Forthcoming in D. Bethlehem, D. McRae, R. Neufeld and I. Van Damme (eds) The *Oxford Handbook on International Trade Law*, 2nd edn., Oxford University Press, 2022.

Chapter 28

Privacy and data protection

Mira Burri

Abstract

Against the background of the centrality of data for contemporary economies, the chapter contributes to a better understanding and contextualization of data protection and its interfaces with global trade law. It looks at existing international, transnational, and selected national frameworks for privacy protection and briefly sketches their evolution. The chapter then explores the application of the WTO rules, which admittedly are in a pre-Internet state, to situations where privacy concerns are affected. Subsequently, the data-related frameworks of FTAs, where most of the new rule-making occurs, are explored. The chapter concludes with an appraisal of the state of affairs and an outlook on the linkages between trade law and data protection in the digital economy.

Keywords: data; cross-border data flows; digital trade; e-commerce; privacy protection; general exceptions; GDPR; CPTPP; USMCA

I. Introduction: privacy protection in the data-driven economy

To someone familiar with the origins and the evolution of international trade law, the protection of personal data and privacy would probably be a topic of marginal interest only. Indeed, most trade agreements,[1] as well as classic trade law treatises, do not cover the topic of privacy.[2] Still, it is fair to note that the link between the reality of information crossing borders and the need to protect certain national interests is not new.[3] In particular, during the late 1970s and the 1980s, as satellites, computers, and software profoundly changed the dynamics of communications, the trade-offs between allowing data to flow freely and asserting national jurisdiction became readily apparent. This was reflected in the work under the auspices of the OECD, which led to the formulation of non-binding principles that sought to balance the free flow of data with national interests in the fields of privacy and security.[4] Yet, as the OECD itself points out, while this privacy framework endured, the situation at that time is profoundly different from the data governance challenges we face today.[5] Ubiquitous digitization, powerful hardware and the Internet as interconnected networks have changed the volume, the intensity, and indeed, the nature of data flows.[6]

Data has become so essential to economic processes that it is said to be the 'new oil'.[7] Although the statement is flawed, data has undeniably risen in value. Increasingly much of modern economic activity, innovation, and growth cannot occur without data.[8] The implications of the recent phenomenon

---

[1] The GATT 1947 makes no reference to privacy and most of the FTAs up to very recently make no mention of it.

[2] See, e.g., J.H. Jackson, *The World Trading System: Law and Policy of International Economic Relations* (Cambridge, MA: MIT Press, 1989); J.H. Jackson, *The World Trade Organization: Constitution and Jurisprudence* (London: Royal Institute of International Affairs, 1998); R. Wolfrum, P. Stoll and H.P. Hestermeyer (eds), *WTO – Trade in Goods* (Leiden: Martinus Nijhoff Publishers, 2011), 1-24.

[3] See, e.g., C. Kuner, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future' *OECD Digital Economy Paper* 187 (2011); S.A. Aaronson, 'Why Trade Agreements Are Not Setting Information Free' 14 *World Trade Review* (2015) 671, at 672, 680-685.

[4] OECD, *Guidelines for the Protection of Personal Information and Transborder Data Flows* (OECD, 1980).

[5] OECD, *The OECD Privacy Framework: Supplementary Explanatory Memorandum to the Revised OECD Privacy Guidelines* (OECD, 2013).

[6] 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 K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (New York: Eamon Dolan/Houghton Mifflin Harcourt, 2013).

[7] *The Economist*, 'The World's Most Valuable Resource Is No Longer Oil, but Data', *The Economist* (6 May 2017).

[8] Manyika et al., above fn 6; N. Henke et al., *The Age of Analytics: Competing in a Data-Driven World*

of Big Data[9] are multiple and sometimes far-reaching.[10] The capacity to handle data increasingly turns into a competitive advantage for companies and countries. It plays out as a power move in the global political economy. The ongoing battle between China and the United States with regard to 5G dominance is revealing in this sense.[11]

The increased dependence on data has brought about a set of new concerns, particularly in the area of privacy protection.[12] Big Data analytics puts into question the distinction between personal and non-personal data. This is because anonymization is only of limited utility[13] and re-identification of data subjects by combining datasets of non-personal data appears possible given that data might be retained indefinitely.[14] Big Data equally questions the fundamental elements of existing privacy protection laws, often relying on transparency and user consent.[15] These challenges have not been left unnoticed and have triggered the reform of data protection laws worldwide, best exemplified by the EU General Data Protection Regulation (GDPR).[16] However, the reform initiatives are not coherent. They are also culturally and socially embedded, reflecting societies' understandings of constitutional values, relationships between citizens and the State and the role of the market. With the augmented value of data and the associated risks, governments have also sought new ways to assert control over data, notably by 'localizing' the data, its storage or suppliers within the State's sovereign space.[17] This barrier to data flows impinges directly on trade and may endanger the realization of an innovative data economy.[18] The provision of digital products and services, cloud computing applications or if we think in more future-oriented terms about the Internet of Things (IoT) and Artificial Intelligence (AI), could not function without cross-border flow of data.[19] Data protectionism also comes with a cost for the countries adopting such measures.[20]

(Washington, DC: McKinsey Global Institute, 2016).

[9] Manyika et al., above fn 6. Definitions vary with scholars agreeing only that the term Big Data is generalized and slightly imprecise. One common identification refers to Big Data's '3-Vs': volume, velocity, and variety. Increasingly, experts add a fourth 'V', the veracity or reliability of the data, and a fifth with regard to its value. See Mayer-Schönberger and Cukier, above fn 6.

[10] Mayer-Schönberger and Cukier, above fn 6. See further also 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.

[11] See, e.g., H. Sender, 'US-China Contest Centres on Race for 5G Domination', *The Financial Times* (25 January 2019).

[12] P. Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' 57 *UCLA Law Review* (2010) 1701-1777; P.M. Schwartz and D.J. Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' 86 *New York University Law Review* (2011) 1814-1894; The White House, *Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President, May 2014; 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.

[13] The White House, above fn 12, at 14.

[14] Ibid at 14-15; also Ohm, above fn 12; I.S. Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' 3 *International Data Privacy Law* (2013) 74-87, at 77.

[15] Rubinstein, above fn 14, at 78.

[16] 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 2016 L 119, p. 1.

[17] See A. Chander, 'National Data Governance in a Global Economy' *UC Davis Legal Studies Research Paper* 495 (2016), at 2; also A. Chander and U.P. Lê, 'Data Nationalism' 64 *Emory Law Journal* (2015) 677-739.

[18] United States International Trade Commission (USITC), *Digital Trade in the US and Global Economies*, Part 1, Investigation No 332-531 (Washington, DC: USITC, 2013); USITC, *Digital Trade in the US and Global Economie*s, Part 2, Investigation No 332-540 (Washington, DC: USITC, 2014). For a country survey, see Chander and Lê, above fn 17.

[19] Chander, above fn 17.

[20] See, e.g., M.F. Ferracane, 'The Costs of Data Protectionism' in M. Burri (ed), *Big Data and Global Trade Law* (Cambridge: Cambridge University Press, 2021) 63-82. For an opposing opinion, see S. Yakovleva and K. Irion, 'Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade' 10 *International Data Privacy Law* (2020) 201-221.

