Cross-border data flows and privacy in global trade law: has trade trumped data protection?

Mira Burri

A. Introduction: from e-commerce to the data-driven economy

Legal adaptation in the face of technological advances, including in the area of trade law, is not necessarily a new topic.[1] This is true also for digital technologies, as on the one hand, the WTO membership realized fairly early on with the 1998 Work Programme on Electronic Commerce that all areas of trade are deeply affected by the Internet and changes in the existing rules for trade in goods, trade in services, as well as those for the protection of intellectual property (IP) rights, may be needed.[2] On the other hand, this acknowledgment has been accompanied with a host of studies that explored where indeed such changes are most urgent and how they may look like, considering also their political feasibility.[3] Yet, it is fair to note that this dual mobilization of policy and scholarship was based on a wave of technological changes that were still so to speak at level 2.0, where the Internet was seen as a mere platform enabling the online sale of services and goods, often framed under 'e-commerce', but failed to recognize the disruptive potential of the Internet as a general purpose technology (GPT) with far-reaching spillover effects.[4] With the changing conditions of trade and the emergence of global value chains (GVCs), intensified convergence and servicification, these effects did become palpable and were considered by a series of later studies.[5] Yet, the centrality of data remained largely ignored, as its embeddedness in the economy and its profound societal effects were at an early stage. It is only recently with the advent of the so-called 'Forth Industrial Revolution' that the impact of data across all sectors of the economy and the disruptive character of digitization were fully acknowledged.[6] And it is only in very recent times, with the shaping of Big Data and

---

[1] See e.g. R. Brownsword, E. Scotford and K. Yeung (eds), *The Oxford Handbook on Law, Regulation and Technology* (Oxford: Oxford University Press, 2017); S. Peng, H. Liu and C. Lin (eds), *Governing Science and Technology under the International Economic Order* (Cheltenham: Edward Elgar, 2018).

[2] World Trade Organization (WTO), Work Programme on Electronic Commerce, WT/L/274 (1998).

[3] See e.g. S. Wunsch-Vincent, *The WTO, the Internet and Digital Products: EC and US Perspectives* (Oxford: Hart, 2006); S. Wunsch-Vincent, 'Trade Rules for the Digital Age', in M. Panizzon, N. Pohl and P. Sauvé (eds), *GATS and the Regulation of International Trade in Services* (Cambridge: Cambridge University Press, 2008), 497–529.

[4] R. Whitt, 'A Deference to Protocol: Fashioning a Three-dimensional Public Policy Framework for the Internet Age', *Cardozo Arts and Entertainment Law Journal* 31 (2013), 689–768; M. Burri, 'Understanding and Shaping Trade Rules for the Digital Era', in M. Elsig, M. Hahn and G. Spilker (eds), *The Shifting Landscape of Global Trade Governance* (Cambridge: Cambridge University Press, 2019), 73–106.

[5] M. Burri and T. Cottier (eds), *Trade Governance in the Digital Age* (Cambridge: Cambridge University Press, 2012); A. Chander, The *Electronic Silk Road: How the Web Binds the World in Commerce* (New Haven: Yale University Press, 2013). Kommerskollegium, *Everybody Is in Services: The Impact of Servicification in Manufacturing on Trade and Trade Policy* (Stockholm: Swedish National Board of Trade, 2012); Kommerskollegium, *No Transfer, No Production: Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods* (Stockholm: Swedish Board of Trade, 2015).

[6] L. Floridi, *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality* (Oxford: Oxford University Press, 2014); K. Schwab, *The Fourth Industrial Revolution* (New York: Portfolio, 2017); WTO, *World Trade Report 2018: The Future of World Trade: How Digital Technologies Are Transforming Global Commerce* (Geneva: World Trade Organization, 2018).

artificial intelligence (AI) as distinct new phenomena, that both policy and academic circles, not exclusively in the area of trade, recognized the need for a change in legal design that goes beyond plain adjustments.[7]

These later stages exposed also in a new way the link between digital trade, or data-enabled/driven trade and privacy protection and their regulation became intensely contested. Previously privacy and trade law were rarely connected and nor has their interface been addressed in the legal frameworks.[8] While there has been a robust scholarly and policy debate on the impact of the 'hard' rules of international economic law on non-economic interests,[9] privacy has rarely been one of the major concerns.[10] The new field of contestation was defined on the one hand by the increased value of data and the affordances of Big Data and Big Data analytics.[11] In this context, there is now broad agreement that data is so essential to economic processes that it is commonly said to be the 'new oil'.[12] Many studies have revealed the vast potential of data,[13] and the dependence of new and emerging technologies, like AI,[14] on data.

