Published in: Klaus Mathis and Avishalom Tor (eds) *Law and Economics of Regulation* (Berlin: Springer, 2021), 129–158.

Data flows versus data protection:
Mapping existing reconciliation models in global trade law

MIRA BURRI*

A. Introduction: trade and privacy protection in the data-driven economy

Privacy protection is not necessarily a theme of direct relevance for international trade law. Trade treaties,[1] as well as classic trade law treatises, do not cover the topic of privacy.[2] The interface between trade and data protection became only relevant with technological advances, which permitted the easy flow of information across borders and exposed the tensions between economic and non-economic interests.[3] During the late 1970s and the 1980s, as satellites, computers and software deeply changed the dynamics of communications, the trade-offs between allowing data to flow freely and asserting national jurisdiction became readily apparent. Some states, echoing the concerns of large multinational companies, started to worry that barriers to information flows may seriously hinder economic activities and looked for mechanisms that can prevent the erection of such barriers. It was clear that some sort of a balancing mechanism was needed. Such a mechanism was found, in a soft legal form, in the principles elaborated under the auspices of the Organisation for Economic Co-operation and Development (OECD).[4] Yet, as the OECD itself points out, while this privacy framework endured and will be briefly discussed later in this chapter, the situation then is profoundly different from the challenges in the realm of data governance we face today.[5] Ubiquitous digitization and powerful hardware, coupled with the societal embeddedness of the Internet, have changed the volume, the intensity, and indeed, the nature of data flows.[6]

The value of data and Big Data,[7] as well as the risks associated with data collection, data

* Senior Lecturer, University of Lucerne. Contact: mira.burri@unilu.ch.

[1] The General Agreement on Tariffs and Trade (GATT) 1947 makes no reference to privacy and most of the free trade agreements 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, W.J. Davey and A.O. Sykes, *Legal Problems of International Economic Relations* (St. Paul, MN: West Group, 1995); 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. 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.

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

[5] OECD, The OECD Privacy Framework: Supplementary Explanatory Memorandum to the Revised OECD Privacy Guidelines (Paris: 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); J.E. Cohen, 'What Privacy Is For', *Harvard Law Review* 126 (2013), 1904–1933; N.M. Richards and J.H. King, 'Big Data Ethics', *Wake Forest Law Review* 49 (2014), 393–432.

[7] There are no clear definitions of small versus Big Data. Definitions vary and scholars seem to agree that the term

Electronic copy available at: https://ssrn.com/abstract=3947049

processing, its use and re-use, by both companies and governments, have dramatically changed. On the one hand, data has become so essential to economic processes that it is said to be the 'new oil',[8] and although this is a flawed statement, since data is not exhaustible and may lose its value over time,[9] it shows well the high value associated with it. Like other factors of production, such as natural resources and human capital, it is increasingly the case that much of modern economic activity, innovation and growth cannot occur without data.[10] Studies have revealed the vast potential of data as a trigger for more efficient business operations and highly innovative solutions in all areas of societal life.[11] Emerging technologies, like Artificial Intelligence (AI), are highly dependent on data inputs as well, so the future of the data-driven economy is in many aspects at stake.[12] Companies as well as governments are therefore encouraged to use the potential of data and to mobilize their resources aptly, so as to make the data-driven economy real.[13]

On the other hand, the increased dependence on data has brought about a new set of concerns. The impact of data collection and use upon privacy has been particularly widely acknowledged by scholars and policy-makers alike, as well as felt by regular users of digital products and services.[14] The risks have only been augmented in the era of Big Data and AI, which presents certain distinct challenges to the protection of personal data and by extension to the protection of personal and family life. For starters, 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.[15] On the other hand,

---

of Big Data is generalized and slightly imprecise. One common identification of Big Data is through its 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. See Mayer-Schönberger and Cukier, above note 6, 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.

[8] *The Economist*, 'The World's Most Valuable Resource Is No Longer Oil, but Data', print edition, 6 May 2017.

[9] Among other arguments, see Burri, above note 7; for a fully analysis, see L. Henry Scholz, 'Big Data Is Not Big Oil: The Role of Analogy in the Law of New Technologies', *Tennessee Law Review* 86 (2019), 863–893.

[10] Manyika et al., above note 6.

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

[12] K. Irion and J. Williams, Prospective Policy Study on Artificial Intelligence and EU Trade Policy (Amsterdam: The Institute for Information Law, 2019); The Royal Society, *Machine Learning: The Power and Promise of Computers That Learn by Example* (London: The Royal Institute, 2017).

[13] See e.g. Manyika et al., above note 6; Henke et al., above note 11; J. Bughin et al., *Digital Europe: Pushing the Frontier, Capturing the Benefits* (Washington, DC: McKinsey Global Institute, 2016).

[14] 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*, Executive Office of the President, May 2014; U. Gasser, 'Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy', *Harvard Law Review* 130:2 (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.

[15] The White House, ibid., at 14.

Electronic copy available at: https://ssrn.com/abstract=3947049

Big Data analytics enable the re-identification of data subjects by using and combining datasets of non-personal data, especially as data is persistent and can be retained indefinitely.[16] Big Data also puts into question the fundamental elements of existing privacy protection laws, which often operate upon requirements of transparency and user consent.[17] Equally is data minimization as another core idea of privacy protection challenged, as firms are 'hungry' to get hold of more data, and the sources of data from smart devices, sensors and social networks interactions multiply.[18] These challenges have not been left unnoticed and have triggered the reform of data protection laws around the world, best exemplified by the EU General Data Protection Regulation (GDPR).[19] 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, as it is illustrated with the discussion of the differences between the US and the EU approaches to data protection that follows later in the chapter.

With the increased value of data and the associated risks, governments have sought new ways to assert control over it – in particular by prescribing diverse measures that 'localize' the data, its storage or suppliers, so as to keep it within the state's sovereign space.[20] This kind of erecting barriers to data flows impinges directly on trade and may endanger the realization of an innovative data economy.[21] The provision of any digital products and services, cloud computing applications, or the development of the Internet of Things (IoT) and AI, are impossible under restrictions on cross-border flows of data.[22] Data protectionism may also be associated with certain costs for the economy that endorses it.[23]

Overall, with the increased role of data in societies, the interfaces between trade and privacy protection have become multiple and intensified, and raise important questions as to adequate regulatory design that can reconcile economic and non-economic concerns, national and international interests. This chapter is set against this complex backdrop and seeks to provide a better understanding and contextualization of the theme of data protection and its interfaces with global trade law. It addresses this task by looking first at the existing international, transnational and selected national frameworks for privacy protection and briefly sketches their evolution over time. In a second step, the chapter explores the application of the rules of the World Trade Organization (WTO), which admittedly are in a pre-Internet state, to situations where privacy concerns are affected. The chapter then looks at the data-relevant and data protection rules that have emerged in preferential trade venues with a focus on the reconciliation mechanisms that these treaties provide. The chapter concludes with an appraisal of the current

---

[16] The White House, ibid., at 14–15; also Ohm, above note 14; I.S. Rubinstein, 'Big Data: The End of Privacy or a New Beginning?', *International Data Privacy Law* 3 (2013), 74–87, at 77.

[17] Rubinstein, ibid., at 78.

