergence regarding treaty language. Only a few agreements still include rules on data, and the data flow conditionalities may differ substantially.[13]

7.2.2 *Emerging Templates for Digital Trade and Stakeholders' Positioning*

In the following sections, the chapter looks at the new rules created in recent agreements through a detailed analysis of the most advanced electronic commerce/digital trade chapters thus far – those of the CPTPP, the USMCA, and the dedicated DEAs. We complement this analysis with an enquiry into the EU treaties, the EU's repositioning on data flows in particular, and into the RCEP as the first agreement with digital trade provisions to include China. The purpose is twofold: on the one hand, to highlight legal innovation in these treaties and, on the other, to give a sense of the positions of the major stakeholders.

7.2.2.1 The CPTPP

The Comprehensive and Progressive Agreement for Trans-Pacific Partnership was agreed upon in 2017 between eleven countries in the Pacific Rim[14] and entered into force on 30 December 2018. Beyond the economic significance of the agreement (Torrey 2018) and the new approach of a 'mega-regional' PTA (Kingsbury et al. 2019a, 2019b), the CPTPP chapter on electronic commerce created at that time the most comprehensive template in the landscape of PTAs. Despite the US having dropped out from the Trans-Pacific Partnership Agreement (TPP) with the start of the Trump Administration, the CPTPP chapter reflects the US efforts under its updated 'Digital 2 Dozen' agenda[15] to secure obligations on digital trade[16] and is a verbatim reiteration of the TPP chapter. A closer look at the CPTPP electronic commerce chapter is, therefore, well-deserved.

In the first part, and not unusually for US-led and other PTAs, the CPTPP electronic commerce chapter clarifies that it applies 'to measures adopted or maintained by a party that affect trade by electronic means' (Article 14.2(2) CPTPP). But it excludes from this broad scope (1) government procurement and (2) information held or processed by or on behalf of a party, or measures related to such information,

[12] So, for instance, 100 PTAs have rules on e-signatures; ninety-four PTAs have rules on paperless trading; and eighty-five PTAs contain a provision on electronic transactions frameworks.

[13] Forty-nine PTAs have rules on data flows; thirty-two PTAs have a ban on data localisation.

[14] Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Viet Nam.

[15] The 'Digital 2 Dozen' agenda sought to promote the digital economy through a free and open Internet and commerce without borders and defined twenty-four objectives, including free data flows, to this effect see https://ustr.gov/sites/default/files/Digital-2-Dozen-Final.pdf.

[16] See also in this sense New Zealand's Waitangi Tribunal (2021: 72 and passim).

including measures related to its collection (Article 14.2(3) CPTPP).[17] The following provisions address, again as customarily, some of the leftovers of the WTO Work Programme on Electronic Commerce and provide for the facilitation of online commerce. In this sense, Article 14.3 CPTPP bans the imposition of customs duties on electronic transmissions, including content transmitted electronically, and Article 14.4 endorses the non-discriminatory treatment of digital products,[18] which are defined broadly pursuant to Article 14.1 CPTPP.

With regard to digital trade facilitation, a number of provisions should be mentioned: Article 14.5 CPTPP is meant to shape the domestic electronic transactions framework by including binding obligations for the parties to follow the principles of the UNCITRAL Model Law on Electronic Commerce 1996 or the UN Convention on the Use of Electronic Communications in International Contracts. Parties must endeavour to (1) avoid any unnecessary regulatory burden on electronic transactions and (2) facilitate input by interested persons in the development of its legal framework for electronic transactions (Article 14.5(2) CPTPP). The provisions on paperless trading (Article 14.9 CPTPP) and electronic authentication and electronic signatures (Article 14.6 CPTPP) complement this by securing the equivalence of electronic and physical forms.

The remainder of the provisions found in the CPTPP electronic commerce chapter can be said to belong to the second and more innovative category of rulemaking that tackles the emergent issues of the data-driven economy. Most importantly, in this context, the CPTPP seeks to curb data protectionism. First, it does so through an explicit ban on the use of data localisation measures. Article 14.13 (2) prohibits the parties from requiring a 'covered person to use or locate computing facilities in that party's territory as a condition for conducting business in that territory'. Second, the CPTPP includes a hard rule on data flows: '[e]ach 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' (Article 14.11(2) CPTPP). The rule has a broad scope and most data transferred over the Internet is likely to be covered.

Measures restricting digital flows or implementing localisation requirements are permitted only if they do not amount to 'arbitrary or unjustifiable discrimination or a disguised restriction on trade' and do not 'impose restrictions on transfers of information greater than are required to achieve the objective' (Article 14.11(3) CPTPP). These non-discriminatory conditions are similar to the strict test formulated by

[17] For greater certainty, measures affecting the supply of a service delivered or performed electronically are subject to the obligations contained in the relevant provisions on investment and services (Article 14.2(4) CPTPP) and some additional exceptions are also specified (Article 14.2(5) and (6) CPTPP).

[18] The obligation does not apply to subsidies or grants, including government-supported loans, guarantees, and insurance, nor to broadcasting. It can also be limited through the rights and obligations specified in the IP chapter. Article 14.2(3) CPTPP.

Article XIV GATS and Article XX General Agreement on Tariffs and Trade (GATT) 1994 – a test that is intended to balance trade and non-trade interests by 'excusing' certain violations but that is also extremely hard to pass, as the WTO jurisprudence has thus far revealed (Andersen 2015). The CPTPP test differs from the WTO norms in two significant elements: (1) while there is a list of public policy objectives in the GATT 1994 and the GATS, the CPTPP provides no such enumeration and simply refers to a 'legitimate public policy objective' (Article 14.11(3) CPTPP); and (2) in the chapeau-like reiteration of 'arbitrary or unjustifiable discrimination', there is no GATT- or GATS-like qualification of 'between countries where like conditions prevail'. The scope of the exception is thus unclear – it can be linked to legal uncertainty, as well as to potentially unworkable safeguards for domestic constituencies.[19] Lastly, it should be noted that the ban on localisation measures is softened on financial services and institutions;[20] government procurement is also excluded (Article 14.8(3) CPTPP).