On the other hand, this increased dependence on data brought about a new set of concerns. The impact of data collection, use and re-use upon privacy was particularly recognized by scholars and policy-makers alike.[15] These challenges triggered a new preoccupation for law-makers and led to reform of data protection laws around the world, best exemplified by the EU General Data Protection Regulation (GDPR).[16] The reform initiatives are however not coherent and are

---

[7] See e.g. 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); N. Henke et al., *The Age of Analytics: Competing in a Data-Driven World* (Washington, DC: McKinsey Global Institute, 2016); A. Renda, *Artificial Intelligence: Ethics, Governance and Policy Challenges*, A Report of the CEPS Task Force (2019).

[8] 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.

[9] See e.g. A.T.F. Lang, 'Reflecting on "Linkage": Cognitive and Institutional Change in the International Trading System', *The Modern Law Review* 70 (2007), 523–549.

[10] With few exceptions: see e.g. G. Shaffer, 'Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards', *Yale Journal of International Law* 25 (2000), 1–88; G. Shaffer, 'Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance through Mutual Recognition and Safe Harbor Agreements', *Columbia Journal of European Law* 9 (2002), 29–77.

[11] For definitions, see e.g. Mayer-Schönberger and Cukier, *supra* note 7; 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.

[12] *The Economist*, 'The World's Most Valuable Resource Is No Longer Oil, but Data', print edition, 6 May 2017. This however is a somewhat flawed statement, since data is not exhaustible and may lose its usefulness over time. See e.g. 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.

[13] See e.g. Manyika et al.; Mayer-Schönberger and Cukier, both *supra* note 7; N. Henke et al., *The Age of Analytics: Competing in a Data-Driven World* (Washington, DC: McKinsey Global Institute, 2016).

[14] K. Irion and J. Williams, *Prospective Policy Study on Artificial Intelligence and EU Trade Policy* (Amsterdam: The Institute for Information Law, 2019); A. Chander, 'Artificial Intelligence and Trade', M. Burri (ed), *Big Data and Global Trade Law* (Cambridge: Cambridge University Press, 2021), 115–127.

[15] 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; J.R. Reidenberg, 'The Transparent Citizen', *Loyola University Chicago Law Journal* 47 (2015), 437–463, at 438–448.

[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 L [2016] 119/1 [hereinafter *GDPR*].

culturally and socially embedded, reflecting societies' understandings of constitutional values, relationships between citizens and the state, and the role of the market, as illustrated later on by a reference to the US and EU's approaches to data protection.

The tensions around data have revived also older questions about sovereignty and international cooperation in cyberspace.[17] Data's intangibility and pervasiveness pose particular difficulties for determining where data is located, as bits of data, even those associated with a single transaction or online activity, can be located anywhere.[18] With the increased value of data and the associated risks and because of the contentious jurisdictional issues, governments have proactively 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.[19] Erecting barriers to data flows has however serious implications for trade[20] and brings about a tension between data protectionism and data sovereignty and the inherent to trade agreements striving to liberalize trade, foster growth and innovation.

Overall, with the amplified role of data in societies, the interfaces between trade and privacy protection have become multiple and intensified. They raise important questions as to adequate regulatory design that can reconcile economic and non-economic concerns, national and international interests. This article is set against this complex backdrop and seeks to provide a better understanding and contextualization of the topic of data protection as a matter of trade law. It looks at the recent proliferation of rules on data flows, specifically addressed in free trade agreements (FTAs), at how data protection has been framed in these treaties as well as at the available reconciliation (or escape) mechanisms developed to interface trade and privacy. The article explores the most advanced models that have been developed in this regard so far with a focus on some US-led and EU-led treaties. These analyses build the basis to test the conjecture of whether trade law has gone too fast and too deep encroaching on domestic privacy law developments that unfold at a much slower pace.