[18] Tene and Polonetsky, above note 14.

[19] 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*).

[20] 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', *Emory Law Journal* 64 (2015), 677–739.

[21] 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 note 20.

[22] See A. Chander, 'National Data Governance in a Global Economy', *UC Davis Legal Studies Research Paper* 495 (2016), at 2.

[23] 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, forthcoming 2020); R.D. Taylor, '"Data localization": The Internet in the Balance', *Telecommunications Policy* 44 (2020), 102003.

Electronic copy available at: https://ssrn.com/abstract=3947049

state of affairs and some thoughts on the pros and cons of the available legal solutions for reconciling trade and privacy protection.

B. Legal frameworks for the protection of privacy

I. International rules for the protection of privacy

The right to privacy is established in international law and is now commonly referred to as one of the fundamental human rights to which every human being should be entitled. The core privacy principle can be found in Art. 12 of the Universal Declaration of Human Rights (UDHR),[24] and the right to privacy was given formal legal protection in Art. 17 of the International Covenant on Civil and Political Rights (ICCPR), which guaranteed individuals protection of their personal sphere as broadly conceived.[25] But the protection has not been robust and some scholars have shown by looking at the negotiation histories of the UDHR and the ICCPR that the right to privacy as an umbrella term almost accidentally found its way into the treaties and was only later enshrined in national constitutions.[26] Over the years, the international framework for privacy has expanded, in particular due to the effects of new technologies and the new perils they may bring to data protection. Despite the fact that the Human Rights Committee has not yet developed a specific set of obligations in the domain of privacy law, it did recognize some of its core aspects, such as that personal information ought to be protected against both public authorities and private entities, the need for data security, the right of data subjects to be informed about the processing of their data and the right to rectification or elimination of unlawfully obtained or inaccurate data.[27] In 1990, the UN General Assembly also adopted Guidelines for the Regulation of Computerized Personal Data Files[28] that stipulate minimum guarantees and include certain key principles of data protection, such as lawfulness, fairness, accuracy, purpose-specification, relevance and adequacy of data collection and processing and data security. The Guidelines are however of non-binding nature and states may depart from the mentioned principles for reasons of national security, public order, public health or morality and the rights of others.[29]

The Council of Europe (CoE) has played an important role in the evolution of the international regime by endorsing stronger and enforceable standards of human rights' protection in its forty-seven members through the 1950 European Convention on Human Rights (ECHR),[30] and in particular through the body of case-law developed by the European Court of Human Rights (ECtHR) on Art. 8.[31] This jurisprudence not only stressed the obligations of states to protect individual's privacy but also importantly clarified the limitations of the right to privacy imposed

---

[24] 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks'.

[25] The text of Art. 17 is identical with Art. 12 UDHR but the two sentences are framed as separate paragraphs.

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

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

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

[29] Ibid., para. 6.

[30] The text of the ECHR, the additional protocols and their signatories are available here: https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=.

[31] Art. 8 'Right to respect for private and family life' reads:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Electronic copy available at: https://ssrn.com/abstract=3947049

either by key public interests or by the rights of others.[32] 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.[33] The CoE is the first international instrument that established minimum standards for personal data protection in a legally binding manner.[34]

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

As earlier mentioned, the OECD was the first organization to endorse principles of privacy protection in recognizing both the need to facilitate trans-border data flows as a basis for economic and social development and the related risks. [35] The 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[36] sought to achieve this balance by agreeing upon certain basic principles of national and international application, which, while keeping free data flows permitted legitimate restrictions, and by offering bases for national implementation and international cooperation.[37] The OECD Guidelines endorse in particular eight principles, applicable in both the public and the private sector, along which countries should develop their own privacy protection frameworks. These principles are: (1) collection limitation; (2) data quality; (3) purpose specification; (4) use limitation; (5) security safeguards Principle; (6) openness; (7) individual participation; (8) accountability, and have become an essential part of all national data protection regimes that were developed later on, including the EU framework, which is discussed in more detail in the next section. In trying to keep pace with newer technological advances, the OECD Guidelines were revised in 2013[38] but these core principles remained unaltered; added were a number of new concepts, including: national privacy strategies; privacy management programmes; and data security breach notification, which again permit for flexibility in implementation but recognize the newer demands from governments to approach data protection as an ever more important topic. Two features remain key to the OECD Guidelines and these are the focus on the practical implementation of privacy protection through an approach grounded in risk management and the need to address the global dimension of privacy through improved interoperability.[39]

The 2005 APEC Privacy Framework[40] is in many ways similar to the OECD Privacy Guidelines[41] and contains a set of principles and implementation guidelines that were created in order to establish effective privacy protection that avoids barriers to information flows in the Asia Pacific Economic Cooperation (APEC) region of 21 countries. Building upon the Privacy Framework, APEC has developed the Cross-Border Privacy Rules (CBPR) system, which has

---

[32] 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* (Strassbourg: Council of Europe, 2019).
[33] The consolidated text is available at: https://rm.coe.int/16808ade9d.
[34] See e.g. European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (Luxembourg: Publications Office of the European Union, 2018), at 15–16.
[35] OECD, *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, OECD Digital Economy Papers (2011), 176, at 7.
[36] OECD (1980), above note 4.
[37] Ibid.
[38] OECD (2013), above note 5.
[39] Ibid.
[40] APEC, *APEC Privacy Framework* (Signapore: APEC Secretariat, 2005).
[41] The APEC framework endorses similar to the OECD Privacy Guidelienes principles: (1) preventing harm; (2) notice; (3) collection limitations; (4) use of personal information; (5) choice; (6) intergrity of personal information; (7) security safeguards; (8) access and correction; and (9) accountability. G. Greenleaf, 'The APEC Privacy Initiative: "OECD Lite" for the Asia-Pacific?', *Privacy Laws and Business* 71 (2004), 16–18.

Electronic copy available at: https://ssrn.com/abstract=3947049

now been formally joined by Australia, Chinese Taipei, Canada, Japan, South Korea, Mexico, Singapore and the United States.[42] The CBPR system does not displace a country's domestic law, nor does it demand specific changes in it, but provides a minimum level of protection through certain compliance and certification mechanisms. It requires that participating businesses develop and implement data privacy policies that are consistent with the APEC Privacy Framework and the APEC Accountability Agents can assess this consistency. The CBPR system is in this sense analogous to the EU–US Privacy Shield, which we discuss later, in that they both provide means for self-assessment, compliance review, recognition, dispute resolution and enforcement.[43] Both the OECD and APEC privacy frameworks are non-binding[44] but do 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.

III. National approaches for data protection: The European Union versus the United States

1. Data protection in the EU

The EU subscribes to a rights-based, omnibus data protection. The right to privacy is a key concept in EU law and has been given significant weight that reflects deep cultural values and understandings. Building upon the Council of Europe's ECHR, which protects the right to private and family life,[45] the Charter of Fundamental Rights of the European Union (CFREU)[46] distinguishes between the right of respect for private and family life in Art. 7 and the right to protection of personal data, which is explicitly enshrined in Art. 8.[47] This distinction is no coincidence but reflects the heightened concern of the EU and translates into a positive duty[48] to implement an effective protection of personal data and to regulate the transmission of such data. The 1995 Data Protection Directive formed an important part of this ongoing project of the EU.[49] As the regulatory environment profoundly changed, in particular the use and role of data in the economy but also in broader societal contexts, as sketched earlier, the Directive urgently demanded an update, so as to ensure the needed high level of protection of privacy. The more active involvement of the EU as a supranational unity was also prompted by the changes brought about by the Treaty of Lisbon,[50] which entered into force in 2009.[51] Next to

---

[42] http://cbprs.org.