The CPTPP addresses other novel issues as well – one of them is source code. Pursuant to Article 14.17, a CPTPP Member may not 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. The prohibition applies only to mass-market software or products containing such software (Article 14.17(2) CPTPP), which means that tailor-made products, as well as the software used for critical infrastructure and in commercially negotiated contracts, are excluded (Article 14.17(2) CPTPP).[21] This ban on forced technological transfer aims to protect IT companies and address their concerns about loss of IP or cracks in the security of their proprietary code. It may also be seen as a reaction to China's demands to access source code from software producers selling in its market (Joint Statement on Trilateral Meeting of the Trade Ministers of the United States, Japan, and the European Union 2020).

These provisions illustrate an important development in the PTA rulemaking in that they do not merely seek the reduction in trade barriers but effectively shape the regulatory space domestically. Particularly critical in this context are also the rules in the area of data protection. Article 14.8(2) requires every CPTPP party to 'adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce'. Yet, there are no standards or benchmarks for the legal framework specified, except for a general requirement that CPTPP parties 'take into account principles or guidelines of relevant international bodies' (Article 14.8(2) CPTPP). A footnote provides some clarification in saying that: '. . . a Party may comply with the obligation in this paragraph by adopting or

[19] See, for example, in this sense New Zealand's Waitangi Tribunal (2021: 132–142). See also Burri and Kugler (2024).

[20] See the definition of 'a covered person' (Article 14.1 CPTPP), which excludes a 'financial institution' and a 'cross-border financial service supplier'.

[21] On the possible interpretations of the provision and difference to including algorithms, see New Zealand's Waitangi Tribunal (2021: 104–112).

maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy' (Article 14.8(2) CPTPP, at footnote 6). These norms can be interpreted as a prioritisation of trade over privacy rights. This has been pushed by the US during the TPP negotiations, as the US subscribes to a relatively weak and patchy protection of privacy (Whitman 2004; Schwartz and Solove 2014; Burri 2021a), which, among other things, means that the US has encountered difficulties in securing unhindered transatlantic data transfers (Burri 2021a; Chander and Schwartz 2023).

Next to the data protection provisions, the CPTPP also includes norms on consumer protection (Article 14.17 CPTPP), spam control (Article 14.14 CPTPP), and net neutrality (Article 14.10 CPTPP), as well as rules on cybersecurity cooperation (Article 14.16 CPTPP). The provisions are of soft law nature but are nonetheless important in trying to provide interoperability between domestic regimes and enhance business trust.

The accession of the UK to the CPTPP and recent requests for accession by China, Costa Rica, Taiwan and other countries (US Congressional Research Service 2021) will potentially expand this agreement's commercial reach and geopolitical dimension. Next to these possibilities for an enlarged CPTPP membership, it should also be pointed out that the CPTPP model has diffused in a substantial number of other agreements, such as the 2016 Chile–Uruguay FTA, the 2016 updated Singapore–Australia FTA (SAFTA), the 2017 Argentina–Chile FTA, the 2018 Singapore–Sri Lanka FTA, the 2018 Australia–Peru FTA, the 2019 Brazil–Chile FTA, the 2019 Australia–Indonesia FTA, the 2018 USMCA, the 2019 Japan–US Digital Trade Agreement (DTA), as well as a number of DEAs. The chapter discusses first the USMCA and then looks at selected DEAs.

7.2.2.2 The USMCA

After the US withdrew from the TPP, there was some uncertainty about the direction the US would take on matters of digital trade. The renegotiated North American Free Trade Agreement (NAFTA), now referred to as the 'USMCA', provides a useful confirmation of the US approach. The USMCA has a comprehensive 'Digital Trade' chapter that follows all critical lines of the CPTPP and creates an even more ambitious template. With regard to replicating the CPTPP model, the USMCA follows the same broad scope of application (Article 19.2 USMCA), bans customs duties on electronic transmissions (Article 19.3 USMCA), and binds the parties to non-discriminatory treatment of digital products (Article 19.4 USMCA). Furthermore, it provides for a domestic regulatory framework that facilitates online trade by enabling electronic contracts (Article 19.5 USMCA), electronic authentication and signatures (Article 19.6 USMCA), and paperless trading (Article 19.9 USMCA).

The USMCA replicates the CPTPP model also with regard to data issues and ensures the free flow of data through a clear ban on data localisation (Article 19.12 USMCA) and a hard rule on free information flows (Article 19.11 USMCA). Article 19.11 specifies further that parties can adopt or maintain a measure inconsistent with the free flow of data provision, if this is necessary to achieve a legitimate public policy objective, provided that there is no arbitrary or unjustifiable discrimination nor a disguised restriction on trade; and the restrictions on transfers of information are not greater than necessary to achieve the objective (Article 19.11(2) USMCA).[22]

Beyond these similarities, the USMCA introduces some novelties. The first is that the USMCA departs from the standard US approach and signals abiding by some data protection principles and guidelines of relevant international bodies. In this sense, Article 19.8 USMCA requires the parties to 'adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. 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, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)' (Article 19.8(2) USMCA). The parties also recognise key data protection principles, including: limitation on collection, choice, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation, and accountability (Article 19.8(3) USMCA), and aim to provide remedies for any violations (Article 19.8(4) and (5) USMCA). This is interesting because it may go beyond what the US has in its national laws on data protection (at least so far) (Chander and Schwartz 2023). Also it reflects some of the privacy protection principles the EU has advocated for, not only within the Union boundaries, but also under the Council of Europe. One can ponder whether this is a development caused by the so-called 'Brussels effect', whereby the EU 'exports' its own domestic standards and they become global (Bradford 2012, 2020), or whether a shift in the US privacy protection regime is underway (Chander et al. 2021).