B. The regulation of data flows and data protection in FTAs

I. Overview of data-relevant rules

As legal adaptation under the umbrella of the WTO has stalled and despite the current reinvigoration of the e-commerce negotiations,[21] many issues of digital trade and of data governance have been addressed in preferential agreements, either of bilateral or regional nature. Out of the 360 FTAs entered into between 2000 and 2022, 196 FTAs contain digital trade provisions, and all recent ones definitely tackle the topic.[22] The United States has been a

[17] See e.g. K.E. Eichensehr, 'The Cyber-Law of Nations', *The Georgetown Law Journal* 103 (2015), 317–380, at 313–334.

[18] See e.g. Eichensehr, ibid.

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

[20] 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, *supra* note 19.

[21] See e.g. M. Burri, 'Towards a New Treaty on Digital Trade', *Journal of World Trade* 55 (2021), 77–100; P. Kerneis, 'The Landing Zone in Trade Agreements for Cross-Border Data Flows', *Jean Monnet Network TIISA Working Paper* 2021-12 (2021); M. Burri, 'A WTO Agreement on Electronic Commerce: An Enquiry into its Substance and Viability', Trade Law 4.0 Working Paper No 1/2021 (forthcoming *Georgetown Journal of International Law* 53 (2023)).

[22] 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*

major driver of these developments endorsing liberal rules in the implementation of its 2002 'Digital Agenda', which defined clear objectives in the area of electronic commerce, including an acknowledgement of the importance of maintaining free flows already at that point of time[23] and has been implemented in a dozen follow-up US-led agreements. 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.[24] Singapore, Australia, Japan and New Zealand have been amongst the drivers of this diffusion but developing countries, like Chile, has also been proactive.

While one can argue that multiple rules found in trade treaties can be of relevance to data, such as those found in the chapter on trade in services or IP,[25] the last decade has witnessed the adoption of new rules that explicitly regulate data flows, although still in a limited number of agreements. This section focuses on these rules that can be found in the dedicated electronic commerce chapters of more recent FTAs in particular, as well as in the new generation of digital economy agreements (DEAs). Particularly important in this context were the negotiations of the Transpacific Partnership Agreement (TPP) between the United States and eleven countries in the Pacific Rim,[26] as the TPP sought to be a distinctly modern trade deal.[27] 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) 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's and the USMCA's electronic commerce chapters build upon the TPP and in this sense reflect the US agenda on the relevant issues. Importantly, they also create a comprehensive template for digital trade with strong rules on data flows. The next section looks in turn at these treaties.

1. Data flows provisions in US-led trade deals

The CPTPP sought for the first time to explicitly curb data protectionism. This is achieved on the one hand through a ban on localization measures;[28] on the other hand, there is also a binding language on free data flows: '[e]ach Party *shall* allow the cross-border transfer of information by electronic means, including personal information'.[29] The rule has a broad scope and notably explicitly covers personal information. After the withdrawal of the United States from the TPP, there was some uncertainty as to the direction the US will follow in its trade deals in general and on matters of digital trade in particular. The USMCA cast 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

International Economic Law 23 (2020), 187–220; for updated data, see: http://unilu.ch/taped.

[23] See Bipartisan Trade Promotion Authority Act of 2002 (Section 2102(b)(9) on e-commerce); also S. Wunsch-Vincent, 'The Digital Trade Agenda of the US: Parallel Tracks of Bilateral, Regional and Multilateral Liberalization', *Aussenwirtschaft* 1 (2003), 7–46.

[24] See e.g. M. Elsig and S. Klotz, 'Data Flow-Related Provisions in Preferential Trade Agreements: Trends and Patterns of Diffusion', in M. Burri (ed), *Big Data and Global Trade Law* (Cambridge: Cambridge University Press, 2021), 42–62.

[25] 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).

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

[27] 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.

[28] Article 14.13(2) CPTPP.