[43] N. Waters, 'The APEC Asia-Pacific Privacy Initiative: A New Route to Effective Data Protection or a Trojan Horse for Self-Regulation', *SCRIPTed: A Journal of Law, Technology and Society* 6 (2009), 74–89.

[44] Some scholars have argued that such soft law frameworks are nonetheless far-reaching, as their implemnetation depends on the power of reputational constraints as treaties do. See e.g. C. Brummer, 'How International Financial LawWorks (and How It Doesn't)', *The Georgetown Law Journal* 99 (2011), 257–327, at 263–272.

[45] Art. 8 ECHR.

[46] Charter of Fundamental Rights of the European Union, OJ C [2010] 83/2.

[47] Art. 8 'Protection of personal data' reads: 1. Everyone has the right to the protection of personal data concerning him or her; 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified; 3. Compliance with these rules shall be subject to control by an independent authority.

[48] European Court of Human Rights, *Refah Partisi (The Welfare Party) and others v. Turkey*, App Nos. 41340/98, 41342/98, 41343/98 and 41344/98, Grand chamber judgment of 13 February 2003.

[49] 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 L [1995] 281/31.

[50] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community OJ C [2007] 306/1.

[51] See C. Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law', *Bloomberg BNA Privacy and Security Law Report* (2012), 1–15; also O. Lynskey, *The Foundations of EU Data Protection Law* (Oxford: Oxford University Press, 2015).

Electronic copy available at: https://ssrn.com/abstract=3947049

this broad underlying need to modernize existing rules and make them fit for the new digital space, there were a number of more concrete decisions and events that triggered the change, as well as made it politically feasible. An important, albeit not directly related, development were the revelations made in 2013 by Edward Snowden that exposed the breadth and depth of surveillance by the US National Security Agency (NSA), which incidentally also involved access to data of millions of private users, including from the systems of Google, Facebook, Apple and other big (US-based) Internet players.[52] Other triggers of reform were a series of seminal decisions of the Court of Justice of the European Union (CJEU), which brought about important changes in existing legal practice, as well as in the overall understanding of individual's rights protection on the Internet in Europe – the *Google Spain* case[53] is perhaps the best known in this context, as it coined the so-called 'the right to be forgotten', which gave priority to privacy over free speech rights and the economic rights of the information intermediaries, such as Google search; another important case was the *Schrems I* judgment of 6 October 2015,[54] which rendered the Safe Harbor Agreement between the EU and the US invalid and illuminated the importance of cross-border data flows, as well as the difficulties with reconciling it with the fundamental right to privacy.

The new EU data protection act, the GDPR, serves the same purpose as the 1995 Data Protection Directive and 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[55] and particularly high standards of protection including enhanced user rights (such as the aforementioned right to be forgotten,[56] but also the right to transparent information,[57] the right of access to personal data;[58] the right to data portability,[59] the right to object[60] and the right not to be subject to automated decision-making, including profiling[61]). The GDPR accordingly foresees also heightened responsibilities of entities controlling and processing data, including data protection by design and by default,[62] and higher penalties for non-compliance.[63]

Noteworthy is also the firmer grasp of the GDPR in terms of its territorial reach. Art. 3(1) specifies the territorial scope as covering the processing of personal data in the context of the

---

[52] See e.g. I. Brown and D. Korff, 'Foreign Surveillance: Law and Practice in a Global Digital Environment', *European Human Rights Law Review* 3 (2014), 243–251.

[53] Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Judgment of the Court (Grand Chamber) of 13 May 2014, ECR [2014] 317.

[54] C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, judgment of 6 October 2015, ECLI:EU:C:2015:650 [hereinafter *Schrems I*].

[55] Art. 5 GDPR specifies that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (*principle of lawfulness, fairness and transparency*); collected for specified, explicit and legitimate purposes (*principle of purpose limitation*); processing must also be adequate, relevant and limited to what is necessary (*principle of data minimization*); as well as accurate and, where necessary, kept up to date (*principle of accuracy*); data is to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (*principle of storage limitation*); data processing must be secure (*principle of integrity and confidentiality*); and the data controller is to be held responsible (*principle of accountability*).

[56] Art. 17 GDPR.

[57] Art. 12 GDPR.

[58] Arts 13, 14, 15 and 19 GDPR.

[59] Art. 20 GDPR.

[60] Arts 21 GDPR.

[61] Art. 22 GDPR.

[62] Art. 25 GDPR.

[63] 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 Art. 83(5), (6) GDPR.

Electronic copy available at: https://ssrn.com/abstract=3947049

activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the Union or not. The GDPR may however also apply to a controller or processor not established in the EU, where 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 EU; or (b) the monitoring of their behaviour as far as their behaviour takes place within the EU.[64] This is in effect a substantial extension of the scope of EU data protection law and bound to have a significant impact in its implementation, potentially becoming applicable to many US and other foreign companies targeting the EU market.[65]

In the context of the extraterritorial application of the GDPR and what has been particular controversial, as exemplified by the *Schrems I* judgment, is the possibility of the European Commission to find that a third country offers 'an adequate level of data protection'[66] – in the sense that the EU unilaterally evaluates the standards of protection in the partner country. The effect of such a decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland, as members of the European Economic Area) to that third country without any further safeguards being necessary,[67] or in other words, transfers to the third country become e assimilated to intra-EU transmissions of data. The European Commission has so far recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay as having adequate level of data protection.

The adequacy test is somewhat strengthened post-*Schrems I*, and the Commission should 'take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law'.[68] The first country subject to an adequacy decision after the adoption of the GDPR is Japan.[69] In a 58-page decision,[70] the Commission found by looking at both the levels of protection provided by Japanese general and sectoral data protection regulations, as well as the redress and oversight mechanisms, that the adequacy standard of Art. 45 GDPR, 'interpreted in light of the Charter of Fundamental Rights of the European Union, in particular in the *Schrems* judgment, is met'.[71]

---

[64] Art. 3(2) GDPR. Guidance to determine whether a controller or a processor is offering goods or services to EU data subjects is provided in Recital 23 GDPR, as well as in more detail by the EU data protection authority (see European Data Protection Board (EDPB), Guidelines 3/2018 on the territorial scope of the GDPR (Art. 3), version 2.0, 12 November 2019).

[65] See e.g. P.M. Schwartz, 'Information Privacy in the Cloud', *University of Pennsylvania Law Review* 161 (2013), 1623–1662; O. Tene and C. Wolf, 'Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation', *Future of Privacy Forum White Paper*, January 2013; 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; C. Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post *Schrems*', *University of Cambridge Faculty of Law Legal Studies Research Paper Series* 14 (2016).

