1

Data Flows and Global Trade Law

*Mira Burri**

A INTRODUCTION

Information has always been a valuable as well as often sensitive asset for companies, states and citizens. In this sense, the link between data flowing across borders and the need to protect certain national interests is not entirely new and has been made before.[1] In particular during the late 1970s and the 1980s, as satellites, computers and software were profoundly changing the dynamics of communications, the trade-offs between allowing data to flow freely and asserting national jurisdiction became apparent. Echoing concerns of large multinational companies, some states worried that barriers to information flows might hinder economic activities and looked for mechanisms that could prevent the erection of such barriers. Non-binding solutions were found under the auspices of the Organisation for Economic Co-operation and Development (OECD) in the form of principles that sought to balance the free flow of data with the national interests in the fields of privacy and security.[2] Yet, as the OECD itself points out, while this privacy framework endured, the situation then was profoundly different from the challenges in the realm of data governance we face today.[3] Ubiquitous digitization and the societal embeddedness of digital media have changed the volume, the intensity and, indeed, the nature of data flows.[4]

* Mira Burri is Professor of International Economic and Internet Law and Managing Director Internationalization, Faculty of Law, University of Lucerne. Contact: mira.burri@unilu.ch.

1 See, e.g., C. Kuner, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future', OECD Digital Economy Paper No 187 (2011); S. A. Aaronson, 'Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security', *World Trade Review* 14 (2015), 671–700, at 672, 680–685.

2 OECD, *Guidelines for the Protection of Personal Information and Transborder Data Flows* (Paris: OECD, 1980).

3 OECD, *The OECD Privacy Framework: Supplementary Explanatory Memorandum to the Revised OECD Privacy Guidelines* (Paris: OECD, 2013).

4 See J. Manyika et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity* (Washington, DC: McKinsey Global Institute, 2011); V. Mayer-Schönberger and

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.182, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

The value of data, as well as the risks associated with data collection, data processing, data use and reuse, by both companies and governments, has dramatically changed. Beyond the flawed mantra of data being the 'new oil',[5] many studies point at the vast potential of data as a trigger for more efficient business operations, highly innovative solutions and better policy choices in all areas of societal life.[6] This transformative potential refers notably not only to 'digital native' areas, such as search or social networking, but also to brick-and-mortar or physical businesses, such as in manufacturing or logistics.[7] Overall, the implications of big data availability and analytics are multiple and some of them far reaching.[8]

Recent enquiries have shown that not only the sheer amount of data and our dependence on it have exponentially increased but also the ways governments assert control over global data flows have changed.[9] Exerting jurisdiction over online matters beyond borders, as exemplified by the seminal French judgment in the *Yahoo!* case,[10] or Internet censorship, as practised by China and many other states,[11] are well-known examples of control. Yet, the new generation of Internet controls seeks to keep information from going *out* of a country, rather than stopping it from

K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (New York: Eamon Dolan/Houghton Mifflin Harcourt, 2013); J. E. Cohen, 'What Privacy Is For', *Harvard Law Review* 126 (2013), 1904–1933, at 1920–1921.

5 *The Economist*, 'The World's Most Valuable Resource Is No Longer Oil, but Data', 6 May 2017.

6 See, e.g., Manyika et al., note 4; Mayer-Schönberger and Cukier, note 4; N. Henke et al., *The Age of Analytics: Competing in a Data-Driven World* (Washington, DC: McKinsey Global Institute, 2016).

7 See, e.g., Manyika et al., note 4.

8 There are no clear definitions of small versus Big Data. Definitions vary and scholars seem to agree that the term of Big Data is generalized and slightly imprecise. One common identification of Big Data is through characteristics of volume, velocity, and variety, also referred to as the '3-Vs'. Increasingly, experts add a fourth 'V' that relates to the veracity or reliability of the underlying data, as well as a fifth 'V' that relates to its value. See Mayer-Schönberger and Cukier, note 4, at 13. For a brief introduction on Big Data applications and review of the literature, see M. Burri, 'Understanding the Implications of Big Data and Big Data Analytics for Competition Law: An Attempt for a Primer', in K. Mathis and A. Tor (eds), *New Developments in Competition Behavioural Law and Economics* (Berlin: Springer, 2019), 241–263.

9 See A. Chander, 'National Data Governance in a Global Economy', UC Davis Legal Studies Research Paper No 495 (2016), at 2; also A. Chander and U. P. Lê, 'Data Nationalism', *Emory Law Journal* 64 (2015), 677–739.

10 Tribunal de Grande Instance de Paris, *Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Société Yahoo! France (LICRA v. Yahoo!)*, R6 00/05308 (2000). For more on the case, see also J. Goldsmith and T. Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford: Oxford University Press, 2001), at 49–64; M. H. Greenberg, 'A Return to Lilliput: The *LICRA* v. *Yahoo* – Case and the Regulation of Online Content in the World Market', *Berkeley Technology Law Review* 18 (2003), 1191–1258.

11 See, e.g., R. Deibert et al. (eds), *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA: MIT Press, 2008); R. Deibert et al. (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010); R. Deibert et al., *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (Cambridge, MA: MIT Press, 2011).

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

entering the sovereign state space. Governments increasingly 'localize' the data within their jurisdictions for a variety of reasons.[12] To be sure, this kind of erecting barriers to data flows impinges directly on trade and may endanger the realization of an innovative data economy. The provision of any digital products and services, cloud computing applications or, if we think in more future-oriented terms, the Internet of Things (IoT) and artificial intelligence (AI), would not function under restrictions on the cross-border flow of data.[13] Data protectionism also comes at a certain cost for the countries adopting such measures.[14]

At the same time, while it may often be true that higher levels of data protection will amount to a trade barrier, one cannot disregard the legitimate desire of countries to safeguard the fundamental rights of their citizens, public interests and values that matter for their constituencies. The impact of data collection and data use upon privacy protection in particular has been, in recent years, widely acknowledged by scholars and policymakers alike, as well as felt on the ground by regular users of digital products and services.[15] The risks have only been augmented in the era of big data, which presents certain distinct challenges to the protection of personal data and, by extension, to the protection of personal and family life.[16]

[12] United States International Trade Commission, *Digital Trade in the US and Global Economies*, Part 1, Investigation No 332-531 (Washington, DC: USITC, 2013); United States International Trade Commission, *Digital Trade in the US and Global Economies*, Part 2, Investigation No 332-540 (Washington, DC: USITC, 2014). For a country survey, see Chander and Lê, note 9.

[13] See Chander, note 9, at 2. See also Chapter 5 in this volume.

[14] See Chapter 3 in this volume.

[15] See P. Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', *UCLA Law Review* 57 (2010), 1701–1777; P. M. Schwartz and D. J. Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information', *New York University Law Review* 86 (2011), 1814–1894; O. Tene and J. Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics', *Northwestern Journal of Technology and Intellectual Property* 11 (2013), 239–273; The White House, *Big Data: Seizing Opportunities, Preserving Values* (Washington, DC: Executive Office of the President, 2014); U. Gasser, 'Perspectives on the Future of Digital Privacy', *Zeitschrift für Schweizerisches Recht* 135 (2015), 335–448; U. Gasser, 'Recoding Privacy Law: Reflections on the Future Relationship among Law, Technology, and Privacy', *Harvard Law Review* 130 (2016), 61–70; C. J. Bennett and R. M. Bayley, 'Privacy Protection in the Era of "Big Data": Regulatory Challenges and Social Assessments', in B. van der Sloot, D. Broeders and E. Schrijvers (eds), *Exploring the Boundaries of Big Data* (Amsterdam: University of Amsterdam Press, 2016), 205–227; S. B. Pan, 'Get to Know Me: Protecting Privacy and Autonomy under Big Data's Penetrating Gaze', *Harvard Journal of Law and Technology* 30 (2016), 239–261; Council of Europe, Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data, Strasbourg, T-PD(2017)01, 23 January 2017. See also Chapter 9 in this volume.

[16] The protection of privacy and family life are fundamental human rights enshrined in a number of international and regional acts, such as the Council of Europe's European Convention on Human Rights. The Charter of Fundamental Rights of the European Union (CFREU) distinguishes between the right of respect for private and family life in Article 7 and the right to protection of personal data, which is explicitly enshrined in Article 8. This distinction is no coincidence but reflects the heightened concern of the EU and translates into a positive duty to implement an effective protection of personal data and to regulate the transmission of such

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

Indeed, big data puts into question the very distinction between personal and non-personal data. On the one hand, it appears that one of the basic tools of data protection – that of anonymization, i.e. the process of removing identifiers to create anonymized datasets – is only of limited utility in a data-driven world, as in reality it is now rare for data generated by user activity to be completely and irreversibly anonymized.[17] On the other hand, big data enables the reidentification of data subjects by using and combining datasets of non-personal data, especially as data is persistent and can be retained indefinitely with the presently available technologies.[18]

Big data also puts into question the fundamental elements of existing privacy protection laws, which often operate upon requirements of transparency and user's consent.[19] Equally is data minimization as another core idea of privacy protection challenged, as firms are 'hungry' to get hold of more and more data.[20] These challenges have not been left unnoticed and have triggered the reform of data protection laws around the world, best exemplified by the European Union's General Data Protection Regulation (GDPR).[21] The reform initiatives are, however, not coherent and are culturally and socially embedded, reflecting societies' deep understandings of constitutional values, relationships between citizens and the state, and the role of the market, to name but a few.[22] The striking divergences both in the perceptions and the regulation of privacy protection across nations and in particular between the fundamental rights approach of the EU and the more market-based, non-interventionist approach of the United States[23] have also meant that conventional forms of international cooperation and an agreement on shared standards of data protection have become highly unlikely.

data. See Charter of Fundamental Rights of the European Union, OJ C [2010] 83/2; also M. Burri and R. Schär, 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy', *Journal of Information Policy* 6 (2016), 479–511.

[17] The White House, note 15, at 14.

[18] Ibid., at 14–15; also Ohm, note 15 and Chapter 9 in this volume.

[19] I. S. Rubinstein, 'Big Data: The End of Privacy or a New Beginning?', *International Data Privacy Law* 3 (2013), 74–87, at 78.

[20] Tene and Polonetsky, note 15.

[21] 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 (General Data Protection Regulation), OJ L [2016] 119/1 [hereinafter: GDPR].

[22] See, e.g., A. Chander, M. E. Kaminski and W. McGeveran, 'Catalyzing Privacy Law', University of Colorado Law Legal Studies Research Paper No 25 (2019).