[29] Article 14.11(2) CPTPP.

clear ban on data localization,[30] as well as a hard rule on free information flows.[31]

It is important to note that the CPTPP created a template that has diffused in a number of subsequent treaties, such as the 2016 Chile-Uruguay FTA, the 2016 Updated Singapore-Australia FTA, the 2019 US-Japan Digital Trade Agreement (DTA), which also covers financial and insurance services, and the dedicated 2020 Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand and Singapore, to mention but a few. The impact of the CPTPP model is also likely to be augmented with the approval for the UK to accede to the CPTPP[32] and recent requests for accession by and China and Taiwan.[33]

2. Data flows provisions in EU-led trade deals

In contrast, the European Union has been in general cautious when committing in the area of digital trade[34] and particularly so, when inserting rules on data in its free trade deals. 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,[35] 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 – basically creating a placeholder, which may however be contingent on changes in the domestic privacy regimes. In more recent years, the EU has repositioned itself on the issue of data flows, which is now fully endorsed in the EU's currently negotiated deals with Australia, New Zealand[36] and Tunisia, which include in their draft digital trade chapters norms on the free flow of data and data localization bans. This repositioning has been confirmed by the now finalized post-Brexit Trade and Cooperation Agreement (TCA) between the EU and the United Kingdom,[37] while the EU's position in the WTO negotiations on electronic commerce is somewhat less straightforwardly expressed.[38] The newer commitments are however also linked with the high data protection standards of the GDPR,[39] as discussed in more detail below.

II. Rules on data protection and reconciliation mechanisms

As earlier mentioned, data protection has not been a 'classic' trade topic but its significance has increased over the years and some 90 FTAs do include provisions on data protection. Yet, the nature of the awarded protection varies considerably, which is symptomatic of the very different

---

[30] Article 19.12 USMCA.
[31] Article 19.11 USMCA.
[32] On 1 February 2021, the UK formally requested to join the CPTPP and on 2 June 2021, the CPTPP commission agreed to start negotiations. For details on the UK's goals, see UK Department for International Trade, *UK Accession to CPTPP: The UK's Strategic Approach* (London: Department for International Trade, 2021).
[33] US Congressional Research Service, 'China and Taiwan Both Seek to Join the CPTPP', 24 September 2021, at https://crsreports.congress.gov/product/pdf/IN/IN11760
[34] See e.g, Burri (2017), supra note 25.
[35] Article 8.81 EU-Japan EPA.
[36] The EU–NZ FTA has now been completed but the final treaty text is not yet available.
[37] 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 444/14.
[38] 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, also Burri (2022), supra note 21.
[39] 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 .

positions that states have and the inherent tensions between the regulatory goals of data innovation and data protection. Beyond some earlier agreements, which included mere hortorary or cooperation provisions on privacy protection, increasingly and more importantly, FTAs have included references to the adoption or maintenance of legislation or regulations that protect the personal data or privacy of users in their respective domestic regimes. Representative of this group are the CPTPP and the USMCA. Yet, while the CPTPP requires a legal framework in place,[40] it specifies no standards or benchmarks, except for a general requirement that CPTPP parties 'take into account principles or guidelines of relevant international bodies'.[41] 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'.[42] Parties are also invited to promote compatibility between their data protection regimes, by essentially treating lower standards as equivalent.[43] Overall, the goal seems to be to prioritize trade over privacy rights and it is apparent that even low standards of data protection, such as the ones in the US, are likely to pass the test.

It should be highlighted in this context that the USMCA has two novel aspects when compared to the CPTPP and the usual US position on data protection issues: While Article 19.8 remains soft on prescribing domestic regimes on personal data protection, it makes an explicit reference to established frameworks and states 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)'.[44] Furthermore, the APEC Cross-Border Privacy Rules system, which is discussed below in this article, is recognized as a valid mechanism to facilitate cross-border information transfers while protecting personal information.[45] 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,[46] and aim to provide remedies for any violations.[47] While the immediate legal effect of such commitments is difficult to identify, this is peculiar because it goes beyond what the US may have in its national laws on data protection and also because it reflects some of the principles the EU has advocated for in the domain of the protection of privacy.