[66] The adoption of an adequacy decision involves a proposal from the European Commission; an opinion of the European Data Protection Board; an approval from representatives of EU countries; and the adoption of the decision by the European Commission. At any time, the European Parliament and the Council may request the European Commission to maintain, amend or withdraw the adequacy decision on the grounds that its act exceeds the implementing powers provided for in the regulation.

[67] Art. 45(1); Recital 103 GDPR.

[68] Recital 104 GDPR and Art. 45(2).

[69] Negotiations are ongoing with South Korea and many of the existing adequacy decisions are up to renewal.

[70] Commission Implementing Decision 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, OJ L [2019] 76/1.

[71] Ibid., at para. 175.

Electronic copy available at: https://ssrn.com/abstract=3947049

In the absence of an 'adequacy decision', a controller or processor may transfer personal data to a third country only if they provide appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.[72] Such appropriate safeguards may be provided for, by: (a) a legally binding and enforceable instrument between public authorities or bodies; (b) binding corporate rules; (c) standard data protection clauses adopted by the Commission; (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission; (e) an approved code of conduct with binding and enforceable commitments; or (f) an approved certification together with binding and enforceable commitments. While the GDPR brings more clarity and certainty with regard to these clauses, they are still related to higher costs and provide only a second-best option.[73] Overall, under the EU data protection regime, there is a priority given to the protection of privacy over economic rights and the EU seeks to 'export' these higher standards either by binding individual countries through the adequacy decision or by applying EU law to foreign business that use EU citizens' data under the GDPR.

2. Data protection in the US

The United States shares a fundamentally different idea of privacy protection, which is deeply rooted in its history and understood as protection of liberty.[74] In this sense, it 'focuses more on restrictions, such as the Fourth Amendment, that protect citizens from information collection and use by government rather than private actors. In fact, private actors are often protected from such restrictions by the First Amendment'.[75] 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',[76] and this has been recently confirmed by the White House strategy on AI.[77]

While under the First Amendment, free speech has been given robust protection in the US, data protection is regulated in a fragmented manner in some federal privacy laws and a great number of state laws.[78] These laws either concern the public sector only or they are information-specific or medium-specific, as they regulate for instance health information, video privacy or electronic communications. While the Federal Trade Commission (FTC) can use its competence to adjudicate on unfair or deceptive trade practices to discipline companies that fail to implement minimal data security measures or fail to meet its privacy policies, the US does not have an official data protection authority.[79] As a consequence of this fragmentation, there is no coherent definition of personal data, neither there is one of sensitive personal data. There are no

---

[72] Art. 46(1) GDPR.

[73] G. Drake, 'Navigating the Atlantic: Understanding EU Data Privacy Compliance Amidst A Sea of Uncertainty', *Southern California Law Review* 91 (2017), 163–194.

[74] 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.

[75] L. Downes, 'The Business Implications of the EU-U.S. "Privacy Shield"', *Harvard Business Review*, 10 February 2016, https://hbr.org/2016/02/the-business-implications-of-the-eu-u-s-privacy-shield.

[76] R.A. Clarke et al., *The NSA Report: Liberty And Security in A Changing World* (Princeton, NJ: Princeton University Press, 2014), at 158.

[77] The White House, Guidance for Regulation of Artificial Intelligence Applications, 2019.

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

[79] For a great overview of US privacy laws, see S.J. Deckelboim, 'Consumer Privacy on an International Scale: Conflicting Viewpoints Underlying The EU-U.S. Privacy Shield Framework and How the Framework Will Impact Privacy Advocates, National Security, and Businesses', *Georgetown Journal of International Law* 48 (2017), 263–296.

Electronic copy available at: https://ssrn.com/abstract=3947049

restrictions on the transfer of personal data by private entities and self-regulation and best practices are the common model of privacy protection. Data is in addition 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 governance in Europe.[80]

3. Bridging the EU–US differences: From Safe Harbor to 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, as the chapter shows below. Transatlantic data flows are of economic significance for both partners[81] and have so far been enabled through an ingenious set of legal mechanisms. First, under the so-called 'Safe Harbor' scheme,[82] which contained in essence a series of principles concerning the protection of personal data to which US undertakings subscribe on a voluntary basis.[83] The CJEU found however in the above-mentioned *Schrems I* judgment that the Safe Harbor did not provide a level of protection of fundamental rights that is essentially equivalent to that guaranteed within the EU.[84] The Court observed in particular that the Safe Harbor scheme is applicable solely to US undertakings that adhere to it but does not bind US public authorities. It was also apparent that US national security, public interest and law enforcement requirements prevail over the Safe Harbor Agreement, so that in effect US undertakings can disregard, without limitation, the rules laid down by that scheme where they conflict with such requirements[85] – thus affecting also fundamental rights of EU citizens. The Court found furthermore that, US legislation is not limited to what is strictly necessary, as it permits, on a generalized basis, storage of all the personal data of all the persons whose data is transferred from the EU to the US without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down for determining the limits of the access of the public authorities to the data and of its subsequent use. There were in addition no legal remedies provided,[86] so the Court ultimately declared the Safe Harbor Decision invalid.[87]

The Safe Harbor agreement was subsequently and after intense negotiations replaced by the so-called the EU–US Privacy Shield.[88] The Privacy Shield is much more stringent and detailed than the Safe Harbor. While US companies (both data controllers and processors) still self-certify on an annual basis, the new arrangement provides stronger obligations upon US companies to protect the personal data of European citizens according to a set of clearly defined principles.[89] In addition, there are much stronger monitoring and enforcement mechanisms.

---

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

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

[82] 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 215/7.

[83] See H. Farrell, 'Constructing the International Foundations of E-Commerce – The EU-US Safe Harbor Arrangement', *International Organization* 57 (2003), 277–306; Schwartz and Solove, above note 74.

[84] *Schrems I*, para. 97.

[85] *Schrems I*, para. 86.

[86] *Schrems I*, paras 93–95.

[87] *Schrems I* paras 105–106.

[88] 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. For an overview, see European Commission, 'EU-US Privacy Shield: Frequently Asked Questions', MEMO/16/434, Brussels, 29 February 2016.

[89] European Commission's Implementing Decision, ibid. Paras 19–29 refer to the Notice Principle, Data Integrity and Purpose Limitation Principle, Choice Principle, Security Principle, Access Principle, Recourse, Enforcement

Electronic copy available at: https://ssrn.com/abstract=3947049

Organizations may choose independent recourse mechanisms in either the EU or in the United States, including the possibility to voluntarily cooperate with the EU data protection authorities (DPAs). Where organizations process human resources data, the cooperation with the DPAs is mandatory. Other alternatives include independent Alternative Dispute Resolution or private-sector developed privacy programmes that commit to the Privacy Principles.[90] It is in this sense the purpose of the Privacy Shield framework to provide data subjects with a number of possibilities to enforce their rights, lodge complaints regarding non-compliance by US companies and ultimately, to have their complaints resolved.[91] Next to the enhanced individual safeguard mechanisms and for the first time, there is explicit assurance from the US that any access of public authorities to personal data will be subject to clear limitations, safeguards, and oversight mechanisms. US authorities have affirmed absence of indiscriminate or mass surveillance.[92] There is in addition a new redress possibility through the EU–US Privacy Shield Ombudsperson, who is to be independent from the US Intelligence Community and can address individual complaints.[93] In the European Commission's assessment, all this conforms with the standards set out in the *Schrems I* judgment, according to which legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 CFREU must impose 'minimum safeguards', cannot involve 'on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States', and must provide sufficient legal remedies.[94] The EU–US Privacy Shield is still the working mechanism for transatlantic data flows[95] but has been subject to both criticism and attacks in court.[96]