[23] See, e.g., J. Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty', *The Yale Law Journal* 113 (2004), 1151–1221; P. M. Schwartz, 'The EU–US Privacy Collision: A Turn to Institutions and Procedures', *Harvard Law Review* 126 (2013), 1966–2009; P. M. Schwartz and D. J. Solove, 'Reconciling Personal Information in the United States and European Union', *California Law Review* 102 (2014), 877–916.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

Against this backdrop of a complex and contentious regulatory environment, data and cross-border data flows in particular have become one of the relatively new topics in global trade law discussions. Many questions have been raised in this context, for instance, whether and how do the existing trade rules apply to data flows? How should they be classified – as a good or a service, and if categorized as a service, under which services sector do they fall? How do we address new trade barriers, such as localization measures? How can we reconcile the free flow of data and countries' privacy, national security and other public interest concerns? How do we ensure that trade law accommodates the data-driven economy and enables global trade for the benefit of all? Which are the appropriate forum and the decision-making processes for moving the global data economy agenda ahead? Many of these questions are still open and this chapter will not give satisfactory answers to them all. It will nonetheless provide valuable information and insights about the current state of global trade law that may help policymakers down the road. In this sense, the chapter has a two-prong objective: first, it seeks to clarify the interfaces between the data-driven economy and existing trade law; second, and more importantly, it traces the regulatory responses and the emerging legal design in preferential trade agreements (PTAs) with regard to digital trade and data flows in particular.

B WTO LAW AS PRE-INTERNET LAW

While PTAs are in the spotlight of this chapter, the multilateral forum of the World Trade Organization (WTO) cannot be simply ignored – on the one hand, because it matters in its own right as a set of hard and enforceable rules on trade in goods, services and intellectual property (IP) protection, and on the other hand, because PTAs are in many senses only an addition to these rules. Politically speaking, the failings of the multilateral system on certain issues have prompted action on those issues in the preferential venues and this is particularly evident in the area of digital trade, as revealed later.

The WTO agreements, the fundamental basis of international trade law, were adopted during the Uruguay Round (1986–1994) and came into force in 1995.[24] Despite some adjustments – such as Information Technology Agreement (ITA),[25] its update in 2015 and the Trade Facilitation Agreement,[26] WTO law has not

[24] General Agreement on Tariffs and Trade 1994, 1867 U.N.T.S. 187; 33 I.L.M. 1153 (1994), entered into force 1 January 1995 [hereinafter: GATT]; General Agreement on Trade in Services, 1869 U.N.T.S. 183; 33 I.L.M. 1167 (1994), entered into force 1 January 1995 [hereinafter: GATS]; Agreement on Trade-Related Aspects of Intellectual Property Rights, 1869 U.N.T.S. 299; 33 I.L.M. 1197 (1994), entered into force 1 January 1995 [hereinafter: TRIPS].

[25] WTO, Ministerial Declaration on Trade in Information Technology Products, WT/MIN(96)/16 (1996).

[26] WTO, Protocol Amending the Marrakesh Agreement Establishing the World Trade Organization, Decision of 27 November 2014, WT/L/940 (2014), entered into force on 22 February 2017 following the ratification by two-thirds of the WTO membership.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

fundamentally changed and is still very much in its pre-Internet state.[27] One could, of course, argue that laws need not change with each and every new technological invention.[28] And indeed, the law of the WTO lends credence to such an argument because it is in many aspects, both in the substance and in the procedure, flexible and resilient. WTO law can be qualified as relatively 'hard', as it involves deep intervention in domestic regulatory regimes and can impose certain sanctions for breach of obligations.[29] It is furthermore based on powerful principles of non-discrimination, such as the most-favoured nation (MFN) and the national treatment (NT) obligations, that address all areas of economic life and could potentially tackle technological developments better than new made-to-measure regulatory acts. Many of the rules with regard to the application of the basic principles, with regard to standards, trade facilitation, subsidies and government procurement do also operate in a technologically neutral way.[30]

Another advantage of WTO law that may be highlighted is that despite its high degree of legalization and focus on economic rules, it also permits some flexibilities. One of those relates to the so-called general exceptions clauses formulated under Article XX of the General Agreement on Tariffs and Trade (GATT) 1994 and Article XIV of the General Agreement on Trade in Services (GATS), which allow WTO members to adopt measures that would otherwise violate their obligations and undertaken commitments, under the condition that these measures are not be applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade. Particularly interesting for this chapter's discussion on data flows are the possibilities that Article XIV of the GATS may open for maintaining existing and adopting new data restrictions. Article XIV enumerates different grounds as possible justifications and includes two specific categories that are of pertinence for our topic: (a) those relating to public order or public morals[31] and

[27] M. Burri, 'The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation', *UC Davies Law Review* 51 (2017), 65–132.

[28] See famously, F. H. Easterbrook, 'Cyberspace and the Law of the Horse', *The University of Chicago Legal Forum* 1996 (1996), 207–216.

[29] G. C. Shaffer and M. A. Pollack, 'Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance', *Minnesota Law Review* 94 (2010), 706–799, at 715.

[30] See M. Burri and T. Cottier (eds), *Trade Governance in the Digital Age* (Cambridge: Cambridge University Press, 2012); for an overview, see M. Burri, 'The International Economic Law Framework for Digital Trade', *Zeitschrift für Schweizerisches Recht* 135 (2015), 10–72.

[31] Article XIV(a) GATS. For an analysis, see J. C. Marwell, 'Trade and Morality: The WTO Public Morals Exception after *Gambling*', *New York University Law Review* 81 (2006), 802–842; M. Wu, 'Free Trade and the Protection of Public Morals: An Analysis of the Newly Emerging Public Morals Clause Doctrine', *Yale Journal of International Law* 33 (2008), 215–250; P. Delimatsis, 'The Puzzling Interaction of Trade and Public Morals in the Digital Era', in M. Burri and T. Cottier (eds), *Trade Governance in the Digital Age* (Cambridge: Cambridge University Press, 2010), 276–296.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

(b) those that are necessary to secure compliance with laws or regulations,[32] including such on 'the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts'.[33] Under this provision, it has been argued, for instance, that the rules of the GDPR may be found to violate the obligations of the EU under the GATS.[34]

Finally, in terms of evolution of norms, it can be maintained that the WTO possesses the advantage of a dispute settlement system that can foster legal evolution.[35] There is strong evidence in the WTO jurisprudence for both the capacity of the dispute settlement mechanism and for the relevance of the Internet in trade conflicts.[36] The *US–Gambling*[37] case is a great example in this context, as it confirmed that the GATS commitments apply to electronically supplied services and clarified key notions of services regulation, such as likeness and the scope of the 'public morals/public order' defence under Article XIV of the GATS.[38]

[32] Article XIV(c) GATS. For a commentary of Article XIV GATS, see T. Cottier, P. Delimatsis and N. Diebold, 'Article XIV GATS: General Exceptions', in R. Wolfrum, P.-T. Stoll and C. Feinäugle (eds), *Max Planck Commentaries on World Trade Law. Vol. 6: Trade in Services* (Leiden: Martinus Nijhoff Publishers, 2008), 287–328; H. Andersen, 'Protection of Non-trade Values in WTO Appellate Body Jurisprudence: Exceptions, Economic Arguments, and Eluding Questions', *Journal of International Economic Law* 18 (2015), 383–405.

[33] Article XIV(c)(ii) GATS.

[34] For a fully-fledged analysis, see R. H. Weber, 'Regulatory Autonomy and Privacy Standards under the GATS', *Asian Journal of WTO and International Health Law and Policy* 7 (2012), 25–47; K. Irion, S. Yakovleva and M. Bartl, *Trade and Privacy: Complicated Bedfellows?* (Amsterdam: Institute for Information Law, 2016), at 27–33. See also Chapter 4 in this volume.

[35] See, e.g., G. Sacerdoti et al. (eds), *The WTO at Ten: The Contribution of the Dispute Settlement System* (Cambridge: Cambridge University Press, 2006). For the current crisis of the WTO dispute settlement, see J. Pauwelyn, 'WTO Dispute Settlement Post 2019: What to Expect?', *Journal of International Economic Law* 22 (2019), 297–321.

[36] In fact, several major GATS cases have had a substantial Internet-related element. See WTO Panel Report, *Mexico – Measures Affecting Telecommunications Services (Mexico – Telecommunications)*, WT/DS204/R, adopted 2 April 2004; Panel Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services (US – Gambling)*, WT/DS285/R, adopted 10 November 2004; Appellate Body Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services (US – Gambling)*, WT/DS285/AB/R, adopted 7 April 2005; Panel Report, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products (China – Publications and Audiovisual Products)*, WT/DS363/R, adopted 12 August 2009; Appellate Body Report, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products (China – Publications and Audiovisual Products)*, WT/DS363/AB/R, adopted 21 December 2009; WTO Panel Report, *China – Certain Measures Affecting Electronic Payment Services (China – Electronic Payment Services)*, WT/DS413/R, adopted 31 August 2012.

[37] Ibid. In *US – Gambling*, Antigua brought a claim against the United States alleging that its restrictions on cross-border gambling services violated its obligations under the GATS. The Panel and the Appellate Body's findings focused on the violation of the US obligations for market access under Article XVI GATS.

[38] M. Krajewski, 'Playing by the Rules of the Game? Specific Commitments after *US – Gambling and Betting* and the Current GATS Negotiations', *Legal Issues of Economic Integration* 32

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

Yet, plainly assuming that the WTO's 'adaptive governance'[39] works will be flawed. Indeed, there are many reasons to question it and be rather sceptic about the match between the existing WTO rules, their implementation and evolution, and contemporary digital trade. Apart from the current political context, which may prevent new and forward-looking rule-making,[40] there are important hindrances in applying the GATS in the digital environment. In particular, the GATS commitments are based upon old pre-Internet classifications of services and sectors, and these have become increasingly disconnected from trade practices.[41] For instance, as the WTO law presently stands, it is unclear whether previously unknown things, such as online games, should be categorized as goods or services (and thus whether the more binding GATT or the GATS apply). Provided that no physical medium is involved and one decides consequently to apply the GATS, the classification puzzle is by no means solved: Online games, for instance, as a new type of content platform, could be potentially fitted into the discrete categories of computer and related services, value-added telecommunications services, entertainment or audiovisual services. One may also be unsure when there is an electronic data flow intrinsic to the service whether to classify this flow separately or as part of the traditional services.[42] Classification is by no means trivial,[43] as each category implies a completely different set of duties and/or flexibilities for the WTO members. If online platforms and the services they offer were to be classified as computer services, for example, states would lack any wiggle-room whatsoever and would have to grant full access to foreign services and services suppliers and treat them as they treat domestic ones – because of the high level of existing commitments under the GATS of

(2005), 417–447; S. Wunsch-Vincent, 'The Internet, Cross-Border Trade in Services, and the GATS: Lessons from *US–Gambling*', *World Trade Review* 3 (2006), 1–37; P. Delimatsis, 'Don't Gamble with GATS–The Interaction between Articles VI, XVI, XVII and XVIII GATS in the Light of the *US–Gambling* Case', *Journal of World Trade* 40 (2006), 1059–1080.