Beyond data protection, three further innovations of the USMCA may be mentioned. The first refers to the inclusion of 'algorithms', the meaning of which is 'a defined sequence of steps, taken to solve a problem or obtain a result' (Article 19.1 USMCA), and has become part of the ban on requirements for the transfer or access to source code in Article 19.16.[23] The second novum refers to the recognition of 'interactive computer services' as particularly vital to the growth of digital trade.

[22] There is a footnote attached, which clarifies: 'A measure does not meet the conditions of this paragraph if it accords different treatment to data transfers solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of service suppliers of another Party.' The footnote does not appear in the CPTPP treaty text.

[23] On the expansion of the scope of the source code provision, see New Zealand's Waitangi Tribunal (2021: 104–112).

Parties pledge in this sense not to 'adopt or maintain measures that treat a supplier or user of an interactive computer service as an information content provider in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by the service, except to the extent the supplier or user has, in whole or in part, created, or developed the information' (Article 19.17(2) USMCA).[24] This provision is important, as it seeks to clarify the liability of intermediaries and delineate it from the liability of host providers with regard to infringement of IP rights. It also secures the application of Section 230 of the US Communications Decency Act,[25] which insulates platforms from liability (Goldman 2019; Goldman 2020; Bone 2021) but has been recently under attack in many jurisdictions in the face of fake news and other negative developments related to platforms' power (Feine 2020; Burri 2022).

The third and rather liberal commitment of the USMCA parties is with regard to open government data. This is truly innovative and very relevant in the domain of domestic regimes for data governance. In Article 19.18, the parties recognise that facilitating public access to and use of government information fosters economic and social development, competitiveness, and innovation. 'To the extent that a Party chooses to make government information, including data, available to the public, it shall endeavour to ensure that the information is in a machine-readable and open format and can be searched, retrieved, used, reused, and redistributed' (Article 19.18 (2) USMCA). There is in addition an endeavour to cooperate, so as to 'expand access to and use of government information, including data, that the Party has made public, with a view to enhancing and generating business opportunities, especially for small and medium-sized enterprises' (Article 19.8(3) USMCA). Finally, it can be mentioned that the cooperation provision of the USMCA goes beyond the CPTPP[26] and envisages an institutional setting to enable this cooperation, 'or any other matter pertaining to the operation of this chapter' (Article 19.14 (2) USMCA).

The US approach towards digital trade issues has been confirmed by the recent US–Japan DTA, signed on 7 October 2019, alongside the US–Japan Trade

[24] Annex 19-A creates specific rules with the regard to the application of Article 19.17 for Mexico, in essence postponing its implementation for three years. There is also a footnote to the provision, which specifies that a party may comply through 'application of existing legal doctrines as applied through judicial decisions'. For the argument that Canada's policy space has remained intact (Wolfe 2019: s78).

[25] Section 230 reads: 'No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider' and in essence protects online intermediaries that host or republish speech.

[26] The provision envisages, among other things linked to enabling global digital trade, exchange of information and experience on personal information protection, particularly with the view to strengthening existing international mechanisms for cooperation in the enforcement of laws protecting privacy, and cooperation on the promotion and development of mechanisms, including the APEC Cross-Border Privacy Rules, that further global interoperability of privacy regimes (Article 19.14(1) USMCA, at paras. (a)(i) and (b) respectively).

Agreement.[27] The US–Japan DTA replicates almost all provisions of the USMCA and the CPTPP,[28] including the rules on open government data (Article 20 US–Japan DTA), source code (Article 17 US–Japan DTA), and interactive computer services (Article 18 US–Japan DTA)[29] but notably covering also financial and insurance services as part of the scope of the agreement. In the current WTO negotiations on electronic commerce, the US endorsed for a number of years an ambitious template, which was essentially a compilation of the USMCA and the DTA (WTO US Communication 2019a, 2019b). Yet, in October 2023, the United States rather surprisingly announced that it would not further pursue provisions on data flows, data localisation and source code, so as to safeguard 'policy space' for a digital trade rethink.[30]

7.2.2.3 DEAs

The increased preoccupation of policymakers with digital trade issues can be perhaps best exemplified by the new generation of the so-called digital economy agreements. This is a relatively new phenomenon in the trade rulemaking landscape and so far only six such treaties have been adopted – the aforementioned US–Japan DTA; the 2019 ASEAN Agreement on Electronic Commerce (within the context of ASEAN); the 2020 Singapore–Australia Digital Economy Agreement (SADEA); the 2020 Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand, and Singapore; the 2021 Korea–Singapore DEA; and the 2022 UK–Singapore DEA. What is important to mention at the outset is that these agreements can be adopted as standalone initiatives, such as the DEPA, or as part of existing or new trade agreements, such as the ones between Singapore and Australia, and the UK and Singapore. The DEAs may also differ in scope and the extent to which they include new items on the regulation of the data-driven economy. So, while, for instance, the US–Japan DTA still very much resembles a conventional, albeit extended, digital trade chapter, the ASDEA, the DEPA, and the UK–Singapore DEA go beyond this and engage in entirely new areas of regulatory cooperation, including a mixed set of hard and soft law provisions. This section looks more closely

[27] For the text of the agreements, see: https://ustr.gov/countries-regions/japan-korea-apec/japan/us-japan-trade-agreement-negotiations/us-japan-digital-trade-agreement-text.

[28] Article 7: Customs Duties; Article 8: Non-Discriminatory Treatment of Digital Products; Article 9: Domestic Electronic Transactions Framework; Article 10: Electronic Authentication and Electronic Signatures; Article 14: Online Consumer Protection; Article 11: Cross-Border Transfer of Information; Article 12: Location of Computing Facilities; Article 16: Unsolicited Commercial Electronic Messages; Article 19: Cybersecurity US–Japan DTA.

[29] A side letter recognises the differences between the US and Japan's systems governing the liability of interactive computer services suppliers and parties agree that Japan need not change its existing legal system to comply with Article 18.