C. Privacy under the WTO framework

As noted at the outset, privacy and data protection have not been a negotiation topic during the Uruguay round and WTO law has not so far undergone any changes that reflect their growing importance or digital transformation in general.[97] Yet, despite this and although WTO law represents a 'hard' form of international law, it does include certain mechanisms meant to reconcile economic and non-economic interests, international commitments and domestic values and sensitivities. Key amongst these mechanisms are the 'general exceptions' formulated under Art. XX of the GATT 1994 and Art. XIV GATS. They permit WTO Members to adopt measures, which would otherwise violate their obligations and undertaken commitments, under the condition that these measures are not disguised restrictions on trade. Particularly interesting for this chapter's discussion are the possibilities that Art. XIV GATS may open for maintaining existing and adopting new data restrictions based on grounds of privacy protection.

---

and Liability Principle, and Accountability for Onward Transfer Principle. The principles are additionally detailed in Annex II attached to the Commission's implementing decision.

[90] European Commission, ibid., at para. 40.

[91] European Commission, ibid., at paras 43–63.

[92] European Commission, ibid., at paras 64–90.

[93] European Commission, ibid, at paras 119–122. For a great analysis of the EU-US Privacy Shield, see Deckelboim, above note 79.

[94] European Commission, above note 88, at paras 90 and 124 citing the *Schrems I* judgment.

[95] European Commission, Report on the third annual review of the functioning of the EU-U.S. Privacy Shield, COM(2019) 495 final, 23 October 2019.

[96] See e.g. Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (Shrems II).*

[97] M. Burri, 'The International Economic Law Framework for Digital Trade', *Zeitschrift für Schweizerisches Recht* 135 (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).

Electronic copy available at: https://ssrn.com/abstract=3947049

While Art. XIV GATS enumerates different grounds as possible justifications, such as the protection of human, animal or plant life or health,[98] especially pertinent for us are two categories: (a) those relating to public order or public morals[99] and (b) those that are necessary to secure compliance with laws or regulations.[100] In the latter context, it is spelled out that this may be the case in particular when necessary to secure compliance with laws or regulations relating 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'.[101] The focus here is on this provision and for the sake of revealing how it is relevant for data flows, it is assumed that the rules of the EU GDPR are tested under it, because they were found to either violate the market access or the national treatment obligations of the EU under the GATS.[102]

Art. XIV GATS, similarly to Art. XX GATT, involves a number of legal tests, as established by the WTO jurisprudence: (i) first, the panels and the Appellate Body consider whether the measure falls within the scope of one of the listed objectives in the exception; (ii) second, the measure must address the relevant public interest at issue, with a sufficient nexus between the measure and the objective pursued;[103] (iii) the thirdly, the measure is examined under the chapeau (the introductory paragraph) of Art. XIV GATS. With regard to (i), there has been a wide margin of appreciation given to WTO Member in their choice of objectives 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. At one end of this continuum lies 'necessary' understood as 'indispensable', which at the opposite side, 'necessary' is taken to mean as 'making a contribution to'. The Appellate Body noted that a 'necessary' measure is located significantly closer to the pole of 'indispensable' than to simply 'making a contribution to'.[104] 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 'necessary'.[105] However, the Appellate Body has also stated that the requirement for measures 'relating to' a goal (as is the case with the GATS privacy exception), is 'more flexible textually' than a strict 'necessity' requirement and may simply require a 'substantial' or 'reasonable'

---

[98] Art. XIV(b) GATS.

[99] Art. XIV(a) GATS. See 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.

[100] Art. XIV(c) GATS. For a commentary of Art. XIV GATS, see 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.

[101] Art. XIV(c)(ii) GATS.

[102] For a fully-fledged analysis of how this may be occur, 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.

[103] 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, at para. 292; see also WTO Appellate Body Report, *Brazil – Measures Affecting Imports of Retreaded Tyres*, WT/DS332/AB/R, adopted 3 December 2007, at paras 119–124.

[104] WTO Appellate Body Report, *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, WT/DS161/AB/R, WT/DS169/AB/R, adopted 11 December 2000 [hereinafter *Korea – Beef*], at para. 161.

[105] Appellate Body Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/AB/R, adopted 7 April 2005 [hereinafter *US – Gambling*], at para. 6.536; see also WTO Panel Report, *Argentina – Financial Services*, WT/DS453/R, adopted 30 September 2015, at paras 7.655, 7.685, 7.727, referring to *Korea – Beef*, at paras 162, 163.

Electronic copy available at: https://ssrn.com/abstract=3947049

relationship of the measure to the objective pursued.[106]

Ultimately, it has also been clarified that this 'weighing and balancing'[107] of factors should also include a comparison of the challenged measure and its possible alternatives.[108] In order to show that the measure does not meet the necessity test, a claimant can demonstrate that a less trade-restrictive alternative to the measure has been 'reasonably available'. The alternative measure cannot pose prohibitive costs or substantial technical difficulties to implement.[109] A measure that has been provisionally justified under the above material requirements of Art. XIV(c)(ii) must also meet the chapeau test, which says that a 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 as 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[110] and by evaluating the 'consistency of enforcement' of the challenged measure.[111]

Admittedly, these tests set a high hurdle for WTO Members and the 'success rate' for passing through them has been rather low.[112] Scholars have argued that if the EU would be challenged before a WTO panel, its GDPR may fail to satisfy the test – on several particular grounds. Irion et al. have argued that the EU may face a problem with finding appropriate evidence on the performance of its data protection law.[113] For instance, the EU–US Safe Harbor agreement,[114] which has now been invalidated, was not particularly stringent as shown by the *Schrems I* judgment, and one can argue that this undermines the strength of a challenged measure's contribution to securing compliance with EU data protection law. Second and this is a critical argument, it can well be maintained that there are less trade restrictive measures that are reasonably available for the attainment of EU's desired level of data protection. The GDPR is indeed in many senses excessively burdensome with sizeable extraterritorial effects, as noted earlier.[115] Especially if compared with other data protection rules around the world, it may be difficult to prove that privacy cannot be otherwise protected.[116] Even if the provisions on the

---

[106] *Korea – Beef*, at para. 49, note 104 (citing WTO Appellate Body Report, *United States – Standards for Reformulated and Conventional Gasoline*, WT/DS2/AB/R, adopted 29 April 1996, at para. 19 and WTO Appellate Body Report, *United States – Import Prohibition of Certain Shrimp and Shrimp Products*, WT/DS58/AB/R, adopted 12 October 1998, at para. 141).

[107] See *US – Gambling*, at para. 78; Appellate Body Report, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, WT/DS363/AB/R, adopted 21 December 2009 [hereinafter *China – Publications and Audiovisual Products*], at para. 239.

[108] WTO Appellate Body Report, *US – Gambling*, para. 306; WTO Panel Report, *Argentina – Financial Services*, para. 7.684.