[39] R. Cooney and A. T. F. Lang, 'Taking Uncertainty Seriously: Adaptive Governance and International Trade', *European Journal of International Law* 18 (2007), 523–551; also A. T. F. Lang and J. Scott, 'The Hidden World of WTO Governance', *European Journal of International Law* 20 (2009), 575–614.

[40] For an analysis of crisis of the WTO, see, e.g., M. Elsig, M. Hahn and G. Spilker (eds), *The Shifting Landscape of Global Trade Governance* (Cambridge: Cambridge University Press, 2019).

[41] See Burri and Cottier, note 30.

[42] For a discussion of the application of technology neutrality to services classification, see S.-Y. Peng, 'GATS and the Over-the-Top Services: A Legal Outlook', *Journal of World Trade* 50 (2016), 21–46. One recent article argues a bit oddly that data should be classified separately as a good in analogy to electricity. See R. S. Neeraj, 'Trade Rules for the Digital Economy: Charting New Waters at the WTO', *World Trade Review* 18 (2019), 121–141.

[43] See R. H. Weber and M. Burri, *Classification of Services in the Digital Economy* (Berlin: Springer, 2012); S.-Y. Peng, 'Renegotiate the WTO Schedule of Commitments? Technological Development and Treaty Interpretation', *Cornell International Law Journal* 45 (2012), 403–430; I. Willemyns, 'GATS Classification of Digital Services – Does "The Cloud" Have a Silver Lining?', *Journal of World Trade* 53 (2019), 59–82.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

virtually all WTO members.[44] On the other hand, were online games classified as audiovisual services, most WTO members would have the policy space to maintain and adopt restrictive and discriminatory measures.[45] The evolutionary interpretation of schedules of specific commitments, as affirmed in *China–Audiovisual Products*, while a positive development, does not necessarily help much to achieve legal certainty in such situations.[46] Neither does the finding that the GATT and the GATS are not mutually exclusive.[47]

The classification dilemma, as particularly critical for digital trade, is an illuminating example of this state of paralysis but by far not the only one. Many other issues, although discussed in the framework of the 1998 WTO Work Programme on Electronic Commerce, have been left without a solution or even a clarification.[48] For instance and as a minimum for advancing on the digital trade agenda, there is still no agreement on a permanent moratorium on customs duties on electronic transmissions and their content.[49] Against the backdrop of pre-Internet WTO law and despite the recent reinvigoration of the e-commerce negotiations under the 2019 Joint Statement Initiative,[50] many of the disruptive changes underpinning the data-driven economy have demanded regulatory solutions outside the ailing multilateral trade forum. States around the world have used in particular the venue of preferential trade agreements to fill in some of the gaps of the WTO framework, clarify its applications and beyond that, address the newer trade barriers and accommodate their striving for seamless digital trade. Quite naturally for developments in

[44] For all members' commitments in the sector, see www.wto.org/english/tratop_e/serv_e/computer_e/computer_e.htm

[45] The EU has strongly argued for such a classification, so as to be able to maintain its supporting schemes. The promotion of local content in digitally delivered services is however not limited to Europe. The Chinese Ministry of Culture reportedly has classified online games as 'cultural products' supports the domestic industry. See USITC (2013), note 12, at 5–7.

[46] In *China – Publications and Audiovisual Products*, note 36, at para. 396. The Appellate Body found that the terms in China's Schedule 'are sufficiently generic that what they apply to may change over time'.

[47] As confirmed by WTO Appellate Body Report, *European Communities – Regime for the Importation, Sale and Distribution of Bananas (EC – Bananas)*, WT/DS27/AB/R, adopted 9 September 1997; WTO Appellate Body Report, *Canada – Certain Measures Affecting the Automotive Industry (Canada – Autos)*, WT/DS139/AB/R, WT/DS142/AB/R, adopted 31 May 2000.

[48] S. Wunsch-Vincent and A. Hold, '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, 2012), 179–221, at 181.

[49] The moratorium has only been temporarily extended several times, the last time for a period of two years following a decision taken in 2019. In recent years, there has even been a push by India and South Africa to rethink the scope, definition and impact of the moratorium. See WTO, Work Programme on Electronic Commerce – Review of Progress, Report by the Chairperson, WT/GC/W/780, 25 July 2019.

[50] WTO, Joint Statement on Electronic Commerce, WT/L/1056, 25 January 2019. As of 29 March 2019, 77 WTO Members support the initiative. For details, see M. Burri, 'Towards a New Treaty on Digital Trade', *Journal of World Trade* 55 (2021), 77–100.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

preferential trade, the framework that has emerged as a result and now regulates contemporary digital trade is not coherent. It is neither evenly spread across different countries, nor otherwise coordinated. Indeed, it is messy and fragmented both with regard to the substantive rules and the agreements' membership.

In the following section, the chapter provides an overview of the developments in PTAs in the last two decades in the area of digital trade governance. The information stems from our own dataset *TAPED*: Trade Agreement Provisions on Electronic Commerce and Data,[51] which ran a detailed mapping and coding of all PTAs that include chapters, provisions, annexes or side documents that directly or indirectly regulate digital trade. In the subsequent section, we look at the new rules on free data flows and their design across different PTAs. We then analyze in more detail the most sophisticated template for digital trade rules that we have so far – that of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and some subsequent developments in the United States–Mexico–Canada Agreement (USMCA). In the final section, the chapter offers some thoughts about the current state of global digital trade law and the prospects of governing data flows.

C EVOLUTION OF DIGITAL TRADE PROVISIONS IN PTAS

I *Overview and Some Emerging Trends*

From the 347 PTAs agreed upon between 2000 and 2019 and reviewed in TAPED, 184 PTAs have provisions related to digital trade.[52] The largest number of provisions is found in e-commerce and intellectual property chapters; overall, the provisions remain however highly heterogeneous, addressing various issues ranging from customs duties and paperless trading to personal data protection and cybersecurity. The depth of the commitments and the extent of their binding nature can also vary significantly. For instance, if one looks at the top countries that have entered into

[51] See M. Burri and R. Polanco, 'Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset', *Journal of International Economic Law* 23 (2020), 187–220. The TAPED dataset is available to all to use and further develop under the creative commons (attribution, non-commercial, share-alike) licence at the University of Lucerne website (www.unilu.ch/taped). For some previous attempts with a limited number of agreements, see, e.g., S. Wunsch-Vincent, 'Trade Rules for the Digital Age', in M. Panizzon, N. Pohl and P. Sauvé (eds), *GATS and the Regulation of International Trade in Services* (Cambridge: Cambridge University Press, 2008), 497–529; Wunsch-Vincent and Hold, note 48; J.-A. Monteiro and R. Teh, 'Provisions on Electronic Commerce in Regional Trade Agreements', WTO Working Paper No 11 (2017).

[52] The tables and figures in this section include treaties until end of 2019 at time of writing. The US–Japan Digital Trade Agreement has been covered but not the Digital Economy Partnership Agreement (DEPA) between Chile, Singapore and New Zealand and the EU–Vietnam FTA.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

PTAs with e-commerce provisions,[53] the European Union occupies the first place with Singapore, yet it is only in the very recent EU PTAs[54] that there is a dedicated chapter on e-commerce and some substantive provisions – beforehand e-commerce provisions were only few, part of the services chapters and limited to mere GATS-level commitments and cooperation pledges.[55]

Putting the digital trade provisions along a chronological line, it is evident that the inclusion of provisions in PTAs referring explicitly to electronic commerce is not a recent phenomenon, although it has evolved significantly in the past eighteen years. The first e-commerce provision dates back to the 2000 Free Trade Agreement (FTA) between Jordan and the United States.[56] Almost at the same time, New Zealand and Singapore agreed upon the Closer Economic Partnership Agreement (CEPA), including an article on paperless trading. Two years later, the Australia–Singapore FTA (SAFTA), concluded on 17 February 2003, was the first PTA to have a dedicated chapter on e-commerce. At the moment of this writing, specific provisions applicable to e-commerce can be found in 109 PTAs, mostly in dedicated chapters (79) (for details, see Table 1.1). The last eight years have witnessed a significant increase in the number of agreements with digital trade provisions. As shown in Figure 1.1, digital trade provisions are, on average, included in more than 68 per cent of all PTAs that were concluded between 2010 and 2019 and despite the fall in agreed upon deals, more of them include digital trade provisions. The rise in the total number of PTAs with such norms is driven mainly by bilateral PTAs: 84 per cent of total PTAs since 2000 and involves both developed and developing countries.[57]

Among the PTAs with digital trade provisions, it is evident that the number and level of detail have also increased significantly over the years, as depicted in Figure 1.2. In 2019, 13 is the average number of provisions found in e-commerce chapters of PTAs, with an average number of 2,527 words (see Table 1.2).

At the moment of writing, the Singapore–Australia Free Trade Agreement (SAFTA), updated in 2016, is the PTA in force with the highest number of provisions in an e-commerce chapter (19 in total), with 2,997 words. As of 2020, the USMCA

[53] The overall list will look like this: (1) Singapore – 22 PTAs; (2) EU – 22 PTAs; (3) Australia – 15 PTAs; (4) United States – 14 PTAs; (5) Chile – 13 PTAs; (6) Canada – 12 PTAs; (7) Colombia – 11 PTAs; (8) South Korea, Japan and Peru – 10 PTAs; (9) Panama, Costa Rica and New Zealand – 8 PTAs. See also Chapter 2 in this volume.

[54] EU–Canada Comprehensive Economic Trade and Investment Agreement (CETA), EU–Singapore FTA, EU–Vietnam FTA, EU–Japan FTA, EU–Indonesia FTA, EU–Philippines FTA and EU–Mexico FTA.

[55] See, e.g., M. Burri, 'The Regulation of Data Flows in Trade Agreements', *Georgetown Journal of International Law* 48 (2017), 408–448.

[56] Article 7 US–Jordan FTA.