Against this background, the topic of privacy and data protection has become a central element in many policy debates at the trade negotiation table. This chapter seeks to provide a better understanding and contextualization of data protection and its interfaces with global trade law. It looks at existing international, transnational, and selected national frameworks for privacy protection and briefly sketches their evolution. Next, the chapter explores the application of the WTO rules, which admittedly are in a pre-Internet state, to situations where privacy concerns are affected. The chapter then looks at the data-related frameworks that have emerged in FTAs. The chapter concludes with an appraisal of the current state of affairs and an outlook on the linkages between trade law and data protection in the digital economy.

II. Legal frameworks for the protection of privacy

A. International rules for the protection of privacy

The right to privacy is established in international law and is now accepted as a fundamental human right. The core privacy principle is found in Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which guarantee individuals' protection of their personal sphere. However, the protection has not been robust. In fact, it appears that the right to privacy as an umbrella term almost accidentally found its way into those treaties and was only later enshrined in national constitutions.[21]

Over the years, the international framework for privacy has expanded. However, the Human Rights Committee has not yet developed a specific set of obligations in the domain of privacy law. It has only recognized some of its core aspects, such as the requirement that personal information requires protection against both public authorities and private entities, the need for data security, and some user rights.[22] In 1990, the UN General Assembly adopted Guidelines for the Regulation of Computerized Personal Data Files,[23] which stipulate minimum guarantees and include certain key principles of data protection, such as lawfulness, fairness, accuracy, purpose-specification, relevance, and adequacy of data collection. However, the Guidelines are non-binding. States may also depart from them for reasons of national security, public order, public health, or morality and the protection of the rights of others.[24]

The Council of Europe (CoE) has endorsed stronger and more enforceable standards of protection by virtue of Article 8 of the 1950 European Convention on Human Rights (ECHR)[25] and a rich body of case-law of the European Court of Human Rights (ECtHR). This jurisprudence has stressed the obligation of States to protect individual's privacy and the limitations of the right to privacy imposed either by key public interests or by the rights of others.[26] Different aspects of data protection were further endorsed through a number of CoE resolutions and ultimately through Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which opened for signature in 1981 and was lastly amended in 2018. The CoE is the first international body to establish legally binding minimum standards for personal data protection.[27]

B. Transnational rules for the protection of privacy: the OECD and the APEC frameworks

The OECD was the first organization to endorse principles of privacy protection, through the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, that recognize

---

[21] O. Diggelmann and M.N. Cleis, 'How the Right to Privacy Became a Human Right' 14 *Human Rights Law Review* (2014) 441-458.

[22] General Comment no. 16 on Article 17 ICCPR (Right to privacy) (1988), para 10.

[23] UN General Assembly, Resolution 45/95 of 14 December 1990.

[24] Ibid at para 6.

[25] The text of the ECHR, the additional protocols and their signatories are available at < https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c= > (last visited 10 September 2021).

[26] For a comprehensive guide to the jurisprudence, see European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence* (Strasbourg: Council of Europe, 2019).

[27] See, e.g., European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (Luxembourg: EU Publications Office, 2018), at 15-16.

both the need for and the risks of facilitating trans-border data flows.[28] Those Guidelines contain certain basic principles for national implementation and international cooperation that promote the free flow of data while also allowing legitimate restrictions.[29] The OECD Guidelines promote eight principles, applicable in both the public and the private sector, which countries should respect in developing their own privacy protection frameworks: (i) collection limitation; (ii) data quality; (iii) purpose specification; (iv) use limitation; (v) security safeguards; (vi) openness; (vii) individual participation; and (viii) accountability. They have become an essential part of all national data protection regimes developed after 1980, including the EU framework. In trying to keep pace with newer technological advances, the OECD Guidelines were revised in 2013,[30] but the core principles remained unaltered.[31]

Likewise, the 2005 APEC Privacy Framework[32] contains principles and implementation guidelines aimed at establishing effective privacy protection that avoids barriers to information flows in the APEC region of 21 countries. Building upon the Privacy Framework, APEC has developed the Cross-Border Privacy Rules (CBPR) system, which has now been formally joined by Australia, Chinese Taipei, Canada, Japan, South Korea, Mexico, Singapore, and the United States. The CBPR system does not displace a country's domestic law, nor does it demand specific changes. However, the CBPR establishes a minimum level of protection through certain compliance and certification mechanisms. It requires that participating businesses develop and implement data privacy policies and allows APEC Accountability Agents to assess their consistency with the APEC Privacy Framework. In this sense, the CBPR system is similar to the EU-US Privacy Shield because it envisages a means for self-assessment, compliance review, recognition, dispute resolution and enforcement.[33]

Although the OECD and APEC privacy frameworks are non-binding,[34] both illustrate the need for international cooperation in the field of data protection, as well as the importance of cross-border data flows as a fundament of contemporary economies.

C. National approaches to data protection: the European Union versus the United States

1. Privacy and data protection in the European Union

The European Union subscribes to a rights-based, omnibus approach to data protection. The right to privacy is a key concept in EU law. Building upon the Council of Europe's ECHR,[35] the Charter of Fundamental Rights of the European Union[36] distinguishes between the right of respect for private and family life in Article 7 and the right to protection of personal data in Article 8. This distinction reflects the heightened concern of the European Union to implement effective protection of personal data and the regulation of the transmission of such data through a positive obligation.[37] The 1995 Data Protection Directive formed an important part of this ongoing project.[38] As the regulatory environment profoundly

---

[28] OECD (1980), above fn 4; OECD, *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, 176 *OECD Digital Economy Papers* (2011), at 7.
[29] Ibid.
[30] OECD (2013), above fn 5.
[31] Ibid.
[32] APEC, *APEC Privacy Framework* (Signapore: APEC Secretariat, 2005). The APEC framework endorses the following principles: (i) preventing harm; (ii) notice; (iii) collection limitations; (iv) use of personal information; (v) choice; (vi) intergrity of personal information; (vii) security safeguards; (viii) access and correction; and (ix) accountability.
[33] N. Waters, 'The APEC Asia-Pacific Privacy Initiative' 6 *SCRIPTed: A Journal of Law, Technology and Society* (2009) 74-89.
[34] Some scholars have argued that such soft law frameworks are nonetheless far-reaching, because their implementation depends on the power of reputational constraints. See, e.g., C. Brummer, 'How International Financial Law Works (and How It Doesn't)' 99 *The Georgetown Law Journal* (2011) 257-327, at 263-272.
[35] Article 8 of the ECHR.
[36] Charter of Fundamental Rights of the European Union OJ 2010 C 83, p. 2.
[37] ECtHR, *Refah Partisi (The Welfare Party) and others v. Turkey*, App Nos. 41340/98, 41342/98, 41343/98 and 41344/98, judgment of 13 February 2003.
[38] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281, p. 31.

changed, particularly around the role of data in the economy but also in broader societal contexts, that Directive urgently required an update. Other reform triggers were a series of seminal decisions of the CJEU, which brought about important changes in existing legal practice, as well as in the overall understanding of individuals' rights protection on the Internet in Europe. In that context, the *Google Spain* case[39] coined the so-called 'right to be forgotten', giving priority to privacy over free speech and the economic rights of the information intermediaries, such as Google search. Another important case was the *Schrems I* judgment of 6 October 2015,[40] which rendered the EU-US Safe Harbor Agreement invalid and illuminated the importance of cross-border data flows, as well as the difficulties in reconciling such data flows with the fundamental right to privacy.