[109] WTO Panel Report, *Argentina – Financial Services*, para. 7.729 referring to WTO Appellate Body Report, *US – Gambling*, para. 308.

[110] *Argentina – Financial Services*, at para. 7.743.

[111] *US – Gambling*, 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 Art. XIV 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.

[112] Only one case has so far passed all the tests. See WTO Appellate Body Report, *US – Import Prohibitions of Certain Shrimp and Shrimp Products* (Recourse to Article 21.5 DSU by Malaysia), WT/DS58/AB/RW, adopted 22 October 2001; also Robert Howse, 'The Appellate Body Rulings in the Shrimp/Turtle Case: A New Legal Baseline for the Trade and Environment Debate', *Columbia Journal of Environmental Law* 27 (2002), 489–519.

[113] Irion et al., above note 102, at 36–39; also D.A. MacDonald. and C.M. Streatfeild, 'Personal Data Privacy and the WTO', *Houston Journal of International Law* 36 (2014), 625–652, 640–650.

[114] 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 215/7.

[115] See references above note 65.

[116] L. Bygrave, *Data Privacy Law: An International Perspective* (Oxford: Oxford University Press 2014); M.

Electronic copy available at: https://ssrn.com/abstract=3947049

transfer of personal data to third countries were to be deemed necessary in order to secure compliance with the GDPR, there is an argument to be made that these provisions have not been consistently implemented and would ultimately fail the chapeau test. If the EU has denied a third country's application for 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, it seems that the chapeau test requirements are hard to meet. The EU may be effectively discriminating between different countries in finding adequate levels of protection there and in engaging in cooperation with them, so that these are secured in terms of substance and procedure.[117]

The general exception clause under Art. XIV GATS is a good example of both the flexibility of WTO law, as well as of its potential to intervene in domestic matters in an attempt to discipline WTO Members and draw a line between licit and illicit protectionism. Despite the current deadlock at the WTO and the crisis of its dispute resolution system, the interpretation of Articles XX GATT and XIV GATS remains of critical importance, as many free trade agreements (FTAs) stimulate their application *mutatis mutandis*.[118]

D. Developments in FTAs

As legal adaptation under the umbrella of the WTO has stalled, many issues of digital trade and of data governance have been addressed in free trade agreements, either of bilateral or regional nature. Indeed, from the 347 FTAs agreed upon between 2000 and 2019, some 184 FTAs have provisions on digital trade. The United States has been a legal entrepreneur and played a key role by endorsing liberal rules in the implementation of its 'Digital Agenda'.[119] The agreements reached since 2002 with Australia, Bahrain, Chile, Morocco, Oman, Peru, Singapore, the Central American countries,[120] Panama, Colombia, South Korea and Japan, as well the updated North American Free Trade Agreement (NAFTA) with Canada and Mexico, 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 well. Singapore, Australia, Japan and Colombia have been among the major drivers of this diffusion. In this section, we map the emerging regulatory landscape in particular with regard to data-relevant norms.[121]

I. Overview of data-related rules in FTAs

One can in general speak of the relevance for trade rules for data and data flows, as they matter for data at least in 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 intermediaries' liability; and (iii) finally, because trade

---

Rotenberg, *Privacy Law Sourcebook 2016: United States Law, International Law, and Recent Developments* (Washington, DC: Electronic Privacy Information Center, 2016)

[117] Irion et al., above note 102, at 36–39.

[118] For instance, the recent Digital Economy Partnership Agreement between Chile, Singapore and New Zealand.

[119] See Sacha Wunsch-Vincent, 'The Digital Trade Agenda of the US: Parallel Tracks of Bilateral, Regional and Multilateral Liberalization', *Aussenwirtschaft* 1 (2003), 7–46.

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

[121] 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', *Journal of International Economic Law* 23 (2020), 187–220 and http://unilu.ch/taped.

Electronic copy available at: https://ssrn.com/abstract=3947049

law can limit the policy space that regulators have at home.[122] 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 on these rules in particular. It needs to be mentioned at the outset that there is no common agreement on a definition of data flows in FTAs, despite the wide-spread rhetoric around the term and its frequent use in reports and studies.[123] Important to note in this regard is that despite the different terms used in treaty language, there seems to be a tendency for a broad and encompassing definition of data flows, (1) where there are bits of information (data) as part of the provision of a service or a product and (2) 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.[124] In addition, it may be noted that there has not been a distinction between different types of data so far – for instance, between personal and non-personal data, personal or company data, or machine-to-machine data.[125] Yet, personal information is commonly included explicitly in the data-related provisions in FTAs, where 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 FTAs but only in handful of agreements. These are rules referring to the cross-border flow of data and rules banning or limiting data localization requirements. Provisions on data flows can also found in chapters, dealing with discrete services sectors, where data is inherent to the very definition of those services – such as in the telecommunications and financial services sectors.[126]

II. Rules on data flows and data localization

Non-binding provisions on data flows appeared early and can already be found in the 2000 Jordan-US FTA.[127] Yet, it is only in recent years that these rules have been made binding and

---

[122] See in this sense 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; F. Casalini and J. López González, 'Trade and Cross-Border Data Flows', *OECD Trade Policy Papers* 220 (2019).

[123] See e.g. Casalini and González, above note 122; OECD, *Trade and Cross-border Data Flows*, Trade Policy Brief, June 2019.

[124] As the OECD (above note 123, 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'.

[125] 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 data into different categories. See OECD, *Data in the Digital Age*, Policy Brief, March 2019.

[126] This chapter does not cover specific services sectors. For a more detailed analysis, see e.g. M. Burri, 'Telecommunications and Media Services in Preferential Trade Agreements: Path Dependences Still Matter', in M. Krajewski and R. Hoffmann (eds), *European Yearbook of International Economic Law: Coherence and Divergence in Agreements on Trade in Services* (Berlin: Springer, 2020).

[127] A similar wording is used in the 2008 Canada-Peru FTA, 2010 Hong-Kong-New Zealand FTA, the 2011 Korea-Peru FTA, the 2011 Central America-Mexico FTA, the 2013 Colombia-Costa Rica FTA, the 2013 Canada-Honduras FTA, the 2014 Canada-Korea FTA, and the 2015 Japan-Mongolia FTA. The 2007 South Korea-US FTA was the first agreement with more concrete language on data flows, albeit in a soft law form (Korea-US FTA, Art. 15.8).

Electronic copy available at: https://ssrn.com/abstract=3947049

more comprehensive. Particularly important in this context were the negotiations of the Transpacific Partnership Agreement (TPP),[128] between the US and eleven countries in the Pacific Rim,[129] as the TPP sought to be a bold 21st century trade deal and move away from the brick-and-mortar WTO Agreements.[130] While the TPP did not eventually materialize because the Trump administration withdrew from it, it gave the basis for two important treaties – (1) the Comprehensive and Progressive Agreement for Transpacific Partnership (CPTPP)[131] between the remainder of the TPP parties; and (2) the renegotiated NAFTA, which is now referred to as 'United States Mexico Canada Agreement' (USMCA). The CPTPP and the USMCA electronic commerce chapters build upon the TPP and in this sense reflect the US agenda on the relevant issues; they create a comprehensive template for digital trade with strong rules on data flows. We look in turn at these treaties.[132]

The CPTPP seeks for the first time to explicitly restrict the use of data localization measures. Art. 14.13(2) prohibits the parties from requiring a 'covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory'. The soft language from the US-South Korea FTA on free data flows is now also 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'.[133] 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 Art. 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'.[134] These non-discriminatory conditions are similar to the test formulated by Art. XIV GATS and Art. XX GATT 1994, 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'.[135] This permits more regulatory autonomy for the CPTPP signatories. However, it also may lead to abuses and overall legal uncertainty. Further, it should be noted that the ban on localization measures is somewhat softened with regard to financial services and institutions.[136] 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.[137]

---

[128] The Trans-Pacific Partnership Agreement, https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text [hereinafter *TPP*].