[57] Following the UN country classification, 48 per cent of the PTAs with digital trade provisions were negotiated between developed and developing countries, and 49 per cent were negotiated between developing countries. Only 3 per cent of PTAs negotiated between developed countries include digital trade provisions. See also Chapter 2 in this volume.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

TABLE 1.1. *PTAs concluded with digital trade provisions per year (2000–2019)*

Year	Total PTAs	WTO notified	Digital trade provisions	E-commerce chapters	% PTAs with digital trade provisions
2000	20	8	2	0	10.00
2001	23	12	2	0	8.70
2002	26	8	4	0	16.00
2003	30	10	6	3	20.69
2004	29	14	6	6	21.43
2005	17	10	5	4	33.33
2006	26	13	7	6	31.82
2007	20	13	4	4	29.41
2008	24	27	9	6	40.91
2009	23	21	6	3	19.05
2010	14	18	5	3	50.00
2011	19	15	2	2	18.75
2012	8	20	3	3	33.33
2013	14	22	9	6	64.29
2014	14	12	10	7	88.89
2015	10	10	6	5	50.00
2016	11	14	7	5	71.43
2017	6	18	3	2	33.33
2018	9	7	9	10	100.00
2019	4	0	4	4	100.00
Total	347	272	109	79	

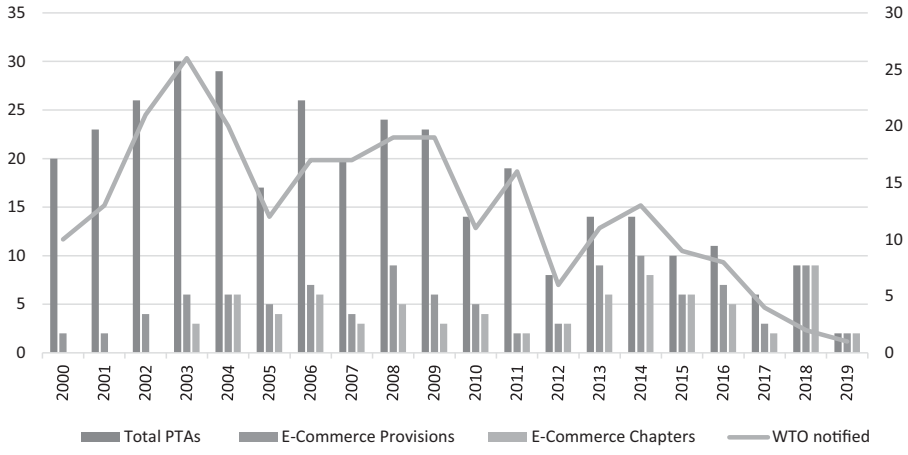

FIGURE 1.1. Evolution of PTAs with digital trade provisions (2000–2019)

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

TABLE 1.2. *PTAs with e-commerce chapters: average number of provisions and words (2000–2019)*

Year	Total PTAs	E-commerce chapters	Average number of articles	Average number of words
2000	20	2	1	91
2001	23	2	1	838
2002	25	4	4	168
2003	29	6	8	395
2004	28	6	6	606
2005	15	5	5	541
2006	22	7	6	801
2007	17	5	7	753
2008	22	9	7	606
2009	21	4	5	606
2010	10	5	3	313
2011	16	3	3	318
2012	9	3	3	233
2013	14	9	7	640
2014	9	8	8	1,073
2015	10	5	8	842
2016	7	5	10	1,390
2017	6	2	2	357
2018	10	10	12	1,697
2019	4	4	13	2,527

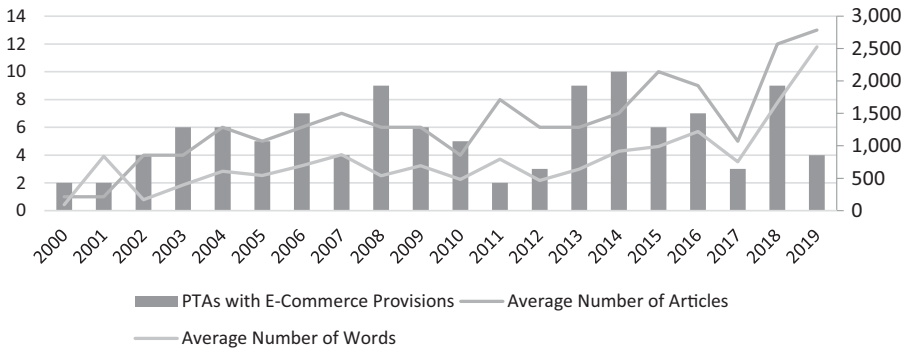

FIGURE 1.2. PTAs with digital trade provisions: average number of articles and words

would overtake SAFTA, as the current text of its Digital Trade chapter has also 19 articles but comprising 3,206 words. The new dedicated digital trade agreements go well beyond: the US–Japan Digital Trade Agreement has 5,346 words, and the Digital Economy Partnership Agreement (DEPA) between Chile, Singapore and New Zealand contains 10,887 words.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

II *Overview of Data-Related Rules in PTAs*

One can in general speak of the relevance of trade rules for data and data flows, as they matter for data in at least three ways: (i) because they regulate the cross-border flow of data by regulating trade in goods and services as well as the protection of intellectual property; (ii) because they may install certain beyond the border rules that demand changes in domestic regulation – for example, with regard to procedures with electronic signatures or data protection; and (iii) finally, because trade law can limit the policy space that regulators have at home.[58] Thinking of the layered structure of the Internet, one also ought to take into account the entire set of global economic law rules that regulate *infrastructure* (e.g. rules with regard to communication networks and services, technical standards and IT hardware) and *applications* and *content* (such as software, computer and audiovisual services), so as to understand the existing regulatory environment with regard to data flows.[59] In addition to this generic trade law framework, whose rules are found both in WTO law and in the WTO-plus preferential agreements, the last decade has also witnessed the emergence of entirely new rules that explicitly regulate data flows. This section provides a brief overview of these rules.

It needs to be mentioned at the outset that there is no common agreement on a definition of data flows in PTAs, despite the wide-spread rhetoric around the term and its frequent use in reports and studies.[60] One of the first agreements that targets data – the South Korea–United States FTA – stressed in its Article 15.8 'the importance of the *free flow of information* in facilitating trade, and acknowledging the importance of protecting personal information' and encouraged the Parties 'to refrain from imposing or maintaining unnecessary barriers to *electronic information flows* across borders'.[61] Later agreements, such as the CPTPP and the USMCA, that are analyzed in more detail later, speak of '*cross-border transfer of information by electronic means*, including personal information'[62] and this has become the most common wording thus far. The new generation of EU FTAs have been cautious with regard to data and has only recently started to promote the inclusion of

[58] See in this sense Burri, note 27; F. Casalini and J. López González, 'Trade and Cross-Border Data Flows', OECD Trade Policy Papers No 220 (2019).

[59] Such a delineation corresponds to the well-known layered model of the Internet (see, e.g., T. Wu, 'Application-Centered Internet Analysis', *Virginia Law Review* 85 (1999), 1163–1204; Y. Benkler, 'From Consumers to Users: Shifting the Deeper Structures of Regulation toward Sustainable Commons and User Access', *Federal Communications Law Journal* 52 (2000), 561–579; K. Werbach, 'A Layered Model for Internet Policy', *Journal of Telecommunications and High Technology Law* 1 (2002), 37–67. For a full-fledged analysis of the trade rules applicable to all layers, see Burri, note 30.

[60] See, e.g., W. J. Drake, 'Background Paper for the Workshop on Data Localization and Barriers to Transborder Data Flows', *World Economic Forum* (2016); Casalini and González, note 58.

[61] Emphases added.

[62] Article 14.11 CPTPP and Article 19.11 USMCA (emphasis added).

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

provisions on the '*free flow of data*'.[63] In essence, what can be maintained is that so far in the trade policy discourse and in the treaty language, there has not been any clear definition but despite the different terms used, there seems to be a tendency for a broad and encompassing definition of data flows (i) where there are bits of information (data) as part of the provision of a service or a product and (ii) where this data crosses borders, although the data flows do not neatly coincide with one commercial transaction and the provision of certain service may relate to multiple flows of data. In this sense, '[t]he geography of data flows is very different from the geography of trade flows'.[64] In addition, it may be noted that there has not been a distinction between different types of data – for instance, between personal and non-personal data, personal or company data or machine-to-machine data.[65] Yet, personal information is commonly included explicitly in the data-related provisions in PTAs,[66] whereby the potential clashes with domestic data protection regimes become evident.

Overall, specific data-related provisions are a relatively new phenomenon and can be found primarily in dedicated e-commerce chapters of PTAs and only in a handful of agreements. The rules refer to both the free cross-border flow of data and to banning or limiting data localization requirements. Provisions on the cross-border flow of data can be also found in chapters dealing with discrete services sectors, where data flows are inherent to the very definition of those services[67] – this is particularly valid for the telecommunications and the financial services sectors, as shown in Table 1.3.

[63] See, e.g., Article 8.81 EU–Japan FTA and the following section. See also S. Yakovleva, 'Should Fundamental Rights to Privacy and Data Protection Be a Part of EU's International Trade "Deals"?' *World Trade Review* 17 (2018), 477–508.

[64] OECD, 'Trade and Cross-Border Data Dlows', OECD Trade Policy Brief (2019). As the OECD (ibid., at 1) further clarifies: 'the actual flow of data reflects individual firm choices: accessing the OECD library from Paris, for instance, actually means contacting a server in the United States (the OECD uses a US-based company for its web services). Moreover, with the cloud, data can live in many places at once, with files and copies residing in servers around the world'.

[65] For instance, Sen classifies data into personal data referring to data related to individuals; company data referring to data flowing between corporations; business data referring to digitised content such as software and audiovisual content; and social data referring to behavioural patterns determined using personal data (see N. Sen, 'Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?', *Journal of International Economic Law* 21 (2018), 323–348, at 343–346). Aaronson and Leblond categorize data into personal data, public data, confidential business data, machine-to-machine data and metadata, although they do not specifically define each of these terms (see S. A. Aaronson and P. Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO', *Journal of International Economic Law* 21 (2018), 245–272). The OECD has also tried to break the data into different categories. See OECD, 'Data in the Digital Age', OECD Policy Brief, March 2019.

[66] It is typically defined as 'any information, including data, about an identified or identifiable natural person'. See, e.g., Article 19.1 USMCA.