The GDPR serves the same purpose as the Data Protection Directive. It seeks to harmonize the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between EU Member States. The GDPR endorses a clear set of principles[41] and imposes particularly high standards of protection, including enhanced user rights (such as the mentioned right to be forgotten,[42] but also the right to transparent information,[43] the right of access to personal data;[44] the right to data portability,[45] the right to object[46] and the right not to be subject to automated decision-making, including profiling[47]). Accordingly, the GDPR envisages heightened responsibilities of entities controlling and processing data, including data protection by design and default[48] and effective penalties for non-compliance.[49] Noteworthy is also the territorial reach of the GDPR. Article 3(1) specifies that the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether the processing takes place in the EU or not. Furthermore, the GDPR may apply to a controller or processor not established in the European Union. This is when the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.[50] This substantial extension of the scope of EU data protection law is bound to have a significant impact in its implementation, as it becomes applicable to many foreign companies present in or targeting the EU market.[51]

In the context of the extraterritorial application of the GDPR, the European Commission can assess whether a third country offers 'an adequate level of data protection' with an effect for the entire European Union. This means that transfers of personal data to that third country may take place without the need to obtain any further authorization.[52] The test is somewhat strengthened post-*Schrems I*.[53] In the absence of an 'adequacy decision', as a second-best and certainly more burdensome option, a controller or processor may transfer personal data to a third country only if they provide appropriate

---

[39] Case C-131/12 *Google Spain*, EU:C:2014:317.
[40] Case C-362/14 *Schrems*, EU:C:2015:650 (*Schrems I*).
[41] Article 5 of the GDPR specifies the principle of lawfulness, fairness and transparency; the principle of purpose limitation; the principle of data minimization; the principle of accuracy; the principle of storage limitation; the principle of integrity and confidentiality; and the principle of accountability.
[42] Article 17 of the GDPR.
[43] Article 12 of the GDPR.
[44] Articles 13, 14, 15 and 19 of the GDPR.
[45] Article 20 of the GDPR.
[46] Article 21 of the GDPR.
[47] Article 22 of the GDPR.
[48] Article 25 of the GDPR.
[49] Depending on the infringement, data protection authorities can impose fines up to 20'000'000 EUR, or in the case of an undertaking, up to 4% of its total worldwide annual turnover of the preceding financial year, whichever is higher. See Article 83(5), (6) of the GDPR.
[50] Article 3(2) of the GDPR. See also European Data Protection Board (EDPB), Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.0, 12 November 2019.
[51] See, e.g., P.M. Schwartz, 'Information Privacy in the Cloud' 161 *University of Pennsylvania Law Review* (2013) 1623-1662; 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' 6 *Journal of Information Policy* (2016) 479-511.
[52] Article 45(1) of the GDPR; recital 103 in the preamble to the GDPR.
[53] Recital 104 in the preamble to the GDPR and Article 45(2) of the GDPR.

safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.[54]

2. Privacy and data protection in the United States

The United States has a fundamentally different idea of privacy protection, understood as related to the notion of 'liberty'.[55] In this sense, US privacy protection law 'focuses more on restrictions, such as the Fourth Amendment, that protect citizens from information collection and use by government rather than by private actors. In fact, private actors are often protected from such restrictions under the First Amendment'.[56] In contrast to free speech, data protection is regulated in a fragmented manner through some federal privacy laws and a great number of state laws.[57] These laws either concern the public sector only or they are information-specific or medium-specific, regulating for instance health information, video privacy or electronic communications. Although the Federal Trade Commission (FTC) may adjudicate on unfair or deceptive trade practices to discipline companies that fail to implement minimal data security measures or fail to meet privacy policies, the United States does not have an official data protection authority.[58] As a result, there is no coherent definition of personal or sensitive data. Self-regulation and best practices are the common models of privacy protection. Furthermore, data is seen as a transaction commodity, and data exports to other countries are not limited. Overall, there is a clear tendency towards liberal, market-based governance in contrast to the socially protective, rights-based approach of the European Union.[59]

3. Bridging the EU-US differences: the Safe Harbor and the Privacy Shield

Reconciling these different understandings of privacy between the two major players in the area of data governance has had many implications, including for trade law. Transatlantic data flows are of economic significance for both partners.[60] So far, these data flows have been enabled through a specific set of legal mechanisms. First, the so-called 'Safe Harbor' scheme[61] contained in essence a series of principles concerning the protection of personal data to which US undertakings subscribed on a voluntary basis.[62] However, the CJEU in the *Schrems I* judgment found that the Safe Harbor did not provide a level of protection of fundamental rights that is essentially equivalent to that guaranteed within the European

---

[54] Article 46(1) of the GDPR. Such appropriate safeguards may be provided for, by: (i) a legally binding and enforceable instrument between public authorities or bodies; (ii) binding corporate rules; (iii) standard data protection clauses adopted by the Commission; (iv) standard data protection clauses adopted by a supervisory authority and approved by the Commission; (v) an approved code of conduct with binding and enforceable commitments; or (vi) an approved certification together with binding and enforceable commitments.

[55] See, e.g., J.Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' 113 *The Yale Law Journal* (2004) 1151-1221; P.M. Schwartz and D.J. Solove, 'Reconciling Personal Information in the United States and European Union' 102 *California Law Review* (2014) 877-916.

[56] L. Downes, 'The Business Implications of the EU-U.S. Privacy Shield' *Harvard Business Review* (10 February 2016). In addition, policies around Internet freedom in the United States have continuously sought 'to preserve and expand the Internet as an open, global space for free expression, for organizing and interaction, and for commerce'. This has been recently confirmed by the White House strategy on AI. See respectively R.A. Clarke et al., *The NSA Report: Liberty and Security in a Changing World* (Princeton, NJ: Princeton University Press, 2014), at 158 and The White House, *Guidance for Regulation of Artificial Intelligence Applications*, 2019.

[57] See, e.g., I. Tourkochoriti, 'Speech, Privacy and Dignity in France and in the USA: A Comparative Analysis' 38 *Loyola of Los Angeles International and Comparative Law Review* (2016) 101-182.

[58] For a great overview of US privacy rules, see S.J. Deckelboim, 'Consumer Privacy on an International Scale' 48 *Georgetown Journal of International Law* (2017) 263-296.

[59] J.R. Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' 52 *Stanford Law Review* (2000) 1315-1371.

[60] See, e.g. M.A., Weiss and K. Archick, 'US-EU Data Privacy: From Safe Harbor to Privacy Shield' *Congressional Research Service Report* 7-5700 (2016).

[61] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000 L 215, p. 7.

[62] See H. Farrell, 'Constructing the International Foundations of E-Commerce: The EU-US Safe Harbor Arrangement' 57 *International Organization* (2003) 277-306; Schwartz and Solove, above fn 55.