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

[130] See e.g. J. Ravenhill, 'The Political Economy of the Trans-Pacific Partnership: a '21st Century' Trade Agreement?', *New Political Economy* 22 (2017), 573–594.

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

[132] For a fully fledged analysis, see Burri (2017), above note 122; also M. Burri, 'Data Flows and Global Trade Law', in M. Burri (ed), *Big Data and Global Trade Law* (Cambridge. Cambridge University Press, forthcoming 2020).

[133] Art. 14.11(2) CPTPP.

[134] Art. 14.11(3) CPTPP.

[135] Art. 14.11(3) CPTPP.

[136] See the definition of 'a covered person' in Art. 14.1, which is said to exclude a 'financial institution' and a 'cross-border financial service supplier'.

[137] The provision reads: 'Each Party shall allow a financial institution of another Party to transfer information in

Electronic copy available at: https://ssrn.com/abstract=3947049

Government procurement is also excluded.[138]

After the withdrawal of the United States from the TPP, there was some uncertainty as to the direction the United States will follow in its trade deals in general and on matters of digital trade in particular. The 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 (Art. 19.12), providing a non-discrimination regime for digital products (Art. 19.4) and a hard rule on free information flows (Art. 19.11). The USMCA keeps the clause on exceptions that permits the pursuit of certain non-economic objectives. Art. 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.[139] The USMCA clarified further that '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',[140] which makes effectively makes a link to the necessity test under WTO law and practice.

Subsequent treaties, such as the 2016 Chile-Uruguay FTA and the 2016 Updated Singapore-Australia FTA, and the 2019 US-Japan Digital Trade Agreement closely follow the CPTPP template and enhance the diffusion of the rules on data flows and data localization. In contrast, the European Union has been cautious in inserting rules on data in its free trade deals and presently none of its treaties has such rules of binding nature. It is only recently that the EU has made a step towards such rules, whereby 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,[141] and in the modernization of the trade part of the EU-Mexico Global Agreement. 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 link this commitment in due time with the high data protection standards of the GDPR.[142]

III. Rules on data protection

83 FTAs so far include provisions on data protection. Yet, the nature of the awarded protection varies considerably and can include a mixed bag of binding and non-binding provisions, which is symptomatic of the very different positions of the major actors and the inherent tensions between the regulatory goals of data innovation and data protection. Earlier agreements, such as 2000 Jordan-US FTA Joint Statement on Electronic Commerce, address privacy issues in hortorary provisions.[143] Later agreements remain still in the domain of soft law but include a

---

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'.

[138] Art. 14.8(3) CPTPP.

[139] Art. 19.11(2).

[140] Art. 19.11(2), footnote 5.

[141] Art. 8.81 EU-Japan EPA.

[142] 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.

[143] Jordan-US, Joint Statement on Electronic Commerce, 7 June 2000, Art. II.

Electronic copy available at: https://ssrn.com/abstract=3947049

variety of cooperation activities in order to improve the level of protection of privacy and curb obstacles to trade that requires transfers of personal data. These activities include sharing information and experiences on regulations, laws and programmes on data protection,[144] or the overall domestic regime for the protection of personal information;[145] technical assistance in the form of exchange of information and experts,[146] research and training activities;[147] or the establishment of joint programmes and projects.[148]

FTAs 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,[149] in several treaties parties specifically commit to adopt or maintain legislation or regulations that protect the personal data or privacy of users. Representative of this group are again the CPTPP and the USMCA. Art. 14.8(2) requires every CPTPP party to 'adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce'. Yet, 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'.[150] 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'.[151] Parties are also invited to promote compatibility between their data protection regimes, by essentially treating lower standards as equivalent.[152] Overall, the goal seems to be to prioritize trade over privacy rights.

The USMCA is interesting in two aspects when compared to the CPTPP and the usual US position on data protection issues: While Art. 19.8 remains soft on prescribing domestic regimes on personal data protection, it recognizes principles and guidelines of relevant international bodies. Art. 19.8 states in particular that '[i]n 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)'.[153] The USMCA 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,[154] and aim to provide remedies for any violations.[155] This is interesting because it goes beyond what the US may have in its national laws on data protection

---

[144] See e.g. Brazil-Chile FTA, Art. 10.8.5 and Art. 10.15(b); Canada-Korea FTA, Art. 13.7(b); Australia-Japan FTA, Art. 13.10.2; Chile-Colombia FTA, Art. 12.5(b); Nicaragua-Taiwan FTA, Art. 14.05(b); Panama-Singapore FTA, Art. 13.4(b); CAFTA-DR-US, Art. 14.5(b); Chile-US FTA, Art. 15.5(b).

[145] Australia-Indonesia FTA, Art. 13.3.1(b)(i); USMCA, Art. 19.14.1(a)(i); Australia-Peru FTA, Art. 13.14(b)(i); Singapore-Sri Lanka FTA, Art. 9.12(c)(i); Singapore-Turkey FTA, Art. 9.9(c); China-Korea FTA, Art. 13.5; Colombia-Costa Rica FTA, Art. 16.6.2; Canada-Colombia FTA, Art. 1506.2.

[146] Chile-EC AA, Art. 30.

[147] Korea-Vietnam FTA, Art. 10.8.1(b).

[148] Chile-EC AA, Art. 30.

[149] Australia-Indonesia FTA, Art. 13.7.1; Brazil-Chile FTA, Art. 10.2.5(f) and Art. 10.8.1; EU-Japan EPA, Art. 8.78.3; Central America-Korea FTA, Art. 14.5.1; Canada-Honduras FTA, Art. 16.2.2(e).

[150] Art. 14.8(2) CPTPP.

[151] Art. 14.8(2) CPTPP, at footnote 6.

[152] Art. 14.8(5) CPTPP.

[153] Art. 19.8(2) USMCA.

[154] Art. 19.8(3) USMCA.

[155] Art.19.8(4) and (5) USMCA.