In terms of reconciliation mechanisms, measures restricting data flows or localization requirements are permitted only if they serve 'a legitimate public policy objective'; 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'.[48] These conditions are similar to the test formulated by the general exception clauses

[40] 14.8(2) CPTPP.
[41] Article 14.8(2) CPTPP.
[42] Article 14.8(2) CPTPP, at footnote 6.
[43] Article 14.8(5) CPTPP.
[44] Article 19.8(2) USMCA.
[45] Article 19.8(6) USMCA.
[46] Article 19.8(3) USMCA.
[47] Article19.8(4) and (5) USMCA.
[48] Article 14.11 CPTPP. The ban on localization measures is somewhat softened with regard to financial services and institutions. 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,

under WTO law,[49] which 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. This permits more regulatory autonomy for the CPTPP signatories; however, it also may lead to abuses and overall legal uncertainty until some precedents emerge. The USMCA keeps the exception clause[50] and follows the CPTPP model, also clarifying 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',[51] which effectively makes a link to the necessity test under WTO law and practice.[52]

The EU has sought more and more binding 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.[53] 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, as exemplified by the additional adequacy decisions of the European Commission, that we discuss below.

As noted earlier, the EU wishes to permit data flows only if coupled with the high data protection standards of the GDPR. In this sense, the EU commitments to cross-border data flows and the ban on localization measures are conditioned: first, as the currently negotiated deals with Australia, New Zealand and Tunisia show, this happens through a dedicated article on data protection, which clearly states that: 'Each Party recognises that the protection of personal data and privacy is a *fundamental right* and that high standards in this regard contribute to trust in the digital economy and to the development of trade'.[54] Interestingly in this context, the post-Brexit TCA has a somewhat different formulation but can be said to convey essentially the same meaning,[55] as the UK has incorporated the European Convention on Human Rights (ECHR) via the Human Rights Act 1998 in its domestic law.[56] The second condition is given through a paragraph on data sovereignty: 'Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the

---

or for prudential reasons. Government procurement is also excluded.

[49] Article XIV GATS and Article XX GATT 1994.

[50] Article 19.11(2) USMCA.

[51] Article 19.11(2), footnote 5.

[52] See e.g. G. Muller, 'The Necessity Test and Trade in Services: Unfinished Business?', *Journal of World Trade* 49 (2015), 951–973; M. Du, 'The Necessity Test in World Trade Law: What Now?', *Chinese Journal of International Law* (2016), 817–847;

[53] See e.g. Cameroon–EC Interim EPA, Chapter 6, Articles 61–65; CARIFORUM–EC EPA, Chapter 6, Articles 197–201.

[54] See Article 6(2) draft EU–Australia FTA (emphasis added). The same wording is found in the draft EU–New Zealand and the EU–Tunisia FTAs.

[55] 'Each Party recognises that individuals have a right to the protection of personal data and privacy and that high standards in this regard contribute to trust in the digital economy and to the development of trade' (Article 202(1) TCA).

[56] See K. Irion and M. Burri, Digitaler Handel (Commentary of the Digital Trade Title of the EU-UK Trade and Cooperation Agreement) in G. Kübek, C.J. Tams, J.P. Terhechte (eds), *Handels- und Kooperationsvertrag EU/GB Handbuch* (Baden-Baden: Nomos, 2022), 343–368.

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'.[57] The EU also wishes to retain the right to correct future developments during the implementation of the FTA depending on how data flows impact the conditions of privacy protection, so there is a review possibility within 3 years of the entry into force of the agreement and parties remain free to request a review of the list of restrictions at any time, which is to be accorded sympathetic consideration.[58] In addition, there is a broad carve-out, in the sense that, '[t]he Parties reaffirm the right to regulate within their territories to achieve legitimate policy objectives, such as the protection of public health, social services, public education, safety, the environment including climate change, public morals, social or consumer protection, privacy and data protection, or the promotion and protection of cultural diversity'.[59] The EU thus reserves ample regulatory leeway for its current and future data protection measures, and essentially can in many ways condition and restrict data flows. The exceptions are also fundamentally different than the objective necessity test under the CPTPP and the USMCA, or that under WTO law, because it is subjective in nature and safeguards EU's right to regulate.[60]

One should also be reminded that many agreements following the EU model, such as the draft e-commerce chapter of the countries of the European Free Trade Area (EFTA)[61] but also the DEPA,[62] include a general exception clause with a reference to Article XIV GATS and Article XX GATT 1994 to be applied *mutatis mutandis,* and permit exceptions across all sectors and on top of the mentioned carve-outs.[63] It is unclear how this reconciliation mechanism would work in practice in general, as a recent decision of the New Zealand's Waitangi Tribunal showed,[64] and specifically for the protection of privacy, as it is only Article XIV GATS that permits such an exception and it has never been tested before a WTO panel or the Appellate Body.[65]