Union.[63] The CJEU was particularly concerned about the fact that the Safe Harbor scheme did not bind US public authorities[64] and that no legal remedies were available.[65]

The Safe Harbor agreement was, after intense negotiations, replaced by the more stringent and detailed EU-US Privacy Shield.[66] While US companies were still to self-certify on an annual basis, the new arrangement imposed stronger obligations to protect the personal data of EU citizens according to a set of clearly defined principles.[67] In addition, the Privacy Shield envisaged stronger monitoring and enforcement, as well as certain remedies for EU citizens.[68] There was also an explicit assurance on the US side that any access of public authorities to personal data will be subject to clear limitations, safeguards and oversight; US authorities also affirmed the absence of indiscriminate or mass surveillance.[69] Despite these additional safeguards, in the 2020 CJEU judgment (*Schrems II*),[70] the CJEU invalidated the Privacy Shield arrangement.[71] The *Schrems II* decision, which has an immediate effect, exposed the difficulties in reconciling free data flows and high data protection standards. The US and EU authorities are currently back at the negotiation table and look for a new solution that can enable transatlantic data transfers, which are now only possible under a strict application of the standard contractual clauses.[72]

III. Privacy under the WTO framework

Privacy and data protection were not discussed during the Uruguay Round. Although the WTO membership recognized early on the implications of digitization for trade by launching a Work Programme on E-commerce in 1998,[73] this initiative to examine and, if needed, adjust the rules in the domains of trade in services, trade in goods, intellectual property protection and economic development did not bear any fruit over two decades. Indeed, WTO law, despite some adjustments through the Information Technology Agreement (ITA), its update in 2015, and the Trade Facilitation Agreement, which entered into force in 2017, is still very much in its pre-Internet state.[74]

WTO law nonetheless applies to online trade.[75] It also includes certain mechanisms, such as the 'general exceptions' formulated under Article XX of the GATT 1994 and Article XIV of the GATS, that are meant to reconcile economic and non-economic interests and domestic values such as privacy

---

[63] *Schrems I*, at para 97.
[64] *Schrems I*, at para 86.
[65] *Schrems I*, at paras 93-95.
[66] European Commission, Commission Implementing Decision of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of protection provided by the EU-US Privacy Shield, C(2016) 4176 final, 12 July 2016.
[67] Ibid at paras 19-29, refer to the Notice Principle, Data Integrity and Purpose Limitation Principle, Choice Principle, Security Principle, Access Principle, Recourse, Enforcement and Liability Principle, and Accountability for Onward Transfer Principle. The principles are additionally detailed in Annex II attached to the Commission's implementing decision.
[68] Ibid at paras 40, 43-63.
[69] Ibid at paras 64-90.
[70] Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (Shrems II),* EU:C:2020:559 (*Schrems II*).
[71] The Court found in particular serious risks for the rights of EU citizens due to the still persisting primacy of US law enforcement requirements over those of the Privacy Shield; the lack of necessary limitations on the power of the US authorities, particularly in light of proportionality requirements; and the lack of remedies for EU data subjects, including deficiencies in the ombudsman mechanism. See *Schrems II*, paras 168-197.
[72] See EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, adopted on 18 June 2021.
[73] WTO, Work Programme on Electronic Commerce, WT/L/274 (30 September 1998).
[74] M. Burri, 'The International Economic Law Framework for Digital Trade' 135 *Zeitschrift für Schweizerisches Recht* (2015) 10-72; WTO, *World Trade Report 2018: The Future of World Trade: How Digital Technologies Are Transforming Global Commerce* (Geneva: World Trade Organization, 2018).
[75] Panel Report, *US – Gambling*, adopted 10 November 2004; Appellate Body Report, *US – Gambling*, adopted 7 April 2005.

protection. Of specific interest is the extent to which Article XIV of the GATS may be used to justify maintaining and adopting data restrictions on the grounds of privacy protection. While Article XIV of the GATS enumerates different grounds as possible justifications,[76] those relating to (i) the protection of public order or public morals[77] and (ii) the need to act for the purpose of securing compliance with laws or regulations[78] are especially relevant. Article XIV(c)(ii) of the GATS specifies that law and regulations related to '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' fall under this category. For the purpose of showing the application of this general exception to privacy laws, we take the EU GDPR as the epitome of strong data protection standards that may impinge on digital trade and assume that the GDPR violates the market access and/or the national treatment obligations under the GATS.[79]

Article XIV of the GATS, similarly to Article XX of the GATT 1994, imposes a number of conditions: (i) the measure must fall within the scope of one of the listed objectives in the exception; (ii) the measure must address the relevant public interest at issue, with a sufficient nexus between the measure and the objective pursued;[80] and (iii) the measure must satisfy the conditions under the chapeau (the introductory paragraph) of Article XIV of the GATS. With regard to (i), WTO Members enjoy a wide margin of appreciation in their choice of objectives which they seek to protect. The second step is much more complex and triggers the so-called 'necessity' test. The Appellate Body has noted that there are different degrees of necessity. The Appellate Body has found that a 'necessary' measure is located significantly closer to the pole of 'indispensable' than to simply 'making a contribution to'.[81] The more important the interest that the measure is designed to protect and the greater the contribution to the objective, the easier it is to accept the measure as being 'necessary'.[82] However, the Appellate Body has also stated that the requirement for measures to 'relat[e] to' a goal (as is the case with the GATS privacy exception) may simply require a 'substantial' or 'reasonable' relationship of the measure to the objective pursued.[83] Furthermore, in respect of the necessity test, the 'weighing and balancing'[84] of factors should include a comparison of the challenged measure and its possible alternatives.[85] In order to show that the measure does not meet the necessity test, a claimant must demonstrate that a less trade-restrictive alternative to the measure was 'reasonably available'. The alternative measure cannot impose prohibitive costs or result in substantial technical difficulties to implement.[86] A measure that has been provisionally justified under one of the subparagraphs must also meet the condition under the chapeau

---

[76] Article XIV(b) of the GATS.

[77] Article XIV(a) of the GATS. See M. Wu, 'Free Trade and the Protection of Public Morals' 33 *Yale Journal of International Law* (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.

[78] Article XIV(c) of the GATS. See further T. Cottier, P. Delimatsis and N. Diebold, 'Article XIV GATS: General Exceptions' in R. Wolfrum et al. (eds), *Max Planck Commentaries on World Trade Law: Trade In Services, Vol. 6* (Leiden: Martinus Nijhoff Publishers, 2008) 287-328.

[79] See R.H. Weber, 'Regulatory Autonomy and Privacy Standards under the GATS' 7 *Asian Journal of WTO and International Health Law and Policy* (2012) 25-47; K. Irion, S. Yakovleva and M. Bartl, *Trade and Privacy: Complicated Bedfellows?* (Amsterdam: Institute for Information Law, 2016), at 27-33.

[80] Appellate Body Report, *US – Gambling*, adopted 7 April 2005, para 292; see also Appellate Body Report, *Brazil – Retreaded Tyres*, adopted 3 December 2007, paras 119-124.

[81] Appellate Body Report, *Korea – Beef*, adopted 11 December 2000, para 161.