[67] For example, banking and other financial services are commonly understood to include the provision and transfer of financial information, and financial data processing and related software by suppliers of other financial services (see Annex 10-A, Article 10.20 Singapore–US FTA; Article 117.9 Chile–EC AA; Annex IV-A Japan–Singapore FTA; Annex 2.1 New Zealand–

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

TABLE 1.3. *Overview of data-related provisions in PTAs*

	Data flows			
	General	Financial services	Telecommunication services	Data localization
Soft commitments	16	0	1	1
Hard commitments	12	70	64	11
Total number of provisions	28	70	65	12

1 Rules on Data Flows

If we look at the evolution of data flow provisions in PTAs, there has been a sea change over the years. Non-binding provisions on data flows appeared early. Already in the 2000 Jordan–US FTA, the Joint Statement on Electronic Commerce highlighted the 'need to continue the free flow of information', although it fell short of including an explicit provision in this regard. The first agreement having such a provision is the 2006 Taiwan–Nicaragua FTA, where as part of the cooperation activities, the parties affirmed the importance of working 'to maintain cross-border flows of information as an essential element to promote a dynamic environment for electronic commerce'.[68] A similar wording is used in the 2008 Canada–Peru FTA,[69] the 2011 Korea–Peru FTA,[70] the 2011 Central America–Mexico FTA,[71] the 2013 Colombia–Costa Rica FTA,[72] the 2013 Canada–Honduras FTA,[73] the 2014 Canada–Korea FTA,[74] and the 2015 Japan–Mongolia FTA.[75] In the same line, in the 2010 Hong Kong–New Zealand FTA, the parties agreed to ensure that 'their regulatory regimes support the free flow of services, including the development of innovative ways of developing services, using electronic means'.[76]

A slightly stronger commitment can be found in the 2007 South Korea–US FTA, where the parties, after 'recognizing the importance of the free flow of information

Singapore CEPA). The same is true for telecommunication services, which are defined as including, inter alia, data transmission typically involving the real-time transmission of customer supplied information between two or more points without any end-to-end change in the form or content of the customer's information, or simply including the transfer of data by electronic means (see Article 9.16(18) Singapore–US FTA; Annex IV-B Japan–Singapore FTA).

[68] Article 14.05(c) Nicaragua–Taiwan FTA.
[69] Article 1508(c) Canada–Peru FTA.
[70] Article 14.9(c) Korea–Peru FTA.
[71] Article 15.5(d) Central America–Mexico FTA.
[72] Article 16.7(c) Colombia–Costa Rica FTA.
[73] Article 16.5(c) Canada–Honduras FTA.
[74] Article 13.7(c) Canada–Korea FTA.
[75] Article 9.12(5) Japan–Mongolia FTA.
[76] Chapter 10, Article 2.1(h) Hong Kong–New Zealand FTA.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

in facilitating trade, and acknowledging the importance of protecting personal information', stated that they '*shall endeavor* to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders'.[77] More recently and as typically for EU-led agreements, the parties have agreed to consider in future negotiations commitments related to cross-border flow of information. Such a clause is found in the 2018 EU–Japan EPA,[78] and in the modernization of the trade part of the EU–Mexico Global Agreement, currently under negotiation. In the latter two agreements, the parties commit to 'reassess' within three years of the entry into force of the agreement, the need for inclusion of provisions on the free flow of data into the treaty. This signals a repositioning of the EU on the issue of data flows, as well as EU's wish to couple this in due time with the high data protection standards of the GDPR.[79] The EU follows this model of endorsing and protecting privacy as a fundamental right also in its proposals for digital trade chapters in the currently negotiated trade agreements with Australia, New Zealand and Tunisia,[80] as well as in the EU proposal for WTO rules on electronic commerce.[81]

The first agreement having a binding provision on cross-border information flows is the 2014 Mexico–Panama FTA. According to this treaty, each party 'shall allow its persons and the persons of the other Party to transmit electronic information, from and to its territory, when required by said person, in accordance with the applicable legislation on the protection of personal data and taking into consideration international practices'.[82] A much more detailed provision in this regard is found in the 2015 amended version of the Pacific Alliance Additional Protocol (PAAP),[83] which was modelled along the negotiated text of the 2016 Transpacific Partnership Agreement (TPP) and which has since then largely influenced all subsequent agreements having data flows provisions, such as notably the CPTPP and the USMCA[84] – both endorsing a strong protection of the free flow of data, as discussed in more detail later.

[77] Article 15.8 Korea–US FTA (emphasis added).

[78] Article 8.81 EU–Japan EPA.

[79] See European Commission, Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection in EU Trade and Investment Agreements, February 2018, available at: https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

[80] Interestingly the 2020 EU–Vietnam FTA includes no provisions on data flows and only three most cooperation provisions on e-commerce. See Articles 8.50–8.52 EU–Vietnam FTA.

[81] WTO, Joint Statement on Electronic Commerce: EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, Communication from the European Union, INF/ECOM/22, 26 April 2019. See also Chapter 10 in this volume.

[82] Article 14.10 Mexico–Panama FTA.

[83] Article 13.11 PAAP (2015).

[84] Such as the 2016 Chile–Uruguay FTA (Article 8.10), the 2016 Updated Singapore–Australia FTA (chapter 14, Article 13), the 2017 Argentina–Chile FTA (Article 11.6), the 2018 Singapore–Sri Lanka FTA (Article 9.9), the 2018 Australia–Peru FTA (Article 13.11), the 2018 Brazil–Chile FTA (Article 10.12) and the 2019 Australia–Indonesia FTA (Article 13.11).

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

2 Data Localization

In recent years, some PTAs have started to include specific provisions on data localization, by either banning or limiting requirements of data localization or data use. An important difference with the data flows provisions analyzed earlier is that almost all the provisions on data localization found in PTAs are binding.[85] The first agreement with such rules is the 2015 Japan–Mongolia FTA. The provision stipulates that neither party shall require a service supplier of the other party, an investor of the other party, or an investment of an investor of the other party in the area of the former party, to use or locate computing facilities in that area as a condition for conducting its business.[86] Later the same year, the 2015 amended version of the PAAP, and as strongly influenced by the parallel TPP negotiations, included a similar provision on the use and location of computer facilities.[87] In 2016, the TPP included a clear ban on localization, which was then replicated in the CPTPP and the USMCA. The diffusion of these norms is clearly discernible in subsequent PTAs, such as the 2016 Chile–Uruguay FTA[88] and the 2016 Updated SAFTA,[89] which closely follow the CPTPP template.[90]

3 Privacy and Data Protection

Eighty-one PTAs in our dataset include provisions on privacy, usually under the concept of 'data protection'. Yet, the way personal data is protected varies considerably and can include a truly mixed bag of binding and non-binding provisions (see Table 1.4), which is symptomatic of the very different positions of the major actors

[85] One of the few provisions on data localization that are not directly binding is found in the 2017 Argentina–Chile FTA, where the parties merely recognize the importance of not requiring a person of the other party to use or locate the computer facilities in the territory of that party, as a condition for conducting business in that territory and pledge to exchange good practices and current regulatory frameworks regarding servers' location. See Article 11.7 Argentina–Chile FTA.

[86] Article 9.10 Japan–Mongolia FTA.

[87] Article 13.11*bis* PAAP (2015).

[88] Article 8.11 Chile–Uruguay FTA.

[89] Chapter 14, Article 15 SAFTA.

[90] Some variations can be found in the 2019 Australia–Indonesia FTA, where a party may promptly renew a measure in existence at the date of entry into force of the agreement or amend such a measure to make it less trade restrictive, at any time (Article 13.12(2)). Additionally, the Australia–Indonesia FTA stipulates that nothing in the agreement shall prevent a party from adopting or maintaining any measure that it considers necessary for the protection of its essential security interests (Article 13.12(3)(b)). A second variation is found in the 2018 Singapore–Sri Lanka FTA, the 2018 Australia–Peru FTA and the 2018 Brazil–Chile FTA, which slightly deviate from the CPTPP, as there is no least restrictive measure requirement mentioned. See correspondingly Article 9.10 Singapore–Sri Lanka FTA; Article 13.12 Australia–Peru FTA; Article 10.13 Brazil–Chile FTA.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

TABLE 1.4. *Overview of privacy-related provisions in PTAs*

Total number of provisions	89
Soft commitments	81
Hard commitments	8

and the inherent tensions between the regulatory goals of data innovation and data protection.[91]

Earlier agreements dealing with privacy issues consist of non-binding declarations. The 2000 Jordan–US FTA Joint Statement on Electronic Commerce, for instance, merely declares it necessary to ensure the effective protection of privacy regarding the processing of personal data on global information networks, yet states also that the means for privacy protection should be flexible and parties should encourage the private sector to develop and implement enforcement mechanisms, such as guidelines and verification and recourse methodologies, recommending the OECD Privacy Guidelines as an appropriate basis for policy development.[92] Similarly, the 2001 Canada–Costa Rica FTA includes a provision on privacy as part of the Joint Statement on Global Electronic Commerce, with both parties agreeing to share information on the functioning of their respective data protection regimes.[93] Later agreements include cooperation activities on enhancing the security of personal data in order to improve the level of protection of privacy in electronic communications and avoid obstacles to trade that requires transfer of personal data.[94] These activities include sharing information and experiences on regulations, laws and programmes on data protection[95] or the overall domestic regime for the protection of personal information;[96] technical assistance in the form of exchange of

[91] See, e.g., Schwartz, note 23; Schwartz and Solove, note 23. See also Chapter 10 in this volume.

[92] Jordan–US, Joint Statement on Electronic Commerce, 7 June 2000, Article II.

[93] Canada–Costa Rica FTA, Joint Statement on Global Electronic Commerce.

[94] Article 13.1 and Article 99(d) EC–Moldova AA.

[95] Article 10.8.5 and Article 10.15(b) Brazil–Chile FTA; Article 14.5.2 Central America–Korea FTA; Article 11.5.5 and Article 11.9(b) Argentina–Chile FTA; Article 8.7.4 and Article 8.13(b) Chile–Uruguay FTA; Article 13.6(1) EAEU–Vietnam FTA; Article 9.12(2) Japan–Mongolia FTA; Article 13.7(b) Canada–Korea FTA; Article 13.10(2) Australia–Japan FTA; Article 14.11(b) Mexico–Panama FTA; Article 13.8(2) and Article 13.12(b) PAAP; Article 11.7(b) Singapore–Taiwan FTA; Article 16.5(b) Canada–Honduras FTA; Article 34 EU–Central America FTA; Article 15.5(b) Central America–Mexico FTA; Article 14.7(2)(b) Korea–Peru FTA; chapter 10, Article 9.1(c) ASEAN–Australia–New Zealand FTA; Article 82.2(a) Japan–Switzerland FTA; Article 1507.1(b) Canada–Colombia FTA; Article 1508(b) Canada–Peru FTA; Article 14.8(b) Colombia–Northern Triangle FTA; Article 14.5(b) Panama–US FTA; Article 12.5(b) Chile–Colombia FTA; Article 14.05(b) Nicaragua–Taiwan FTA; Article 13.4(b) Panama–Singapore FTA; Article 14.5(b) CAFTA–DR–US; Article 15.5(b) Chile–US FTA.