[30] See Inside US Trade, 'US to End Support for WTO E-commerce Proposals, Wants "Policy Space" for Digital Trade Rethink', 24 October 2023.

at the DEPA as a representative of this latter category and a model of innovative digital trade rulemaking.

The 2020 DEPA between Chile, New Zealand, and Singapore,[31] all parties also to the CPTPP, is, as noted earlier, not conceptualised as a pure trade agreement but one that is meant to address the broader issues of the digital economy. In this sense, its scope is wide, open, and flexible and covers several emergent issues, such as those in the areas of artificial intelligence (AI) and digital inclusion. The agreement is also not a closed deal, but one that is open to other countries (Article 16.2 DEPA) and the DEPA is meant to complement the WTO negotiations on electronic commerce and build upon the digital economy work underway within Asia-Pacific Economic Cooperation (APEC), the OECD, and other international forums. To enable flexibility and cover a wide range of issues, the DEPA follows a modular approach that provides countries with more options to pick and choose from and is very different from the 'all-or-nothing' approach of conventional trade treaties (Bacchus 2021: 8). After Module 1, specifying general definitions and initial provisions, Module 2 focuses on 'Business and Trade Facilitation'; Module 3 'Treatment of Digital Products and Related Issues'; Module 4 'Data Issues'; Module 5 'Wider Trust Environment'; Module 6 'Business and Consumer Trust'; Module 7 'Digital Identities'; Module 8 'Emerging Trends and Technologies'; Module 9 'Innovation and the Digital Economy'; Module 10 'Small and Medium Enterprises Cooperation'; and Module 11 'Digital Inclusion'. The rest of the modules deal with the operationalisation and implementation of the DEPA and cover common institutions (Module 12); exceptions (Module 13); transparency (Module 14); dispute settlement (Module 15); and some final provisions on amendments, entry into force, accession, and withdrawal (Module 16).

The type of rules varies across the different modules. On the one hand, all rules of the CPTPP are replicated; some of the USMCA rules, such as the one on open government data (Article 9.4 DEPA) (but not source code), and some of the US–Japan DTA provisions, such as the one on information and communication technology (ICT) goods using cryptography (Article 3.4 DEPA),[32] have been included too. On the other hand, there are many other rules – so far unknown to trade agreements – that try to facilitate the functioning of the digital economy and enhance cooperation on key issues. So, for instance, Module 2 on business and trade facilitation includes, next to the standard CPTPP-like norms,[33] additional efforts 'to establish or maintain a seamless, trusted, high-availability and secure interconnection of each Party's single window to facilitate the exchange of data

[31] For details and the text of the DEPA, see: www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/digital-economy-partnership-agreement/; for a comparison of the DEPA with existing PTAs, see Soprana (2021).

[32] The Article also provides detailed definitions of cryptography, encryption, and cryptographic algorithm and cipher.

[33] Article 2.2: Paperless Trading; Article 2.3: Domestic Electronic Transactions Framework.

relating to trade administration documents, which may include: (a) sanitary and phytosanitary certificates and (b) import and export data' (Article 2.2(5) DEPA).[34] Parties have also touched upon other important issues around digital trade facilitation, such as electronic invoicing (Article 2.5), express shipments and clearance times (Article 2.6), logistics (Article 2.4), and electronic payments (Article 2.7). Module 8 on emerging trends and technologies is also particularly interesting to mention, as it highlights a range of key topics that demand attention from policymakers, such as in the areas of fintech and AI. In the latter domain, the parties agree to promote the adoption of ethical and governance frameworks that support the trusted, safe, and responsible use of AI technologies, and in adopting these AI Governance Frameworks, parties would seek to follow internationally recognised principles or guidelines, including explainability, transparency, fairness, and human-centred values (Article 8.2(2) and (3) DEPA). The DEPA parties also recognise the interfaces between the digital economy, government procurement, and broader competition policy and agree to actively cooperate on these issues (Articles 8.3 and 8.4 DEPA). Along this line of covering broader policy matters in order to create an enabling environment that is also not solely focused on and driven by economic interests, DEPA deals with the importance of a rich and accessible public domain (Article 9.2 DEPA) and digital inclusion, which can cover enhancing cultural and people-to-people links, including between Indigenous peoples, as well as improving access for women, rural populations, and low socio-economic groups (Article 11.2 DEPA).

Overall, the DEAs are a new phenomenon in international trade law with the distinct objective of reflecting the broad range of issues the digital economy impinges upon. Digital economy agreements offer a good basis for harmonisation and interoperability of domestic frameworks and international cooperation that adequately takes into account the complex challenges of contemporary data governance that has essential trade but also non-trade elements. The appeal of the DEAs as a form of enhanced, but also flexible, cooperation on issues of the data-driven economy has been confirmed by South Korea's accession to the treaty in 2024 and Canada's (Government of Canada 2021) interest in joining the DEPA. Another example is the follow-up UK–Singapore DEA, which goes in some aspects beyond the DEPA and covers issues, such as lawtech cooperation and decent work for workers in the digital sector.

7.2.2.4 EU's Approach to Digital Trade

The EU has been a relatively late mover on digital trade issues and, for a long time, did not develop a distinct strategy. Although EU's PTAs did include provisions on

[34] 'Single window' is defined as a facility that allows parties involved in a trade transaction to electronically lodge data and documents with a single entry point to fulfil all import, export, and transit regulatory requirements (Article 2.1 DEPA).

electronic commerce, such as the 2002 agreement with Chile, the language tended to be cautious, with commitments not exceeding GATS levels, and limited to soft cooperation pledges in the services chapter (Article 102 EU–Chile FTA)[35] and in the fields of IT, information society, and telecommunications (Article 37 EU–Chile FTA). In more recent agreements, such as the EU–South Korea FTA (signed in 2009), the first EU Agreement with a dedicated electronic commerce chapter, the language is more concrete and binding, imitating some of the US template provisions, for instance, by confirming the applicability of the WTO agreements to measures affecting electronic commerce and subscribing to a permanent duty-free moratorium on electronic transmissions. Cooperation is also increasingly framed in more concrete terms and includes mutual recognition of electronic signature certificates, coordination on Internet service providers' liability, consumer protection, and paperless trading (Article 7.49 EU–South Korea FTA). As particularly insistent on data protection policies, the EU has also sought commitments from its PTA partners that the development of electronic commerce must be fully compatible with the international data protection standards (Article 7.48 EU–South Korea FTA).