[82] Appellate Body Report, *US – Gambling*, adopted 7 April 2005, para 6.536; see also Panel Report, *Argentina – Financial Services*, adopted 30 September 2015, paras 7.655, 7.685, 7.727.

[83] Appellate Body Report, *Korea – Beef*, adopted 11 December 2000, para 49, fn 104 (citing Appellate Body Report, *US – Gasoline*, adopted 29 April 1996, 19; Appellate Body Report, *US – Shrimp*, adopted 12 October 1998, para 141).

[84] See Appellate Body Report, *US – Gambling*, adopted 7 April 2005, para 78; Appellate Body Report, *China – Publications and Audiovisual Products*, adopted 21 December 2009, para 239.

[85] Appellate Body Report, *US – Gambling*, adopted 7 April 2005, para 306; Panel Report, *Argentina – Financial Services*, adopted 30 September 2015, para 7.684.

[86] Panel Report, *Argentina – Financial Services*, adopted 30 September 2015, at para 7.729 referring to Appellate Body Report, *US – Gambling*, adopted 7 April 2005, para 308.

according to which the measure should 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 in services. The chapeau has been interpreted as directed at preventing abuses or misuses of the right to invoke the exception[87] and by evaluating the 'consistency of enforcement' of the challenged measure.[88]

Admittedly, this test sets a high hurdle for WTO Members. It is regularly invoked, but the 'success rate' in meeting it has been low.[89] Scholars have argued that if the European Union would need to defend the GDPR under the GATS, it might not meet this test. First, Irion et al. have argued that the European Union might not find appropriate evidence on the performance of its data protection law.[90] For instance, the now invalidated EU-US Safe Harbor Agreement was not particularly stringent, as shown by the *Schrems I* judgment. It could be maintained that this insufficient performance undermines the strength of a challenged measure's contribution to securing compliance with EU data protection law. Second, there are arguably less trade restrictive measures reasonably available for attaining the European Union's desired level of data protection. The GDPR is in many respects excessively burdensome with sizeable extraterritorial effects.[91] Especially if compared with other data protection rules worldwide, it may be difficult to prove that privacy cannot be otherwise protected.[92] Third, even if the provisions on the transfer of personal data to third countries were deemed necessary in order to secure compliance with the GDPR, these provisions might not have been consistently implemented and would ultimately fail the chapeau test. Suppose the European Union has denied a third country's application for an adequacy assessment or a request to negotiate a sectoral scheme similar to that of the US-EU Safe Harbor or its newer version of the Privacy Shield. In that case, it seems that the chapeau test requirements are hard to meet. The European Union could be found to discriminate between different countries in finding adequate levels of protection there and in cooperating with them.[93]

Article XIV of the GATS embodies the necessary balancing that permits legitimate protections while prohibiting illegal trade protectionism. Despite the current deadlock at the WTO and the crisis of its dispute settlement system,[94] the interpretation of Article XX of the GATT 1994 and Article XIV of the GATS remains of critical importance. This is also because many FTAs and some of the recent proposals under the reinvigorated WTO E-commerce Programme and the Joint Statement Initiative[95] adopt them verbatim or *mutatis mutandis*.[96]

---

[87] Appellate Body Report, *Argentina – Financial Services*, adopted 9 May 2016, para 7.743.

[88] Appellate Body Report, *US – Gambling*, adopted 7 April 2005, para 351. In *US – Gambling*, the Appellate Body confirmed that the US ban on online gambling did not meet the requirement of the chapeau of Article XIV of the GATS due to ambiguity in relation to the scope of one US statute, which appeared to permit domestic suppliers to have remote betting services for horse racing.

[89] Only one case has so far passed all of the conditions. See Appellate Body Report, *US – Shrimp (Article 21.5 – Malaysia)*, adopted 22 October 2001.

[90] Irion et al., above fn 79, at 36-39; also D.A. MacDonald and C.M. Streatfeild, 'Personal Data Privacy and the WTO' 36 *Houston Journal of International Law* (2014) 625-652, at 640-650.

[91] See references above fn 51.

[92] L. Bygrave, *Data Privacy Law: An International Perspective* (Oxford: Oxford University Press, 2014); Arguably, this is not a very strong point, as the sole fact that other States might have less burdensome requirements might not necessarily mean that the EU measures are not necessary, given that the European Union pursues a high level of protection and other States might pursue a different level of protection.

[93] Irion et al., above fn 79, at 36-39.

[94] See, e.g., J. Pauwelyn, 'WTO Dispute Settlement Post 2019: What to Expect?' 22 *Journal of International Economic Law* (2019) 297-321.

[95] See, e.g., WTO, Joint Statement on Electronic Commerce, Communication From Brazil, INF/ECOM/27 (30 April 2019). For details on the Joint Statement Initiative, see M. Burri, 'Towards a New Treaty on Digital Trade' 55 *Journal of World Trade* (2021) 77-100.

[96] For instance, the 2020 Digital Economy Partnership Agreement (DEPA) between Chile, Singapore and New Zealand.

IV. Mapping the regulatory landscape in FTAs

A. Introduction

As negotiations in the WTO have stalled, States have turned to bilateral and regional agreements to address digital trade and data governance issues. Out of the 353 FTAs entered into between 2000 and 2020, 194 FTAs contain digital trade provisions.[97] The United States has played a key role in this process and has sought to promote liberal rules under its so-called 'Digital Agenda'.[98] Since 2002, the United States reached agreements with Australia, Bahrain, Chile, Morocco, Oman, Peru, Singapore, the Central American countries, Panama, Colombia, Korea and Japan, and has played a critical role in the formulation of newer templates under the CPTPP, the USMCA and the US-Japan Digital Trade Agreement.

All these treaties contain critical WTO-plus (by exceeding) and WTO-extra (by addressing new issues) commitments in the area of digital trade. The emergent regulatory template for digital trade is not limited to US agreements but has diffused and can be found in other FTAs as well. Singapore, Australia, Japan and Colombia have been among the major drivers of this diffusion, but the issues covered and the levels of legalization may vary substantially. Many States, such as the EFTA countries, have not yet developed and implemented distinct digital trade strategies. The European Union too has been rather cautious. In general, the European Union has mirrored in its FTAs the level of commitments under the GATS, including only a few and mostly cooperation-type of provisions in the area of digital trade.[99] It is only very recently that the European Union has addressed data flow issues. In this section, we map the emerging regulatory landscape in particular with regard to data-relevant norms.[100]

B. Overview of data-related rules in FTAs

Trade rules are relevant for data and data flow, for at least three reasons: (i) they regulate the cross-border flow of data by regulating trade in goods and services and the protection of intellectual property; (ii) they may require certain beyond-the-border rules that demand changes in domestic regulation – for example, with regard intermediaries' liability or data protection; and (iii) finally, they can limit the policy space that regulators have at home.[101] In this sense, it is useful to take into account the entire set of rules that regulate infrastructure (e.g. rules on communication networks and services, and IT hardware), as well as those rules that apply for applications and content (such as computer and audiovisual services), to understand the existing regulatory environment with regard to data flows.[102] In addition to this generic trade law framework, the last decade has also witnessed the emergence of entirely new rules that explicitly regulate data flows. This section focuses especially on the latter type of rules.