Electronic copy available at: https://ssrn.com/abstract=3947049

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,[156] or whether we are seeing a shift in US privacy protection regimes as well.[157]

As signalled earlier, the EU has sought more commitments for privacy protection in its FTAs. Many of the EU's agreements 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.[158] The EU has also pushed for more safeguards, so that its partners adopt appropriate measures to ensure the privacy protection while allowing the free movement of data, establishing a criterion of 'equivalence'. Parties commit also to inform each other of their applicable rules and negotiate reciprocal, general or specific agreements,[159] as exemplified by the additional adequacy decisions of the European Commission, most recently with Japan. As noted above, the EU wishes to permit data flows only if coupled with the high data protection standards of the GDPR. In its currently negotiated trade deals with Australia, Indonesia, New Zealand and Tunisia, as well as in the EU proposal for WTO rules on electronic commerce,[160] the EU follows a distinct model of endorsing and protecting privacy as a fundamental right.[161] In addition, there is broad carve-out, in the sense that: 'Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, *including through the adoption and application of rules for the cross-border transfer of personal data*. Nothing in this agreement *shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards*'.[162] The EU thus reserves ample regulatory leeway for its current and future data protection measures. The exception is also fundamentally different that the objective necessity test under the CPTPP and the USMCA, because it is subjective in nature and safeguards EU's right to regulate.[163]

E. Pros and cons of the different reconciliation models

The above sections revealed not only the intensified contestation between free data flows as an essential element of the data-driven economy and the protection of privacy as a sovereign right

---

[156] 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).
[157] For a great analysis, see A. Chander, M.E. Kaminski and W. McGeveran, 'Catalyzing Privacy Law', *University of Colorado Law Legal Studies Research Paper* No 19-25 (2019).
[158] Cameroon-EC Interim EPA, Chapter 6, Arts 61-65; CARIFORUM-EC EPA, Chapter 6, Arts 197-201. 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: Argentina-Chile FTA, Art. 11.2.5(f) footnote 1; Chile-Uruguay FTA, Art. 8.2.5(f), footnote 3.
[159] EC-Singapore FTA, Art. 8.54.2; Understanding 3 Additional Customs-Related Provisions, Arts 9.2 and 11.1; EC-Ghana EPA, Protocol on Mutual Administrative Assistance on Custom Matters, Art. 10; Bosnia and Herzegovina-EC SAA, Protocol 5 on Mutual Administrative Assistance on Custom Matters, Art. 10.2; Algeria EC Euro-Med Association Agreement, Art. 45 and Protocol No 7.
[160] 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.
[161] See European Commission (2018), above note 142.
[162] Ibid. (emphases added).
[163] S. Yakovleva, 'Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy', *University of Miami Law Review* 74 (2020), 416–519, at 496.

Electronic copy available at: https://ssrn.com/abstract=3947049

of states to safeguard their citizens, but also the very different regulatory approaches that have been sought to reconcile these interests. In the face of failing international cooperation and the diverging positions of the major stakeholders of the EU and the US, trade venues, and perhaps oddly or even wrongly so,[164] have become platforms for rule-creation that try to interface data flows and privacy protection. We are far from an optimal model however and states are still grappling to find viable mechanisms, which not only provide a level of certainty and market access for businesses but also reflect the state's societal values.

Each of the existing models does come with certain pros and cons. The international framework is not fully developed with regard to privacy protection; it is not binding, nor does it have mechanisms that can effectively reconcile the clash of rights. The transnational regimes under the OECD and APEC, whereas still not binding and of club nature, have provided agreement on some basic regulatory principles that shape domestic frameworks, while at the same time ensuring the free flow of information. As the underlying principles of these frameworks become increasingly integrated into trade law, which enhances their regulatory strength and diffusion across countries, they may provide a good way to tackle the tensions. Oversight and enforceability in case of violations remain however important questions without an adequate answer and for countries, like the EU Member States, that demand appropriate checks and balances for the protection of individual rights, they may plainly be not enough. In the area of international trade law, we have the generic exception clauses under Art. XX GATT and Art. XIV GATS, which have been also replicated in a number of FTAs *mutatis mutandis*. They provide for a stringent test that seeks to constrain protectionism, when states pursue non-economic objectives, but since we have no jurisprudence, are yet unsure how they will be applied in practice, and whether for instance the EU's GDPR will not be found in violation of the EU's commitments under the GATS. It is also questionable whether an *ex post*, timewise protracted, case-by-case examination of alleged infringements can match the fluidity of the digital economy and the high stakes at hand. The CPTPP and the USMCA templates are modelled along the WTO norms but are linked to an even higher degree of uncertainty, as the legitimate objectives are not clearly spelled out. Coupled with the low privacy protection guarantees that these treaties provide, there seems to be a priority given to economic rights. Such a stance, although it may make certain economic sense and boost growth and innovation, may be however unacceptable for some actors, such as notably the European Union, which place a high value on fundamental rights and seek to ensure their effective protection. The EU has accordingly sought to export its high standards of protection through an extension of the territorial application of the GDPR and unilateral adequacy decisions that short of international harmonization provide for an adequate level of protection of EU citizens' data. This unilateral approach, while justified on the side of the EU, may be linked to higher costs of compliance for foreign firms and countries and may have negative implications even for the EU's economy and innovation capabilities in the era of Big Data and AI. One ingenuine solution discussed above is the EU-US Privacy Shield as a flexible mechanism that reconciles the high standards of protection in the EU and the fairly low levels of personal data protection in the US. The EU-US Privacy Shield is by no means perfect, as it fails to satisfy high demands of bindingness and enforceability; on the other hand, it has certain advantages as there are working supervisory and remedy mechanisms, at least post-*Schrems*. Moreover, firms are not required to establish a costly presence in the EU and the assessment of conformity with EU standards takes place at home by domestic regulators. It may thus be worthwhile contemplating to what extent such or similar mechanisms may be extended and made viable in plurilateral or multilateral contexts.[165]

---

[164] Yakovleva, ibid.

[165] A. Mattoo and J.P. Meltzer, 'Data Flows and Privacy: The Conflict and Its Resolution' *Journal of International Economic Law* 21 (2018) 769–789.

Electronic copy available at: https://ssrn.com/abstract=3947049

While the current negotiations on electronic commerce under the auspices of the WTO reveal at this stage little agreement and willingness to move forward,[166] preferential trade venues can serve as governance laboratories and pave the way towards regulatory cooperation and possible implementation of the Privacy Shield model.

Summing up, one can underscore that privacy protection has clearly become a key topic on the trade negotiation tables and there is new rule-making evolving that seeks to interface the demands of the digital economy to permit free flowing data and the sovereign wish to adequately safeguard the rights and values embedded in individual societies. Trade policy has the capacity to promote trade and innovation despite varying standards for privacy protection but there is a clear demand for enhanced regulatory cooperation.[167] As the complexity of the data-driven society rises, such regulatory cooperation seems indispensable for moving forward, since data issues cannot be addressed by the plain 'lower tariffs, more commitments' stance in trade negotiations but demand effective reconciliation mechanisms and continuous oversight.

[166] See e.g. I. Willemyns, 'Agreement Forthcoming? A Comparison of EU, US, and Chinese RTAs in Times of Plurilateral E-Commerce Negotiations', *Journal of International Economic Law* 23 (2020), 221–244; M. Burri, 'Towards a New Treaty on Digital Trade', *Journal of World Trade* 55 (2021).

[167] T.J. Bollyky and P.C. Mavroidis, 'Trade, Social Preferences, and Regulatory Cooperation: The New WTO-Think' *Journal of Inernational 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 digital trade); also U. Ahmed, 'The Importance of Cross-Border Regulatory Cooperation in the Era of Digital Trade' *World Trade Review* 18 (2019), s99–s120.

Electronic copy available at: https://ssrn.com/abstract=3947049