---

[57] See Article 6(2) draft EU–Australia FTA. The same wording is found in the draft EU–New Zealand and the EU–Tunisia FTAs. Article 202(2) TCA contains again a slightly different formulation: 'Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border data transfers, provided that the law of the Party provides for instruments enabling transfers under conditions of general application for the protection of the data transferred', with a footnote: 'For greater certainty, "conditions of general application" refer to conditions formulated in objective terms that apply horizontally to an unidentified number of economic operators and thus cover a range of situations and cases'.

[58] Article 5(2) draft EU–Australia FTA. The same wording is found in the draft EU–New Zealand and the EU–Tunisia FTAs. Article 201(2) TCA.

[59] Article 2 draft EU–Australia FTA and Article 198 TCA. The same wording is found in the draft EU–New Zealand and the EU–Tunisia FTAs.

[60] 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.

[61] The EFTA countries are Lichtenstein, Norway, Switzerland and Iceland. They have so far not included any e-commerce provisions in their FTAs, as a group or separately, except for the Japan-Switzerland FTA of 2009, which has some, mostly non-binding provisions on digital trade.

[62] Article 13.1 DEPA.

[63] It is often the case that there are sectorial carve-outs too that this article does not elaborate upon – for instance, in the areas of audiovisual and financial services, as well as government procurement.

[64] New Zealand's Waitangi Tribunal, Report on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (November 2021).

[65] On how this may work, see K. Irion, S. Yakovleva and M. Bartl, *Trade and Privacy: Complicated Bedfellows?* (Amsterdam, Institute for Information Law, 2016); D.A. MacDonald. and C.M. Streatfeild, 'Personal Data Privacy and the WTO', *Houston Journal of International Law* 36 (2014), 625–652; M. Burri, 'Interfacing Privacy and Trade', *Case Western Journal of International Law* 53 (2021), 35–88.

C. Reconciliation models outside of the trade law framework

I. The OECD and the APEC frameworks for interfacing trade and privacy

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. [66] The 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[67] 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.[68] 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; (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.[69] Yet, the core principles remained unaltered as well as the two key features of the OECD system, which 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.[70]

The 2005 APEC Privacy Framework[71] is in many ways similar to the OECD Privacy Guidelines but applies in contrast exclusively to processing of personal data in the private sector.[72] It 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 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 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.[73] A newer development in the context of non-binding mechanisms is the recent initiative

---

[66] OECD, *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, OECD Digital Economy Papers (2011), 176, at 7.
[67] OECD, *Guidelines for the Protection of Personal Information and Transborder Data Flows* (OECD, 1980).
[68] Ibid.
[69] OECD, *The OECD Privacy Framework: Supplementary Explanatory Memorandum to the Revised OECD Privacy Guidelines* (OECD, 2013).
[70] Ibid.
[71] APEC, *APEC Privacy Framework* (Singapore: APEC Secretariat, 2005).
[72] The APEC framework endorses similar to the OECD Privacy Guidelines principles: (1) preventing harm; (2) notice; (3) collection limitations; (4) use of personal information; (5) choice; (6) integrity of personal information; (7) security safeguards; (8) access and correction; and (9) accountability. See G. Greenleaf, 'The APEC Privacy Initiative: "OECD Lite" for the Asia-Pacific?', *Privacy Laws and Business* 71 (2004), 16–18.
[73] 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.

championed by the US[74] of a Global CBPR Forum as a novel international cooperation on cross-border flows, which, while following a similar to APEC's certification mechanism, is outside of its institutional umbrella and to be governed by an independent secretariat.[75]

II. Unilateral reconciliation models: The European Union's approach

The EU subscribes to a robust 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,[76] the Charter of Fundamental Rights of the European Union (CFREU)[77] distinguishes between the right of respect for private and family life in Article 7 and the right to protection of personal data, which is explicitly enshrined in Article 8. This distinction reflects the heightened concern of the EU and translates into a positive duty to implement an effective protection of personal data. The 1995 Data Protection Directive formed an important part of this ongoing project of the EU.[78] As the regulatory environment profoundly changed, in particular the use and role of data in the economy but also in broader societal contexts, and also due to the exogenous shock of the 2013 Snowden revelations that exposed the breadth and depth of surveillance by the US National Security Agency (NSA),[79] there was an urgency to update EU data protection law. Reflecting these developments, the 2016 GDPR endorses particularly high standards of protection including enhanced user rights and heightened obligations for data controllers and processors.