[96] Article 13.3(1)(b)(i) Australia–Indonesia FTA; Article 19.14(1)(a)(i) USMCA; Article 13.14(b)(i) Australia–Peru FTA; Article 9.12(c)(i) Singapore–Sri Lanka FTA; Article 9.9(c) Singapore–

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

information and experts;[97] research and training activities;[98] the establishment of joint programmes and projects;[99] maintaining a dialogue;[100] holding consultations on matters of data protection;[101] or in general, other cooperation mechanisms to ensure the protection of personal data.[102]

PTAs have also dealt with personal data protection with reference to the adoption of domestic standards. While some merely recognize the importance or the benefits of protecting personal information online,[103] in several treaties parties specifically commit to adopt or maintain legislation or regulations that protect the personal data or privacy of users,[104] in relation to the processing and dissemination of data,[105] which may also include administrative measures,[106] or the adoption of non-discriminatory practices.[107] Few agreements include qualifications of this commitment, in the sense that each party shall take measures it deems appropriate and necessary considering the differences in existing systems for personal data protection,[108] that such measures shall be developed insofar as possible,[109] or that the

Turkey FTA; Article 13.5 China–Korea FTA; Article 16.6(2) Colombia–Costa Rica FTA; Article 1506.2 Canada–Colombia FTA.

97 Article 30 Chile–EC AA.

98 Article 10.8(1)(b) Korea–Vietnam FTA.

99 Article 30 Chile–EC AA.

100 Article 163.1(e) Colombia–EU–Peru FTA.

101 Article 16.10(1) Australia–Chile FTA.

102 Article 14.7(1)(a) Central America–Korea FTA; Annex-B, Article 2(e) Colombia–Israel FTA; Article 19.7(1)(b) Colombia–Panama FTA; Article 12.6(1)(c) Colombia–Korea FTA; Article 13 Armenia–EU CEPA; Article 15 EC–Ukraine AA; Article 14 EC–Georgia AA.

103 Article 13.7(1) Australia–Indonesia FTA; Article 10.2(5)(f) and Article 10.8.1 Brazil–Chile FTA; Article 8.78(3) EU–Japan EPA; Article 14.5(1) Central America–Korea FTA; Article 16.2(2)(e) Canada–Honduras FTA.

104 Article 13.7(2) Australia–Indonesia FTA; Article 10.8.2 Brazil–Chile FTA; Article 19.8(1–2) USMCA; Article 13.8(1–2) Australia–Peru FTA; Article 9.7(1–2) Singapore–Sri Lanka FTA; Article 11.5(1–2) Argentina–Chile FTA; Article 16.4 CETA; chapter 14, Article 9.1-2 Australia–Singapore FTA (2016); Article 8.7(1–2) Chile–Uruguay FTA; Article 14.8(1–2) TPP/CPTPP; Article 9.7(1-2) Singapore–Turkey FTA; Article 13.5 China–Korea FTA; Article 13.5 EAEU–Vietnam FTA; Article 10.6(1) Korea–Vietnam FTA; Article 9.6(3) Japan–Mongolia FTA; Article 13.8(1) Australia–Japan FTA; Article 15.8 Australia–Korea FTA; Article 14.8 Mexico–Panama FTA; Article 13.8(1) PAAP; Article 19.6 Colombia–Panama FTA; chapter 9, Article 2 (d)(i) New Zealand–Taiwan; Article 12.3 Colombia–Korea FTA; Article 55 Chile–China FTA (2018); Article 15.8(1) Australia–Malaysia FTA; Article 1506.1 Canada–Colombia FTA.

105 Annex II, Article 1(c)(i) Central America–EFTA; Annex XVI, Article 1(c)(i) EFTA–GCC FTA; Annex I, Article 1(c)(i) EFTA–Colombia FTA; Annex I, Article 1(c)(i) EFTA–Peru FTA.

106 Article 16.6(1) Colombia–Costa Rica FTA; Article 14.7 Korea–Peru FTA; chapter 10, Article 2.1 (f) Hong Kong–New Zealand FTA; chapter 10, Article 7.1-2 ASEAN–Australia–New Zealand FTA; Article 16.8 Australia–Chile FTA; Article 1507 Canada–Peru FTA.

107 Article 13.6(3) Australia–Indonesia FTA; Article 10.8(3) Brazil–Chile FTA; Article 19.8(4) USMCA; Article 13.8(3) Australia–Peru FTA; Article 11.5(3) Australia–Chile FTA; chapter 14, Article 9.3 Australia–Singapore FTA (2016); Article 14.8(3) TPP/CPTPP.

108 Article 12.8(1) Australia–China FTA; Article 11.7(1)(j) Chile–Thailand FTA; chapter 14, Article 7.1 Australia–Singapore FTA (2003).

109 Annex-B, Article 3 Colombia–Israel FTA.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

parties have the right to define or regulate their own levels of protection of personal data in pursuit or furtherance of public policy objectives, and shall not be required to disclose confidential or sensitive information.[110] Some PTAs add that in the development of online personal data protection standards, each party shall take into account the existing international standards,[111] as well as criteria or guidelines of relevant international organizations or bodies[112] – such as the APEC Privacy Framework and the OECD Guidelines on Transborder Flows of Personal Data (2013);[113] or to accord a high level of protection compatible with the highest international standards in order to ensure the confidence of e-commerce users.[114] In a handful of treaties, the parties commit to publish information on the personal data protection it provides to users of e-commerce,[115] including how individuals can pursue remedies and how businesses can comply with any legal requirements.[116] Certain agreements put special emphasis on the transfer of personal data, stipulating that it shall only take place if necessary for the implementation, by the competent authorities, of agreements concluded between the parties,[117] or that the countries need to have an adequate level of safeguards for the protection of personal data.[118] Some treaties add that the parties will encourage the use of encryption or security mechanisms for the personal information of the users, and their dissociation or anonymization, in cases where said data is provided to third parties.[119]

PTA parties have also employed more binding options to protect personal information online. A first option is to consider the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the

[110] Article 18.1(2)(h) and Article 18.16(7) EU–Japan EPA.
[111] Article 8.57(4) EC–Singapore FTA; Article 11.5(1-2) Argentina–Chile FTA; Article 8.7(2) Chile–Uruguay FTA.
[112] Article 13.7(3) Australia–Indonesia FTA; Article 13.8(2) Australia–Peru FTA; Article 16.4 CETA; chapter 14, Article 9.2 Australia–Singapore FTA (2016); Article 14.8(2) TPP/CPTPP; Article 12.8(2) Australia–China FTA; Article 10.6(2) Korea–Vietnam FTA; Article 13.8(2) Australia–Japan FTA; Article 139.2 EC–Ukraine AA; Article 127.2 EC–Georgia AA; Article 15.8 Australia–Korea FTA; Article 14.8 Mexico–Panama FTA; Article 11.7(j) Chile–Thailand FTA; Article 19.6 Colombia–Panama FTA; Article 16.6(1) Colombia–Costa Rica FTA; Article 12.1(2) and Article 12.3 Colombia–Korea FTA; Article 201.2 EU–Central America FTA; Article 15.8(2) Australia–Malaysia FTA; chapter 10, Article 7.3 ASEAN–Australia–New Zealand FTA; Article 16.8 Australia–Chile FTA; Article 10.5 New Zealand–Thailand FTA; Article 1106 Australia–Thailand FTA; chapter 14, Article 7.2 Australia–Singapore FTA (2003).
[113] Article 19.8(2) USMCA.
[114] Article 197.2 Armenia–EU CEPA; Article 162.2 Colombia–EU–Peru FTA; Article 119.2; Chile–EC AA and Article 202 CARIFORUM–EC EPA.
[115] Article 10.8(4) Brazil–Chile FTA.
[116] Article 19.8(5) USMCA; Article 13.8(4) Australia–Peru FTA; Article 9.7(3) Singapore–Sri Lanka FTA; chapter 14, Article 9.4 Australia–Singapore FTA (2016); Article 8.7(3) Chile–Uruguay FTA; Article 14.8(4) TPP/CPTPP; Article 9.7(3) Singapore–Turkey FTA.
[117] Article 13.2 EC–Moldova AA.
[118] Article 10.6(2) Korea–Vietnam FTA.
[119] Article 10.8(6) Brazil–Chile FTA; Article 11.5(6) Argentina–Chile FTA; Article 8.7(5) Chile–Uruguay FTA.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

protection of confidentiality of individual records as an exception in specific chapters of the agreement – such as for trade in services,[120] investment or establishment,[121] movement of persons,[122] telecommunications[123] and financial services.[124] Certain agreements, mostly EU led, even have special chapters on protection of personal data, including the principles of purpose limitation, data quality and proportionality, transparency, security, right to access, rectification and opposition, restrictions on onward transfers, and protection of sensitive data, as well as provisions on enforcement mechanisms, coherence with international commitments and cooperation between the parties in order to ensure an adequate level of protection of personal data.[125] The USMCA was the first US-led PTA to include such a provision that recognizes key principles of data protection.[126]

A second option lets countries adopt appropriate measures to ensure the privacy protection while allowing the free movement of data, establishing a criterion of 'equivalence' – meaning that countries agree that personal data may be exchanged only where the receiving party undertakes to protect such data in at least an equivalent, similar or adequate way to the one applicable to that particular case in the party that supplies it. This has been largely the EU approach and to that end, parties commit to inform each other of their applicable rules and negotiate reciprocal general or specific agreements.[127]

[120] Article 69.1(c) Japan–Singapore FTA.

[121] Article 135.1(e)(ii) Chile–EC AA; Article 83.1(c)(ii) Japan–Singapore FTA.

[122] Article 95.1(c)(ii) Japan–Singapore FTA.