At the outset, it should be noted that despite the widespread rhetoric around the term of data flows and its frequent use in reports and studies,[103] in the trade policy discourse and the treaty language, no clear definition can be found. However, despite the fact that different terms are used in various agreements, there seems to be a tendency towards a broad and encompassing definition of data flows. Specifically, (i) where data forms part of the provision of a service or a product and (ii) where this data crosses borders, even if the data flows do not neatly coincide with one commercial transaction and the

---

[97] For a review of all digital trade related trends in FTAs, see M. Burri, 'Data Flows and Global Trade Law' in M. Burri (ed) *Big Data and Global Trade Law* (Cambridge: Cambridge University Press, 2021), 11-41.

[98] S. Wunsch-Vincent, 'The Digital Trade Agenda of the US' 1 *Aussenwirtschaft* (2003) 7-46.

[99] For details, see M. Burri, 'The Regulation of Data Flows in Trade Agreements' 48 *Georgetown Journal of International Law* (2017) 408-448.

[100] This analysis is based on a dataset of all data-relevant norms in trade agreements (TAPED). See M. Burri and R. Polanco, 'Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset' 23 *Journal of International Economic Law* (2020) 187-220 and < http://unilu.ch/taped > (last visited 10 September 2021).

[101] See, in this sense, M. Burri, 'The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation' 51 *UC Davies Law Review* (2017) 65-132; F. Casalini and J. López González, 'Trade and Cross-Border Data Flows' 220 *OECD Trade Policy Papers* (2019).

[102] For a fully-fledged analysis of these rules, see Burri (2015), above fn 74.

[103] See, e.g., Casalini and González, above fn 101; OECD, *Trade and Cross-border Data Flows*, Trade Policy Brief, June 2019.

provision of certain services may relate to multiple flows of data. In addition, it may be noted that so far there has not been a distinction between different types of data – for instance, between personal and non-personal data, personal and company data or machine-to-machine data.[104] Yet, personal information is commonly included explicitly in the data-related provisions of FTAs (e.g., the CPTPP and the USMCA speak of the 'cross-border transfer of information by electronic means, including personal information'[105]), whereby the potential clashes with domestic data protection regimes become evident.

Data-related provisions are a relatively new phenomenon and can be found primarily in the dedicated e-commerce chapters of FTAs. Relevant provisions on the cross-border flow of data can also be found in chapters dealing with discrete services sectors, like telecommunications and financial services, as shown in Table 1 below.

Table 1. Overview of data-related provisions in FTAs (2000-2020)[106]

	Provisions in e-commerce chapters	**Financial services**	**Telecommunication services**	**Data localization**
Soft commitments	11	0	2	1
Intermediate commitments	8	0	1	0
Hard commitments	14	80	70	16
Total number	**33**	**80**	**73**	**17**

3. Rules on data flows

There has been a sea change over the years in the number and type of data flow provisions in FTAs. Non-binding provisions on data flows appeared quite early. 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 obligation. 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'.[107] Similar soft wording is used in the 2008 Canada-Peru FTA,[108] the 2011 Korea-Peru FTA[109] the 2011 Central America-Mexico FTA,[110] the 2013 Colombia-Costa Rica FTA,[111] the 2013 Canada-Honduras FTA,[112] the 2014 Canada-Korea FTA[113] and

[104] For some attempts to classify data, see N. Sen, 'Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?' 21 *Journal of International Economic Law* (2018) 323-348; S. Ariel Aaronson and P. Leblond, 'Another Digital Divide: The Rise of Data Realms and its Implications for the WTO' 21 *Journal of International Economic Law* (2018) 245-272; OECD, *Data in the Digital Age*, Policy Brief, March 2019.
[105] Article 14.11 of the CPTPP; Article 19.11 of the USMCA.
[106] For information on the collected data, see above fn 100.
[107] Article 14.05(c) of the Nicaragua-Taiwan FTA.
[108] Article 1508(c) of the Canada-Peru FTA.
[109] Article14.9(c) of the Korea-Peru FTA.
[110] Article 15.5(d) of the Central America-Mexico FTA.
[111] Article 16.7(c) of the Colombia-Costa Rica FTA.
[112] Article 16.5(c) of the Canada-Honduras FTA.
[113] Article 13.7(c) of the Canada-Korea FTA.

the 2015 Japan-Mongolia FTA.[114]

A more explicit commitment, albeit still of soft law nature, can be found in the 2007 South Korea-US FTA, where the parties, after 'recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information', agreed that they 'shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders'.[115] More recently, different parties have agreed to consider in future negotiations commitments related to cross-border flow of information. Such a clause is notably found in the 2018 EU-Japan EPA and in the modernization of the trade part of the EU-Mexico Global Agreement, which has signalled the repositioning of the European Union in the data flows debates. Within three years of the entry into force of the agreement, the parties pledge to 'reassess' the need to include provisions on the free flow of data into the treaty.[116]

The first binding provision on cross-border information flows is in 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'.[117] A more detailed provision was negotiated in the 2016 TPP – the text was then replicated in the amended PAAP[118] and the CPTPP and has influenced all subsequent data flows provisions.[119]

4. Data localization

In recent years, some FTAs have also included provisions on data localization, either prohibiting the practice or limiting it. Unlike most data flows provisions, data localization provisions are binding. The first agreement with data localization provisions is the 2015 Japan-Mongolia FTA, which included an article prohibiting measures that require computing facilities to be located in a party's territory.[120] In 2016, the TPP included a hard ban on localization. The CPTPP, the PAAP and the USMCA replicated this prohibition in full. The localization ban has diffused and become part of other agreements, such as the 2016 Chile-Uruguay FTA[121] and the 2016 Updated SAFTA,[122] closely following the CPTPP template. One of the few non-binding provisions on data localization is found in the 2017 Argentina-Chile FTA. In this FTA, the parties recognize the importance of not requiring a person of the other party to use or locate the computer facilities as a condition for conducting business in that territory and pledge to exchange good practices regarding servers' location.[123] The recent Regional Comprehensive Economic Partnership (RCEP), which includes for the first time commitments of China on data-related issues, provides only for conditional data flows and data localization, while preserving a lot of policy space for domestic policies, which very well may be of data protectionist nature.[124]

5. Privacy and data protection

103 FTAs so far include provisions on privacy, usually under the concept of 'data protection'. Yet, the levels of protection vary considerably, including both binding and non-binding provisions (see Table 2), which is symptomatic of the different positions of the major actors and the inherent tensions between the regulatory goals of data innovation and data protection.

---

[114] Article 9.12.5 of the Japan-Mongolia FTA.
[115] Article 15.8 of the Korea-US FTA.
[116] Article 8.81 of the EU-Japan EPA and Article XX of the EU-Mexico Modernised Global Agreement.
[117] Article 14.10 of the Mexico-Panama FTA.
[118] Article 13.11 of the PAAP (2015).
[119] Such as the 2016 Chile-Uruguay FTA, the Updated Singapore-Australia FTA, the 2017 Argentina-Chile FTA, the 2018 Singapore-Sri Lanka FTA, the 2019 Australia-Indonesia FTA and the USMCA.
[120] Article 9.10 of the Japan-Mongolia FTA.
[121] Article 8.11 of the Chile-Uruguay FTA.
[122] Chapter 14 Article 15 of the SAFTA.
[123] Article 11.7 of the Argentina-Chile FTA.
[124] Articles 12.14 and 12.15 of the RCEP.