The 2016 EU Agreement with Canada – the Comprehensive Economic and Trade Agreement (CETA) – goes a step further. The CETA provisions concern commitments ensuring (a) clarity, transparency, and predictability in their domestic regulatory frameworks; (b) interoperability, innovation, and competition in facilitating electronic commerce; as well as (c) facilitating the use of electronic commerce by small and medium-sized enterprises (Article 16.5 CETA). The EU succeeded in deepening the privacy commitments as the CETA has a specific norm on trust and confidence in electronic commerce, which obliges the parties to adopt or maintain laws, regulations, or administrative measures for the protection of personal information of users engaged in electronic commerce in consideration of international data protection standards (Article 16.4 CETA). Yet, there are no deep commitments on digital trade, or any rules on data and data flows (Wolfe 2019).

It is only very recently that the EU took up a more modern, CPTPP-comparable, approach towards the regulation of digital trade. Some indications for this turn were given by the 2018 EU–Japan Economic Partnership Agreement (EPA) (Article 8.81 EU–Japan EPA) and the modernisation of the trade part of the EU–Mexico Global Agreement. In these agreements, data flows were mentioned for the first time but still cautiously, as the parties only committed to 'reassess' within three years of the agreement's entry into force. The new EU approach towards the issue of cross-border data is now fully endorsed in the EU's currently negotiated deals with Australia and Tunisia, the 2020 post-Brexit Trade and Cooperation Agreement

[35] The agreement states that '[t]he inclusion of this provision in this Chapter is made without prejudice of the Chilean position on the question of whether or not electronic commerce should be considered as a supply of services'.

(TCA) with the UK,[36] as well as the 2022 Agreement with New Zealand. These PTAs' digital trade chapters include norms on the free flow of data and data localisation bans. However, this repositioning and newer commitments are also linked with high levels of data protection (European Commission 2018).

The EU wishes to permit data flows only if coupled with the high standards of its General Data Protection Regulation (GDPR)[37] and endorses a distinct model of privacy as a fundamental right. While the EU and its partners seek to permit the flow of data, these commitments are conditioned: first, by a dedicated article on data protection, which clearly states that: 'Each Party recognises that the protection of personal data and privacy is a *fundamental right* and that high standards in this regard contribute to trust in the digital economy and to the development of trade' (e.g. Article 6(1) draft EU–Australia FTA (emphasis added)),[38] followed by a paragraph on data sovereignty: 'Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards' (e.g. Article 202(2) TCA).[39] The EU also wishes to retain the right to see how the implementation of the provisions on data flows impacts the conditions of privacy protection, so there is a review possibility within three years of the entry into force of the agreement, and parties remain free to propose to review the list of restrictions at any time (e.g. Article 201(2) TCA).[40] In addition, there is a broad carve-out, in the sense that: 'The Parties reaffirm the right to regulate within their territories to achieve legitimate policy objectives, such as the protection of public health, social services, public education, safety, the environment including climate change, public morals, social or consumer protection, privacy and data protection, or the promotion and protection of cultural diversity' (e.g. Article 198 TCA).[41] The EU thus reserves ample regulatory

[36] Trade and Cooperation Agreement between the EU and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, OJ L [2020] 444/14.

[37] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), OJ 2016 L 119/1.

[38] The same wording is found in the EU–New Zealand and the draft EU–Tunisia FTA. Interestingly, the TCA does not explicitly mention data protection as a fundamental right. This can be, however, presumed, since the UK incorporates the European Convention on Human Rights (ECHR) through the Human Rights Act of 1998 into its domestic law (Irion and Burri 2022).

[39] The same wording is found in the EU–New Zealand and the draft EU–Tunisia FTA, as well as in the amended in 2023 Article 8.81 EU–Japan FTA.

[40] The same wording is found in the EU–New Zealand and the draft EU–Tunisia FTA, as well as in the amended in 2023 EU–Japan FTA.

[41] The same wording is found in the EU–New Zealand and the draft EU–Tunisia FTA, as well as in the amended in 2023 EU–Japan FTA.

leeway for its current and future data protection (and other) measures. The exceptions are also fundamentally different than the objective necessity test under the CPTPP and the USMCA, or that under WTO law, because it is subjective and safeguards the EU's right to regulate (Yakovleva 2020: 496; Burri and Kugler 2024).

Beyond the topic of data flows and its interface with data protection, it should be noted that the rest of the EU digital trade template includes the issues covered by the CPTPP/USMCA model, such as software source code (Article 207 TCA),[42] facilitation of electronic commerce (Articles 205 and 206 TCA), online consumer protection (Article 208 TCA), spam (Article 209 TCA), and open government data (Article 210 TCA). However, provisions on non-discrimination of digital products are missing and audiovisual services are excluded from the scope of application of the digital trade chapter (Article 197(2) TCA).