[123] Article 18.3(4) USMCA; Article 8.44(4) EU–Japan EPA; Article 12.4(4) Australia–Peru FTA; Article 8.3(4) Singapore–Sri Lanka FTA; Article 10.3(4) Argentina–Chile FTA; Article 10.3(4) Australia–Singapore FTA (2016); Article 8.3(5) Singapore–Turkey FTA; Annex 5, Article 3 Japan–Mongolia FTA; Article 13.3(4) Korea–Peru FTA; Article 13.2(4) Panama–US FTA; Annex VI, Article IX(a) Japan–Switzerland FTA; Article 13.02(4) Nicaragua–Taiwan FTA; Article 11.3(4) Korea–Singapore FTA; Article 13.2(4)(b) Morocco–US FTA; Article 13.2(4) Chile–US FTA.

[124] Annex 17-A USMCA; Article 8.63 EU–Japan EPA; Article 8.45 EU–Vietnam FTA; Article 8.54 (2) EC–Singapore FTA; Article 10.21 Australia–Peru FTA; Article 185 Armenia–EU CEPA; Article 13.15(4) CETA; Annex 9-B Australia–Singapore FTA (2016); Annex 11-B TPP/CPTPP; Article 10.12 Singapore–Turkey FTA; Annex 4, Article 11 Japan–Mongolia FTA; Article 129.2 EC–Ukraine AA; Article 118.2 EC–Georgia AA; chapter 10, Annex on Financial Services, Article 7.2 ASEAN–Australia–New Zealand FTA; Annex VI, Article VIII Japan–Switzerland FTA; Annex XVI – financial services, Article 8 EFTA–Colombia FTA; Article 245 EC–Moldova AA; Article 135.1(e)(ii) Chile–EC AA.

[125] Chapter 6, Articles 61–65 Cameroon-EC Interim EPA; chapter 6, Articles 197–201 CARIFORUM-EC EPA. Other agreements merely recognize principles for the collection, processing and storage of personal data such as prior consent, legitimacy, purpose, proportionality, quality, safety, responsibility and information, but without developing this in detail: Article 11.2(5)(f), footnote 1, Argentina–Chile FTA; Article 8.2(5)(f), footnote 3, Chile–Uruguay FTA.

[126] Article 19.8(3) USMCA; see also below.

[127] Article 8.54(2) EC–Singapore FTA; Articles 9.2 and 11.1 Understanding 3 on Additional Customs-Related Provisions; Protocol on Mutual Administrative Assistance on Custom Matters, Article 10 EC–Ghana EPA; Protocol 5 on Mutual Administrative Assistance on Custom Matters, Article 10.2

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

A third, less used, option leaves the development of rules on data protection to a treaty body. For example, in the 2012 Colombia–EU–Peru FTA (which also now includes Ecuador), the Trade Committee may establish a working group with the task of proposing guidelines to enable the signatory Andean Countries to become a 'safe harbour' for the protection of personal data. To this end, the working group shall adopt a cooperation agenda that defines priority aspects for accomplishing that purpose, especially regarding the respective homologation processes of data protection systems.[128]

D SUBSTANTIVE DEVELOPMENTS IN DIGITAL TRADE GOVERNANCE

As evident from the earlier overview, the regulatory environment for data flows has been substantially shaped by PTAs. The United States has played a key role in this process and has sought to endorse liberal rules in implementation of its 'Digital Agenda'.[129] The agreements reached since 2002 with Australia, Bahrain, Chile, Morocco, Oman, Peru, Singapore, the Central American countries,[130] Panama, Colombia and South Korea, all contain critical WTO-plus (going above the WTO commitments) and WTO-extra (addressing issues not covered by the WTO) provisions in the broader field of digital trade. The emergent regulatory template on digital issues is not however limited to US agreements but has diffused and can be found in other FTAs, as evident from the earlier overview. Singapore, Australia, Japan and Colombia have been among the major drivers of this diffusion but as earlier mentioned, the issues covered and the levels of legalization may still vary substantially.[131]

Key aspects of digital trade are typically addressed in (i) specifically dedicated e-commerce chapters; (ii) the chapters on cross-border supply of services; and (iii) the IP chapters. The electronic commerce chapters show by far the most substantial evolution over time – moving from less to more binding and from a mere compensation for the lack of progress in the WTO towards new (and partially innovative) digital trade rule-making. In the former sense, they have included a clear definition of 'digital products', which treats digital products delivered offline equally as those delivered online, so that technological neutrality is ensured. The chapters also recognize the applicability of WTO rules to electronic commerce, and establish a permanent moratorium on duties on the import or export of digital products by

Bosnia and Herzegovina–EC SAA; Article 45 and Protocol No 7 Algeria EC Euro-Med Association Agreement.

[128] Article 109(b) Colombia–EU–Peru FTA.

[129] See S. Wunsch-Vincent, 'The Digital Trade Agenda of the US: Parallel Tracks of Bilateral, Regional and Multilateral Liberalization', *Aussenwirtschaft* 58 (2003), 7–46.

[130] The DR–CAFTA includes Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua and the Dominican Republic.

[131] See Chapter 2 in this volume.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

electronic transmission. Critically, the e-commerce chapters, especially those of US-led agreements, ensure both MFN and NT for digital products trade; discrimination is banned on the basis that digital products are 'created, produced, published, stored, transmitted, contracted for, commissioned, or first made available on commercial terms outside the country's territory' or 'whose author, performer, producer, developer, or distributor is a person of another party or a non-party'.[132]

The e-commerce chapters do also include rules that go beyond the WTO and next to provisions on IT standards and interoperability, cybersecurity, electronic signatures and payments, paperless trading and e-government, the rules on data flows are the most illustrative example in this context. In the following two sections, we look more closely at the most advanced template for digital trade chapters endorsed by the CPTPP and slightly further developed by the USMCA, including also some remarks on the dedicated US–Japan Digital Trade Agreement.

I *The CPTPP*

The Comprehensive and Progressive Agreement for Transpacific Partnership (CPTPP; also known as the TPP11 or TPP 2.0)[133] was agreed upon in 2017 among eleven countries in the Pacific Rim[134] and entered into force on 30 December 2018. The CPTPP represents 13.4 per cent of the the global gross domestic product, or $13.5 trillion, making it the third largest trade agreement after the North American Free Trade Agreement and the single market of the European Union.[135] Beyond the broader economic impact and, more importantly, for the discussion of this chapter, the CPTPP chapter on e-commerce created the most comprehensive template so far in the landscape of PTAs. It comprises eighteen articles and includes a number of new features.[136] It is fair to note that the e-commerce chapter of the CPTPP 'survived' the TPP negotiations in its entirety and without any change, so in a sense it still very much reflects the efforts of the United States in the domain of digital trade rule-making.

The CPTPP sought for the first time to explicitly restrict the use of data localization measures. Article 14.13(2) prohibits the parties from requiring a 'covered person

[132] See, e.g., Article 14.3 US–Singapore FTA; Article 16.4 US–Australia FTA. For a more comprehensive analysis, see Burri and Polanco, note 51.

[133] The Comprehensive and Progressive Agreement for Transpacific Partnership, available at: http://international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cptpp-ptpgp/text-texte/index.aspx?lang=eng.

[134] Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam.

[135] Z. Torrey, 'TPP 2.0: The Deal without the US: What's New about the CPTPP and What Do the Changes Mean?', *The Diplomat*, 3 February 2018.

[136] Such as provisions on domestic electronic transactions framework, personal information protection, Internet interconnection charge sharing, location of computing facilities, unsolicited commercial electronic messages, source code, and dispute settlement. See Articles 14.5, 14.8, 14.12, 14.13, 14.14, 14.17, and 14.18 CPTPP respectively.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory'. The soft language from the US–South Korea FTA on free data flows is now framed as a hard rule: '[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'.[137] The rule has a broad scope and most data that is transferred over the Internet is likely to be covered, although the word 'for' may suggest the need for some causality between the flow of data and the business of the covered person.

Measures restricting digital flows or localization requirements under Article 14.13 CPTPP 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'.[138] These non-discriminatory conditions are similar to the test formulated by Article XIV GATS and Article XX GATT, which, as earlier noted, is meant to balance trade and non-trade interests. The CPTPP test differs from the WTO norms in one significant element: while there is a list of public policy objectives in the GATT and the GATS (such as public morals or public order), the CPTPP provides no such enumeration and simply speaks of a 'legitimate public policy objective'.[139] This permits more regulatory autonomy for the CPTPP signatories. However, it also may lead to overall legal uncertainty. Further, it should be noted that the ban on localization measures is somewhat softened with regard to financial services and institutions.[140] An annex to the financial services chapter has a separate data transfer requirement, whereby certain restrictions on data flows may apply for the protection of privacy or confidentiality of individual records, or for prudential reasons.[141] Government procurement is also excluded.[142]

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.[143] This means that tailor-made products are excluded, as well as software used for critical infrastructure and those in commercially negotiated contracts.[144] The aim of this provision is to protect software

[137] Article 14.11(2) CPTPP.
[138] Article 14.11(3) CPTPP.
[139] Article 14.11(3) CPTPP.
[140] See the definition of 'a covered person' in Article 14.1, which is said to exclude a 'financial institution' and a 'cross-border financial service supplier'.
[141] The provision reads: 'Each Party shall allow a financial institution of another Party to transfer information in electronic or other form, into and out of its territory, for data processing if such processing is required in the institution's ordinary course of business'.
[142] Article 14.8(3) CPTPP.
[143] Article 14.17(2) CPTPP.
[144] Article 14.17(2) CPTPP.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

companies and address their concerns about loss of IP or cracks in the security of their proprietary code.[145]

These provisions illustrate an important development this chapter alluded to earlier, namely, the evolution of digital trade rules that go beyond the WTO and do not simply entail a clarification of existing bans on discrimination or more liberal commitments. It is also evident that the new rules do not merely set higher standards, as is generally anticipated from trade agreements; rather, they shape the regulatory space domestically and may even lower certain standards. A commitment to lower standards of protection is particularly palpable in the field of privacy and 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'. No standards or benchmarks for the legal framework have been specified, except for a general requirement that CPTPP parties 'take into account principles or guidelines of relevant international bodies'.[146] A footnote provides some clarification in saying that '[f]or greater certainty, a Party may comply with the obligation in this paragraph by adopting or 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'.[147] Parties are also invited to promote compatibility between their data protection regimes.[148] Overall, there is a priority given to trade over privacy protection. This commitment had been pushed by the United States, which subscribes to a relatively weak and patchy protection of privacy. Timewise, this insertion can be linked to the *Schrems I* judgment of the Court of Justice of European Union (CJEU) that struck down the EU–US Safe Harbor Agreement.[149]

The CPTPP contains also rules on consumer protection,[150] network neutrality[151] and spam control,[152] although these are fairly weak. The same is true for the newly

[145] It is interesting to note that China does demand access to source code from software producers selling in its market, so this provision may be interpreted as a reaction to this.
[146] Article 14.8(2) CPTPP.
[147] Article 14.8(2) CPTPP.
[148] Article 14.8(5) CPTPP.
[149] C-362/14, *Maximilian Schrems v Data Protection Commissioner and Digital Rights Ireland Ltd*, [2015], ECLI:EU:C:2015:650. Maximillian Schrems is an Austrian citizen, who filed a suit against the Irish supervisory authority (the Data Protection Commissioner), after it rejected his complaint over Facebook's practice of storing user data in the United States. The plaintiff claimed that his data was not adequately protected in light of the recent NSA revelations and this, despite the existing agreement between the EU and the United States – the 'Safe Harbor' scheme – that expressly sought to ensure that the United States provides for an adequate level of protection of the transferred personal data.
[150] Article 14.17 CPTPP.
[151] Article 14.10(a) CPTPP.
[152] Article 14.14 CPTPP.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

introduced rules on cybersecurity under Article 14.16, which identifies a relatively limited scope of activities for cooperation, in situations of 'malicious intrusions' or 'dissemination of malicious code', and capacity-building of governmental bodies dealing with cybersecurity incidents.