Table 2. Overview of privacy-related provisions in FTA e-commerce chapters

Total N° of provisions	**103**
Soft commitments	20
Intermediate commitments	73
Hard commitments	10

Earlier agreements dealing with privacy issues consist of side declarations that are of programmatic and non-binding nature. The 2000 Jordan-US FTA Joint Statement on Electronic Commerce refers to the need of ensuring the effective protection of privacy regarding the processing of personal data on global information networks. However, parties remain flexible and should merely encourage the private sector to develop and implement enforcement mechanisms, recommending the OECD Privacy Guidelines as an appropriate basis for policy development.[125] Later agreements include cooperation activities on enhancing the security of personal data to improve the level of protection of privacy in electronic communications and avoid obstacles to trade that require personal data transfers. These activities include sharing information and experiences on domestic data protection frameworks or technical assistance in the form of exchange of information and experts, research and training activities, or joint programmes.[126]

FTAs have also dealt with personal data protection with reference to the adoption of domestic standards. In several treaties, parties have committed to adopting or maintaining legislation or regulations that protect the personal data or privacy of users.[127] Some agreements include qualifications of this commitment that secures some flexibility, in the sense that each party shall take measures it deems appropriate and necessary considering the differences in existing systems for personal data protection,[128] or that the parties have the right to define or regulate their own levels of protection of personal data in the pursuit of public policy objectives.[129] Some FTAs add that in the development of online personal data protection standards, each party must take into account the existing international standards (often however without mentioning these explicitly),[130] and criteria or guidelines of relevant international organizations or bodies[131] – such as the APEC Privacy Framework and the OECD Privacy Guidelines.[132] Moreover, in a handful of treaties, the parties commit to publishing information on the personal data protection it provides to users of e-commerce,[133] including how individuals can use remedies and how businesses can comply with any legal requirements.[134] Certain treaties add that the parties will encourage the use of encryption or security mechanisms for users' information, and the

[125] Article II of the Jordan-US FTA, Joint Statement on Electronic Commerce (7 June 2000).
[126] See, e.g., Articles 8.7.4 and 8.13(b) of the Chile-Uruguay FTA; Article 13.7(b) of the Canada-Korea FTA; Article 13.10.2 of the Australia-Japan FTA; Article 82.2(a) of the Japan-Switzerland FTA.
[127] See, e.g., Article 13.7.2 of the Australia-Indonesia FTA; Article 10.8.2 of the Brazil-Chile FTA; Article 19.8.1-2 of the USMCA.
[128] See, e.g., Article 12.8.1 of the Australia-China FTA; Article 11.7.1(j) of the Chile-Thailand FTA.
[129] Articles 18.1.2(h) and 18.16.7 of the EU-Japan EPA.
[130] See, e.g., Article 8.57.4 of the EC-Singapore FTA. Article 11.5.1-2 of the Argentina-Chile FTA notes in a footnote that: 'For greater certainty, the Parties shall understand that the collection, treatment and storage of personal data will be carried out following the general principles of prior consent, legitimacy, purpose, proportionality, quality, security, responsibility and information'. The EU tends to view the CoE Convention 108 as the relevant international standard.
[131] See, e.g., Article 13.7.3 of the Australia-Indonesia FTA; Article 14.8.2 of the TPP/CPTPP; Article 19.6 of the Colombia-Panama FTA; Article 1106 of the Australia-Thailand FTA.
[132] Article 19.8.2 of the USMCA.
[133] Article 10.8.4 of the Brazil-Chile FTA.
[134] See, e.g., Article 19.8.5 of the USMCA; Chapter 14, Article 9.4 of the Australia-Singapore FTA (2016); Article 8.7.3 of the Chile-Uruguay FTA; Article 14.8.4 of the TPP/CPTPP.

dissociation or anonymization, in cases where the said data is provided to third parties.[135]

Yet, FTA 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 protection of confidentiality of individual records as an exception in specific chapters of the agreement – such as for trade in services,[136] investment or establishment,[137] movement of persons,[138] telecommunications,[139] and financial services.[140] Certain agreements, mostly EU-led, have special chapters on the 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 to ensure an adequate level of data protection.[141] The 2018 USMCA is the first (and so far the only[142]) US-led FTA to include the key principles of data protection.[143] A second option lets countries adopt appropriate measures to ensure privacy protection while allowing the free movement of data, establishing a criterion of 'equivalence' – in the sense that personal data may be exchanged only where the receiving party undertakes to protect such data in at least an equivalent way. This has mainly been the EU approach, and to that end, parties commit to inform each other of their applicable rules and negotiate reciprocal, general or specific agreements.[144] This EU approach has been particularly strengthened in its most recent trade deals, best exemplified by the post-Brexit Trade and Cooperation Agreement (TCA) with the United Kingdom,[145] which while permitting free data flows and banning data localization, asserts privacy as a fundamental human right and binds the parties to the high standards of protection under the GDPR.[146] A third, but less used option, leaves the development of rules on data protection to a treaty body.[147]

The following sections look more closely at the most advanced template for digital trade endorsed by the CPTPP and slightly further developed by the USMCA.

6. The CPTPP and the USMCA

The Comprehensive and Progressive Agreement for Transpacific Partnership (CPTPP, also known as the TPP11 or TPP 2.0) was agreed in 2017 between eleven countries in the Pacific Rim.[148] It entered into force on 30 December 2018. The chapter on e-commerce created the most comprehensive template in the landscape of FTAs. It includes new features, 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.[149] Despite the United States having dropped out of the agreement, the chapter reflects its efforts to secure obligations on digital trade and is a verbatim reiteration of the TPP chapter.

---

[135] See, e.g., Article 10.8.6 of the Brazil-Chile FTA; Article 8.7.5 of the Chile-Uruguay FTA.
[136] Article 69.1(c) of the Japan-Singapore FTA.
[137] Article 135.1(e)(ii) of the Chile-EC AA; Article 83.1(c)(ii) of the Japan-Singapore FTA.
[138] Article 95.1(c)(ii) of the Japan-Singapore FTA.
[139] See, e.g., Article 18.3.4 USMCA; Article 8.44.4 of the EU-Japan EPA; Article 12.4.4 of the Australia-Peru FTA; Article 8.3.4 of the Singapore-Sri Lanka FTA.
[140] See, e.g., Annex 17-A of the USMCA; Article 8.63 of the EU-Japan EPA.
[141] See, e.g., Chapter 6, Articles 197-201 of the CARIFORUM-EC EPA.
[142] The subsequent US-Japan Digital Trade Agreement does not include reference to such principles.
[143] Article 19.8.3 of the USMCA.
[144] See, e.g., Articles 9.2 and 11.1 of the EC-Singapore FTA; Article 10 of Protocol on Mutual Administrative Assistance on Custom Matters, EC-Ghana EPA.
[145] Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, OJ 2020 L 444, p. 14. Similar templates have been also followed in the current negotiations with Australia, New Zealand and Tunisia.
[146] See M. Burri, 'Interfacing Privacy and Trade' 53 *Case Western Law Review* (2021) 35-88.
[147] Article 109(b) of the Colombia-EC-Peru FTA.
[148] Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam.
[149] Articles 14.5, 14.8, 14.12, 14.13, 14.14, 14.17 and 14.18 of the CPTPP, respectively.