7.2.2.5 The RCEP

An interesting and much-anticipated development against the backdrop of the diverging, at least on data flows, EU and US positions has been the RCEP, signed on 15 November 2020 between the ASEAN Members,[43] China, Japan, South Korea, Australia, and New Zealand. The RCEP has been in force since 1 January 2022.[44]

Chapter 12 of the RCEP includes the relevant electronic commerce rules. In a similar fashion to the CPTPP, it clarifies its application 'to measures adopted or maintained by a Party that affect trade by electronic means' but excludes from this broad scope (1) government procurement and (2) information held or processed by or on behalf of a party, or measures related to such information, including measures related to its collection. Regarding trade facilitation, the RCEP includes provisions on paperless trading, electronic authentication, and electronic signatures (Article 12.6 RCEP). On paperless trading, the RCEP Members avoid entering into binding commitments. They, instead, commit to 'work toward', 'endeavour', or 'cooperate' (Article 12.5 RCEP). The norms on accepting the validity of electronic signatures are

[42] Again with notable safeguards, specified in paragraphs 2 and 3 of Article 207, including the general exceptions, security exceptions, and prudential carve-out in the context of a certification procedure; voluntary transfer of source code on a commercial basis, a requirement by a court or administrative tribunal, or a requirement by a competition authority pursuant to a party's competition law to prevent or remedy a restriction or a distortion of competition; a requirement by a regulatory body pursuant to a party's laws or regulations related to the protection of public safety with regard to users online; the protection and enforcement of IP; and government-procurement-related measures.

[43] Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Viet Nam.

[44] The RCEP entered into force on 1 January 2022 for ten original parties: Australia, New Zealand, Brunei Darussalam, Cambodia, China, Japan, Laos, Singapore, Thailand, and Viet Nam. The RCEP entered into force for the Republic of Korea on 1 February 2022 and for Malaysia on 18 March 2022. For the details and the text of the RCEP, see https://rcepsec.org/legal-text/.

more binding but, in contrast to the CPTPP and USMCA, permit domestic laws and regulations to provide otherwise and prevail in case of inconsistency.

Regarding commitments to create a conducive environment for electronic commerce, the inclusion of provisions on online personal information protection (Article 12.8 RCEP) and cybersecurity (Article 12.13 RCEP) is remarkable. On the former, RCEP Members establish that they shall adopt or maintain a legal framework that ensures personal information protection. Unsurprisingly, the RCEP is not prescriptive as to how parties may comply with this obligation. As for the latter aspect of cybersecurity, the parties do not establish a binding provision but recognise the importance of building capabilities and using existing collaboration mechanisms to cooperate. The RCEP Members also commit to adopt or maintain laws or regulations regarding online consumer protection (Article 12.7 RCEP), unsolicited commercial electronic messages (Article 12.9 RCEP), and a framework governing electronic transactions that take into account international instruments (Article 12.10 RCEP), as well as commit to transparency (Article 12.12 RCEP).

Concerning data flows, in essence, and similar to the EU PTAs, the RCEP provides only for conditional data flows, while preserving room for domestic policies, which may be of a data-protectionist nature. So, while the RCEP electronic commerce chapter includes a ban on localisation measures (Article 12.14 RCEP), as well as a commitment to free data flows (Article 12.15 RCEP), there are clarifications that give RCEP Members a lot of policy space and essentially undermine the impact of the made commitments. In this line, there is an exception possible for legitimate public policies and a footnote to Article 12.14.3(a), which says that: 'For the purposes of this subparagraph, the Parties affirm that the *necessity* behind the implementation of such legitimate public policy *shall be decided* by the implementing Party.'[45] This essentially goes against any exceptions assessment, as we know it under WTO law, and triggers a self-judging mechanism. In addition, subparagraph (b) of Article 12.14.3 says that the provision does not prevent a party from taking 'any measure that it considers necessary for the protection of its *essential security interests*. Such measures shall not be disputed by other Parties'.[46] Article 12.15 RCEP on cross-border transfer of information follows the same language and thus secures plenty of policy space, for countries like China or Viet Nam, to control data flows without further justification.

Noteworthy are also some things missing from the RCEP: in comparison to the CPTPP, the RCEP does not include provisions on customs duties, non-discriminatory treatment of digital products, source code, principles on access to and use of the Internet for electronic commerce, and Internet interconnection charge sharing. It is finally interesting to observe that the RCEP did not, at least

[45] Emphasis added.

[46] Emphasis added. The 'essential security interest' language has been endorsed by China also in the framework of the WTO electronic commerce negotiations.

initially, reflect China's position in the WTO negotiations, where China was more cautious and somewhat fuzzy in its demands. For instance, at the WTO, China subscribed to a very narrow definition of digital trade, arguing that the negotiations should focus on the discussion of cross-border trade *in goods* enabled by the Internet, together with relevant payment and logistics services, while paying attention to the digitisation trend of trade in services (WTO China Communication 2019: paragraph 2.5), and not engaging in commitments on data flows. This did change in later stages of the negotiations on the Joint Statement Initiative on Electronic Commerce, where China became more open to committing on digital trade issues, particularly those that facilitate it. This can be seen as a shift in China's position that now views a more open data economy as a key contributor to growth and can also be linked to China's wish to join the CPTPP.

7.3 THE NEW DESIGN ELEMENTS ON DIGITAL TRADE IN PTAS: CONCLUDING REMARKS

The above analysis of the developments in PTAs reveals the critical importance of digital trade as a negotiation topic and the substantial efforts made, particularly in recent years, to address it and create an adequate rule framework that goes beyond conventional trade liberalisation efforts. The achievements made by some PTAs and the dedicated DEAs are quite impressive. New and innovative approaches seek to address not only the 'old' issues raised under the 1998 WTO Work Programme on Electronic Commerce but also the contemporary issues in the context of a global data-driven economy. However, the new set of regulatory questions is not neatly defined and encompasses miscellaneous subject matters – from electronic contracts through source code to open government data. The question of free data flows and how to balance these against demands of digital sovereignty has become critical in recent years (Burri and Kugler 2024). In this context, the topic of personal data protection, typically one of fundamental rights' protection, has become a new preoccupation for trade negotiators (Burri 2021a; Chander and Schwartz 2023). The latter development attests to the fact that datafication has extended the scope of trade-related issues and that the electronic commerce/digital trade chapters have turned into centres of gravity to regulate all these.

One can also observe convergence on certain issues, in particular in the area of digital trade facilitation, but also divergence, in particular with regard to permitting and/or conditioning cross-border data flows, as this impacts on the sovereignty of states and their ability to protect the interests of their citizenry. This complex interface between domestic and international data governance regimes can be linked to crafting new reconciliation mechanisms in trade agreements but also to radical shifts and disengagement on data issues, as exemplified by the change in the US position from one of a legal *demandeur* to a more conservative stance (at least for now).