II *The USMCA*

After the withdrawal of the United States from the TPP, there was some uncertainty as to the direction it will follow in its trade deals in general and on matters of digital trade in particular. The renegotiated NAFTA, now referred to as 'United States–Mexico–Canada Agreement' (USMCA), casts the doubts aside. The USMCA has a comprehensive electronic commerce chapter, which is now also properly titled 'Digital Trade' and follows all critical lines of the CPTPP in ensuring the free flow of data through a clear ban on data localization (Article 19.12), providing a non-discrimination treatment for digital products (Article 19.4) and a hard rule on free information flows (Article 19.11).

The USMCA appears particularly interesting in two aspects. The first one is that it keeps the clause on exceptions that permits the pursuit of certain non-economic objectives. Article 19.11 specifies, very much in the sense of the CPTPP, 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 the measure (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective.[153] Furthermore and departing from the standard US approach, the USMCA signals abiding to some data protection principles. While Article 19.8 remains soft on prescribing domestic regimes on personal data protection, it recognizes principles and guidelines of relevant international bodies. Article 19.8 recognizes 'the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade'[154] and requires from 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

[153] Article 19.11(2). 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.

[154] Article 19.8(1) USMCA.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

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)'.[155]

The parties also recognize key principles of data protection, which include limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability,[156] and aim to provide remedies for any violations.[157] This is interesting because it may go beyond what the United States has in its national laws on data protection and also because it reflects some of the principles the European Union has advocated in the domain of the protection of privacy. One can of course wonder whether this is a development caused by the 'Brussels effect', whereby the EU 'exports' its own domestic standards and they become global,[158] or whether we are seeing a shift in US privacy protection regimes as well.[159]

Finally, three 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'[160] and has become part of the ban on requirements for the transfer or access to source code in Article 19.16. The second novum refers to the recognition of 'interactive computer services' as particularly vital to the growth of digital trade. 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'.[161] 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 IP rights' infringement.[162] It also secures the application of Section 230 of

[155] Article 19.8(2) USMCA.
[156] Article 19.8(3) USMCA.
[157] Article19.8(4) and (5) USMCA.
[158] See A. Bradford, 'The Brussels Effect', *Northwestern University Law Review* 107 (2012), 1–68; A. Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford: Oxford University Press, 2020).
[159] For a great analysis, which argues that a convergence of standards of protection is unlikely, see Chander et al., note 22; for a different opinion, see E. Büyüksagis, 'Towards a Transatlantic Concept of Data Privacy', *Fordham Intellectual Property, Media and Entertainment Law Journal* 30 (2019), 139–221.
[160] Article 19.1 USMCA.
[161] Article 19.17(2) USMCA. 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.
[162] On intermediaries' liability, see, e.g., S. K. Katyal, 'Filtering, Piracy, Surveillance and Disobedience', *The Columbia Journal of Law and the Arts* 32 (2009), 401–426; U. Gasser and W. Schulz (eds), *Governance of Online Intermediaries* (Cambridge, MA: Berkman Center for Internet and Society, 2015).

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

the US Communications Decency Act,[163] which insulates platforms from liability but has been recently under attack in many jurisdictions, including in the United States, in the face of fake news and other negative developments related to platforms' power.[164] The third and rather liberal commitment of the USMCA parties regards 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 recognize 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 endeavor to ensure that the information is in a machine-readable and open format and can be searched, retrieved, used, reused, and redistributed.'[165] 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'.[166]

The US approach towards digital trade issues has been confirmed also by the recent US–Japan Digital Trade Agreement (DTA), signed on 7 October 2019, alongside the US–Japan Trade Agreement.[167] The DTA can be said to replicate almost all provisions of the USMCA and the CPTPP,[168] including the new USMCA rules on open government data,[169] source code[170] and interactive computer services[171] but notably covering also financial and insurance services as part of the scope of agreement. A new provision has been added with regard to ICT goods that use cryptography,[172] which complements the source code provisions and is similar to

[163] 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.

[164] See, e.g., L. Feine, 'Big Tech's Favorite Law Is Under Fire', *CNBC*, 19 February 2020. For an analysis of the free speech implications of digital platforms, see J. M. Balkin, 'Free Speech Is a Triangle', *Columbia Law Review* 118 (2018), 2011–2055.

[165] Article 19.18(2) USMCA.

[166] Article 19.8(3) USMCA.

[167] 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.

[168] 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. Some things are missing in the US–Japan DTA, when compared to the USMCA – such as rules on paperless trading, net neutrality and the mention of data protection principles.

[169] Article 20 US–Japan DTA.

[170] Article 17 US–Japan DTA.

[171] Article 18 US–Japan DTA. A side letter recognizes 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.

[172] Article 21.3 US–Japan DTA.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

Annex 8-B, section A.3 of the CPTPP chapter on technical barriers to trade, which addresses practices by several countries, in particular China, that impose bans on encrypted products or set specific technical regulations that restrict the sale of such products.[173]

E CONCLUSION

The era of big data has ushered in new challenges for global trade law. Policymakers are faced with the extremely difficult task to match the existing, largely analogue-based, institutions and rules of international economic law with the dynamic, scruffy innovation of digital platforms[174] and data that flows regardless of state borders. At the same time, and this only makes the task more taxing, it is evident that the regulatory framework that will be chosen will have immense effects on innovation and the fate of the data-driven economy,[175] as well as on fundamental rights beyond the province of the economy, such as the protection of citizens' privacy. Despite the importance and the urgency of finding appropriate governance solutions, global trade law has not undergone a radical overhaul so far and legal adaptation has been slow and patchy, as this chapter showed. PTAs have become the preferred venue, where digital trade rules have been adopted – on the one hand, so as to compensate for the lack of progress under the umbrella of the WTO and on the other hand, and more importantly, so as to create new rules that address new trade barriers, such as data localization measures; new and pressing concerns, such as the acute need to interface trade and personal data protection mechanisms, and overall, to provide a regulatory environment that is conducive to the practical reality of digital trade and that provides a level of legal certainty for all actors involved. It has been the chapter's objective to provide a better understanding of this newly emerged governance landscape by tracing broader developments and trends, by looking in particular at the data-related rules across PTAs and analyzing more closely the most sophisticated templates of e-commerce chapters so far, as found in the CPTPP and the USMCA.

The understanding of the existing rules on digital trade and their evolution over time is absolutely essential for future attempts of individual states and of the

[173] See H.-W. Liu, 'Inside the Black Box: Political Economy of the Trans-Pacific Partnership's Encryption Clause', *Journal of World Trade* 51 (2017), 309–334.

[174] Y. Benkler, 'Growth-Oriented Law for the Networked Information Economy: Emphasizing Freedom to Operate Over Power to Appropriate', in Kauffman Taskforce on Law, Innovation and Growth (ed), *Rules for Growth: Promoting Innovation and Growth through Legal Reform* (Kansas City: Kauffman Foundation, 2011), 313–342; P. K. Yu, 'Trade Agreement Cats and Digital Technology Mouse', in B. Mercurio and N. Kuei-Jung (eds), *Science and Technology in International Economic Law: Balancing Competing Interests* (Abington: Routledge, 2014), 185–211.

[175] A. Chander, 'How Law Made Silicon Valley', *Emory Law Journal* 63 (2014), 639–694; see generally J. L. Zittrain, *The Future of the Internet – and How to Stop It* (New Haven, CT: Yale University Press, 2008).

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003

international community to grapple with the digital challenge. It may be important also for other governance actors, such as companies, think tanks, non-governmental organizations and even individual citizens who wish to more actively engage in the rule-making processes in trade agreements, which by definition tend to be behind closed doors and with little to none stakeholder involvement.[176] The experience gathered in PTAs may also be invaluable for the ongoing reinvigorated efforts in the WTO to reach an agreement on electronic commerce, as well as in new bolder deals that go beyond existing commitments and look at a range of emerging issues, such as digital identity, AI, electronic invoicing and open data, such as those covered under the DEPA.

As a final thought, one may stress that the data economy has placed higher demands on regulatory cooperation.[177] As the complexity of the data-driven society rises, enhanced regulatory cooperation seems indispensable for moving forward, since data issues cannot be covered by the mere 'lower tariffs, more commitments' stance in trade negotiations but entail the need for reconciling different interests and the need for oversight. In this context, while the paths for engaging in and advancing regulatory cooperation would ideally be followed in the multilateral forum,[178] preferential trade venues can serve as governance laboratories. The way forward may be truly bright but remains highly (and perhaps unfortunately so) dependent on the role that the key players, the United States, the EU and China, are willing to assume.

[176] For a general critique, see S. Cho and C. R. Kelly, 'Are World Trading Rules Passé?'. *Vanderbilt Journal of International Law* 53 (2013), 623–666, at 623–627; for a more contextualized critique, see Burri, note 27.

[177] T. J. Bollyky and P. C. Mavroidis, 'Trade, Social Preferences, and Regulatory Cooperation: The New WTO-Think', *Journal of International Economic Law* 20 (2017), 1–30, at 11–13 (Bollyky and Mavroidis discuss the need for regulatory competition in the context of global value chains; their argument is only strengthened in the domain of overall digital trade and data flows).

[178] Ibid., at 21. See also Chapter 4 in this volume.

Downloaded from https://www.cambridge.org/core. IP address: 76.65.11.162, on 09 Nov 2021 at 05:19:26, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108919234.003