The CPTPP explicitly prohibits the parties from requiring a 'covered person to use or locate computing facilities in that party's territory as a condition for conducting business in that territory'.[150] The soft language on free data flows found in the US- Korea FTA is 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'.[151] 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. The prohibition on localization measures is somewhat softened with regard to financial services.[152] Furthermore, government procurement is excluded from the scope of the e-commerce chapter.[153]

Measures restricting digital data 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'. Moreover, they cannot 'impose restrictions on transfers of information greater than are required to achieve the objective'.[154] These non-discriminatory conditions are similar to the test formulated by Article XIV of the GATS and Article XX of the GATT 1994. Still, they differ from the WTO exceptions in that they apply to any 'legitimate public policy objective', not just to the objectives enumerated in the WTO general exceptions.[155] This permits more regulatory autonomy for the CPTPP signatories. Legal uncertainty may, however, be compromised. Perhaps a better solution to the reconciliation mechanism dilemma is offered by the more recent Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand and Singapore. The DEPA restates the texts of Article XIV of the GATS and Article XX of the GATT 1994 and parties pledge to apply them *mutatis mutandis*.[156]

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'.[157] Parties are also invited to promote compatibility between their data protection regimes, by essentially treating lower standards as equivalent,[158] which seems to give some priority to economic over privacy rights and reflects the US stance on these issues.

After the United States' withdrawal from the TPP, there was some uncertainty as to the direction, which the United States would follow in its trade deals in general and on matters of digital trade in particular. The renegotiated NAFTA, which is now referred to as 'United States Mexico Canada Agreement' (USMCA), casts the doubts aside. It 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 regime for digital products (Article 19.4) and a hard rule on free information flows (Article 19.11).

The USMCA is particularly interesting in two aspects. First, it contains a CPTPP-like exceptions clause in Article 19.11 that parties may adopt or maintain a measure inconsistent with the free flow of data provision, if this is necessary to achieve a legitimate public policy objective. However, this is if the

---

[150] Article 14.13(2) of the CPTPP.

[151] Article 14.11(2) of the CPTPP.

[152] An annex to the Financial Services chapter has a separate data transfer requirement, whereby certain restrictions on data flow may apply for the protection of privacy or confidentiality of individual records, or for prudential reasons.

[153] Article 14.8(3) of the CPTPP.

[154] Article 14.11(3) of the CPTPP.

[155] Article 14.11(3) of the CPTPP.

[156] Article 13.1 of the DEPA.

[157] Article 14.8(2) of the CPTPP. Footnote 6 provides some clarification: '[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'.

[158] Article 14.8(5) of the CPTPP.

measure: (i) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (ii) does not impose restrictions on transfers of information greater than are necessary to achieve the objective.[159] Furthermore, and departing from the standard US approach, the USMCA signals abiding to some data protection principles. While Article 19.8 USMCA remains soft on prescribing domestic standards, it states that '… in the development of its legal framework for the protection of personal information, each party should take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)'.[160] The parties also recognize that key principles of data protection that include: limitation on collection, choice, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation, and accountability,[161] and aim to provide remedies for any violations.[162] This is interesting because it may go beyond US data protection laws and also because it reflects some of the principles the European Union has advocated in the domain of privacy protection. One wonders whether this is a development caused by the so-called 'Brussels effect', whereby the European Union 'exports' its own domestic standards and they become global[163] (also because many major US digital companies have in the meantime become GDPR-compliant) or whether this is triggered by domestic factors driving the US privacy law reform, such as the far-reaching California Consumer Privacy Act.[164]

V. Conclusions

The era of Big Data has ushered in new challenges for trade law. Policy-makers are faced with the difficult task of matching the existing, largely analogue-based, institutions and rules of international economic law with the dynamic innovation of digital platforms[165] and data that flows regardless of State borders. At the same time, and this only makes the task more taxing, the regulatory framework that will be chosen will have immense effects on innovation and the fate of the data-driven economy, 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, trade law has not undergone a radical overhaul so far, and legal adaptation has been slow and patchy.

FTAs have become the preferred venue for new digital trade rules in response to the lack of progress within the WTO. The new rules address trade barriers, such as data localization measures, as well as new and pressing concerns, such as the acute need to interface trade and personal data protection mechanisms. Overall, they provide a regulatory environment with some level of legal certainty for all actors that is conducive to the practical reality of digital trade. Trade policy can promote trade and innovation despite varying standards for privacy protection, but there is a clear demand for enhanced regulatory cooperation.[166] As the complexity of the data-driven society rises, such regulatory

---

[159] Article 19.11(2). A footnote attached 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.

[160] Article 19.8(2) of the USMCA.

[161] Article 19.8(3) of the USMCA.

[162] Article19.8(4) and (5) of the USMCA.

[163] See A. Bradford, 'The Brussels Effect' 107 *Northwestern University Law Review* (2012) 1-68; A. Bradford, *The Brusself Effect: How the European Union Rules the World* (Oxford: Oxford University Press, 2020).

[164] See A. Chander, M.E. Kaminski and W. McGeveran, 'Catalyzing Privacy Law' 105 Minnesota Law Review (2021) 1733-1802.

[165] 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.

[166] T.J. Bollyky and P.C. Mavroidis, 'Trade, Social Preferences, and Regulatory Cooperation: The New WTO-Think' 20 *Journal of Inernational Economic Law* (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 digital trade); also U. Ahmed, 'The Importance of Cross-Border Regulatory Cooperation in the Era of Digital

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,[167] preferential trade venues can serve as governance laboratories.[168]

Further reading

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

M. Burri, *Big Data and Global Trade Law* (Cambridge: Cambridge University Press, 2021)

M. Burri, 'Interfacing Privacy and Trade' 53 *Case Western Law Review* (2021) 35-88

M. Burri and T. Cottier (eds), *Trade Governance in the Digital Age* (Cambridge: Cambridge University Press, 2010)

M. Burri and R. Polanco, 'Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset' 23 *Journal of International Economic Law* (2020) 1-34

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' 6 *Journal of Information Policy* (2016) 479-511

S.J. Deckelboim, 'Consumer Privacy on an International Scale' 48 *Georgetown Journal of International Law* (2017) 263-296.

K. Irion, S. Yakovleva, and M. Bartl, *Trade and Privacy: Complicated Bedfellows?* (Amsterdam: Institute for Information Law, 2016)

WTO, *World Trade Report 2018: The Future of World Trade: How Digital Technologies Are Transforming Global Commerce* (Geneva: WTO, 2018)

Trade' 18 *World Trade Review* (2019) 99-120.

[167] Bollyky and Mavroidis, ibid, at 21.

[168] See, e.g., A. Mattoo and J.P. Meltzer, 'Data Flows and Privacy: The Conflict and Its Resolution' 21 *Journal of International Economic Law* (2018) 769-789; Burri, above fn 146.