Finally, in terms of the overall evolution of international economic law, it is apparent that PTAs can serve as regulatory laboratories – testing new approaches as to scope, depth, different treaty language, and even new treaty forms, such as the DEAs. However, the political economy of this legal experimentation is complex, as it is linked to the formation of geopolitical blocks with overlaps that may lead to potential contestations and uncertainties as to the impact of the agreements on the ground. In this context, we see, for instance, that New Zealand is a member of the CPTPP, the RCEP, and the DEPA and also has an agreement with the EU; similarly, the UK has a deal with the EU, while also entering into ambitious digital trade commitments under DEAs and the CPTPP.

Overall, the landscape of digital trade rulemaking is likely to remain highly dynamic. We are bound to see the development of even newer design elements in PTAs as technology advances and as countries continue to position themselves – in particular in the area of AI regulation. The coming years will test the willingness for international cooperation in the domain of digital trade regulation and to what extent achievements made in the PTA venues can be translated to the multilateral forum of the WTO (Burri 2023a, 2023c). It would also test to what extent the digital trade agreements will be able to take up the new slew of issues that the data-driven economy affects – such as those around sustainability, platform power, and the protection of fundamental rights that are not solely focused on privacy (Burri 2023b). There are certain challenges intrinsic to these developments that would demand that treaty language adequately reflects the often precarious balance between economic and non-economic objectives, between domestic regulatory efforts and their external trade aspect. Moreover, digital trade rulemaking ought to become more inclusive and take the interests of developing and least developed countries on board.

REFERENCES

Abbott, K. W. and D. Snidal 2000. 'Hard and Soft Law in International Governance', *International Organization* 54(3): 421–456.

Adlung, R. and H. Mamdouh 2013. 'How to Design Trade Agreements in Services: Top Down or Bottom Up?' WTO Staff Working Paper 8.

Andersen, H. 2015. 'Protection of Non-Trade Values in WTO Appellate Body Jurisprudence: Exceptions, Economic Arguments, and Eluding Questions', *Journal of International Economic Law* 18(2): 383–405.

Bacchus, J. 2021. *The Digital Decide: How to Agree on WTO Rules for Digital Trade*. Special Report. Waterloo, ON: Centre for International Governance Innovation.

Barlow, J. P. 1996. 'A Declaration of the Independence of Cyberspace, 8 February 1996', www.eff.org/cyberspace-independence.

Bone, T. 2021. 'How Content Moderation May Expose Social Media Companies to Greater Defamation Liability', *Washington University Law Review* 98(3): 937–963.

Bradford, A. 2012. 'The Brussels Effect', *Northwestern University Law Review* 107(1): 1–68.

2020. *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press.
Burri, M. 2015. 'The International Economic Law Framework for Digital Trade', *Zeitschrift für Schweizerisches Recht* 135(2): 10–72.
2017. 'The Regulation of Data Flows in Trade Agreements', *Georgetown Journal of International Law* 48(1): 408–448.
2019. 'Understanding and Shaping Trade Rules for the Digital Era', in M. Elsig, M. Hahn and G. Spilker (eds.), *The Shifting Landscape of Global Trade Governance*. Cambridge: Cambridge University Press.
2021a. 'Interfacing Privacy and Trade', *Case Western Journal of International Law* 53(1): 35–88.
2021b. 'Data Flows and Global Trade Law', in M. Burri (ed.), *Big Data and Global Trade Law*. Cambridge: Cambridge University Press.
2022. 'Fake News in Times of Pandemic and Beyond: An Enquiry into the Rationales for Regulating Information Platforms', in K. Mathis and A. Tor (eds.), *Law and Economics of the Coronavirus Crisis*. Berlin: Springer.
2023a. 'A WTO Agreement on Electronic Commerce: An Enquiry into its Substance and Viability', *Georgetown Journal of International Law* 53(4): 565–625.
2023b. 'Digital Trade Law and Human Rights', *AJIL Unbound* 117: 110–115.
2023c. 'Trade Law 4.0: Are We There Yet?' *Journal of International Economic Law* 26(1): 90–100.
Burri, M. and T. Cottier (eds.) 2012. *Trade Governance in the Digital Age*. Cambridge: Cambridge University Press.
Burri, M. and R. Polanco 2020. 'Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset', *Journal of International Economic Law* 23(1): 187–220.
Burri, M., M. Vasquez Callo-Müller and K. Kugler 2024. 'The Evolution of Digital Trade Law: Insights from TAPED', *World Trade Review* 22(1): 1–18, https://doi.org/10.1017/S1474745623000472.
Chander, A. and P. M. Schwartz 2023. 'Privacy and/or Trade', *University of Chicago Law Review* 90(1): 50–135.
Chander, A., M. E. Kaminski and W. McGeveran 2021. 'Catalyzing Privacy Law', *Minnesota Law Review* 105(4): 1733–1802.
Eichensehr, K. E. 2015. 'The Cyber-Law of Nations', *The Georgetown Law Journal* 103(6): 317–380.
Elsig, M. and S. Klotz 2021. 'Data Flow-Related Provisions in Preferential Trade Agreements: Trends and Patterns of Diffusion', in M. Burri (ed.), *Big Data and Global Trade Law*. Cambridge: Cambridge University Press.
European Commission 2018. 'Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection in EU Trade and Investment Agreements', https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.
Feine, L. 2020. 'Big Tech's Favorite Law Is under Fire', CNBC. (19 February 2020) www.cnbc.com/2020/02/19/what-is-section-230-and-why-do-some-people-want-to-change-it.html.
Fliess, B. and P. Sauvé 1998. *Of Chips, Floppy Disks and Great Timing: Assessing the WTO Information Technology Agreement*. Paris: Institut Français des Relations Internationales.
Gao, H. 2018. 'Regulation of Digital Trade in US Free Trade Agreements: From Trade Regulation to Digital Regulation', *Legal Issues of Economic Integration* 45(1): 47–70.
Goldman, E. 2019. 'Why Section 230 Is Better Than the First Amendment', *Notre Dame Law Review Reflection* 95(1): 33–46.

2020. 'An Overview of the United States' Section 230 Internet Immunity', in: G. Frosio (ed.), *The Oxford Handbook of Online Intermediary Liability*. Oxford: Oxford University Press.

Government of Canada 2021. 'Global Affairs, Background: Canada's Possible Accession to the Digital Economy Partnership Agreement', www.international.gc.ca/trade-commerce/consultations/depa-apen/background-information.aspx?lang = eng.

Henke, N. et al. 2016. *The Age of Analytics: Competing in a Data-Driven World*. Washington, DC: McKinsey Global Institute.

Horn, H., P. C. Mavroidis and A. Sapir 2009. *Beyond the WTO? An Anatomy of EU and US Preferential Trade Agreements*. Brussels: Bruegel Print.

Irion, K. and M. Burri 2022. 'Digitaler Handel (Commentary of the Digital Trade Title of the EU–UK Trade and Cooperation Agreement)', in G. Kübek et al. (eds.), *Handels- und Kooperationsvertrag EU/GB Handbuch*. Baden-Baden: Nomos.

Joint Statement on Trilateral Meeting of the Trade Ministers of the United States, Japan, and the European Union. 2020. Washington, DC, https://trade.ec.europa.eu/doclib/docs/2020/january/tradoc_158567.pdf.

Kingsbury, B. et al. (eds.) 2019b. *Megaregulation Contested: Global Economic Ordering after TPP*. Oxford: Oxford University Press.

Kingsbury, B., P. Mertenskötter, R. B. Stewart and T. Streinz 2019a. 'The Trans-Pacific Partnership as Megaregulation', IILJ Working Paper 2019/2.

López-González, J. and M. Jouanjean 2017. 'Digital Trade: Developing a Framework for Analysis', OECD Trade Policy Papers 205.

López-González, J., F. Casalini and T. Nemoto 2022. 'Mapping Approaches to Cross-Border Data Flows', in I. Borchert and L. A. Winters (eds.), *Addressing Impediments to Digital Trade*. Brussels: CEPR Press.

Manyika, J. et al. 2011. *Big Data: The Next Frontier for Innovation, Competition, and Productivity*. Washington, DC: McKinsey Global Institute.

Mayer-Schönberger, V. and K. Cukier 2013. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. New York: Eamon Dolan/Houghton Mifflin Harcourt.

New Zealand's Waitangi Tribunal 2021. 'Report on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership'. (19 November 2021) https://forms.justice.govt.nz/search/Documents/WT/wt_DOC_195473606/Report%20on%20the%20CPTPP%20W.pdf.

Schwartz, P. M. and D. J. Solove 2014. 'Reconciling Personal Information in the United States and European Union', *California Law Review* 102(4): 877–916.

Shaffer, G. C. and M. A. Pollack 2010. 'Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance', *Minnesota Law Review* 94(3): 706–799.

Soprana, M. 2021. 'The Digital Economy Partnership Agreement (DEPA): Assessing the Significance of the New Trade Agreement on the Block', *Trade, Law and Development* 13(1): 143–169.

Torrey, Z. 2018. 'TPP 2.0: The Deal without the US: What's New about the CPTPP and What Do the Changes Mean?' *The Diplomat*. (03 February 2018) https://thediplomat.com/2018/02/tpp-2-0-the-deal-without-the-us/.

US Congress 2001. 'Bipartisan Trade Promotion Authority Act of 2001', H.R. 3005.

US Congressional Research Service 2021. 'China and Taiwan Both Seek to Join the CPTPP', https://crsreports.congress.gov/product/pdf/IN/IN11760.

Whitman, J. Q. 2004. 'The Two Western Cultures of Privacy: Dignity versus Liberty', *The Yale Law Journal* 113(6): 1151–1221.

Wolfe, R. 2019. 'Learning about Digital Trade: Privacy and E-Commerce in CETA and TPP', *World Trade Review* 18(S1): s63–s84.

WTO 1996. 'Ministerial Declaration on Trade in Information Technology Products', WT/MIN(96)/16.
1998. 'Work Programme on Electronic Commerce', WT/L/274.
2018. *World Trade Report 2018: The Future of World Trade: How Digital Technologies Are Transforming Global Commerce*. Geneva: World Trade Organization.
WTO China Communication 2019. 'Joint Statement on Electronic Commerce, Communication from China', INF/ECOM/19.
WTO 2019a. 'Joint Statement on Electronic Commerce, Communication from the United States', INF/ECOM/5.
2019b. 'Joint Statement on Electronic Commerce, Communication from the United States', INF/ECOM/23.
2019c. *World Trade Report 2019: The Future of Services Trade*. Geneva: WTO.
2021. 'Work Programme on Electronic Commerce: The Moratorium on Custom Duties on Electronic Transmissions: Need for Clarity on its Scope and Impact', WT/GC/W/833.
Wunsch-Vincent, S. 2003. 'The Digital Trade Agenda of the US', *Aussenwirtschaft* 58(1): 7–46.
2006. *The WTO, the Internet and Digital Products: EC and US Perspectives*. Oxford: Hart.
Wunsch-Vincent, S. and A. Hold 2012. 'Towards Coherent Rules for Digital Trade: Building on Efforts in Multilateral versus Preferential Trade Negotiations', in M. Burri and T. Cottier (eds.), *Trade Governance in the Digital Age*. Cambridge: Cambridge University Press.
Yakovleva, S. 2020. 'Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy', *University of Miami Law Review* 74(2): 416–519.
Yonhap News Agency 2021. 'South Korea Starts Process to Join DEPA', https://en.yna.co.kr/view/PYH20211006124000325.