Noteworthy for the article's discussion is the firm grasp of the GDPR in terms of its territorial reach. Beyond companies established in the EU, the GDPR may 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.[80] While admittedly there is a nexus with the EU jurisdiction, as the rights of EU citizens may be affected,[81] this is in effect a substantial extension of the scope of EU data protection law, which is now applicable to many US and other foreign companies targeting the EU market.[82]

In the context of the extraterritorial application of the GDPR and what has been particular

---

[74] Along with Canada, Japan, the Republic of Korea, the Philippines, Singapore and Chinese Taipei.

[75] US Department of Commerce, Global Cross-Border Privacy Rules Declaration, available at: https://www.commerce.gov/global-cross-border-privacy-rules-declaration

[76] Article 8 ECHR.

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

[78] 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.

[79] *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.

[80] Article 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 (Article 3), version 2.0, 12 November 2019).

[81] See e.g. C. Ryngaert and M. Taylor, 'The GDPR as Global Data Protection Regulation?', *AJIL Unbound* 45 (2019), 5–9.

[82] See e.g. P.M. Schwartz, 'Information Privacy in the Cloud', *University of Pennsylvania Law Review* 161 (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', *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).

controversial is the possibility of the European Commission to find that a third country offers 'an adequate level of data protection' – 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,[83] or in other words, transfers to the third country become assimilated into intra-EU transmissions of data. The European Commission has so far recognized a selected number of countries, including Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, South Korea, the United Kingdom and Uruguay.[84] The adequacy test has also been made more stringent over time, in particular under the influence of the decisions of the Court of Justice of the European Union (CJEU), so that the Commission needs to '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'.[85]

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.[86] 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 contractual clauses (SCCs) 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. Some of these additional avenues, in particular the SCCs have become widely used but can still be linked to higher costs for businesses in comparison to the all-encompassing adequacy decision.[87]

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 businesses that use EU citizens' data under the GDPR. Finding adequacy has been somewhat problematic with the EU's key partner in global data-driven economy, namely the US.[88] The United States shares a fundamentally different idea of privacy protection, which is deeply rooted in its history and understood as protection of liberty[89] and in this sense 'focuses more on restrictions, such as the Fourth Amendment, that protect citizens from information collection and use by government rather than private actors. Data protection in the US is regulated in a fragmented manner in some federal privacy laws and a great number of state laws.[90] These laws

---

[83] Article 45(1); Recital 103 GDPR.

[84] For all decisions and updates, *see* https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[85] Recital 104 and Article 45(2) GDPR.

[86] Article 46(1) GDPR.

[87] G. Drake, 'Navigating the Atlantic: Understanding EU Data Privacy Compliance Amidst a Sea of Uncertainty', *Southern California Law Review* 91 (2017), 163–194; E. van der Marel, 'Regulating the Globalization of Data: Which Model Works Best?', *ECIPE Policy Brief* No 9 (2021).

[88] 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).

[89] 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.

[90] See e.g. I. Tourkochoriti, 'Speech, Privacy and Dignity in France and in the USA: A Comparative Analysis',

either concern the public sector only or 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.[91] Furthermore, there are no restrictions on the transfer of personal data by private entities; data is seen as a transaction commodity and data exports to other countries are not limited, at least thus far and not due to privacy concerns.[92] Overall, there is a clear tendency towards liberal, market-based governance in contrast to the socially protective, rights-based governance in Europe.[93] Even recent efforts at the state level to endorse stronger consumer privacy rights, such as the ones in the state of California, do show major differences to the EU fundamental rights' model.[94]

The divergence in the overall approach, as well as the protection on the ground granted in the US in specific sectors, could hardly be deemed adequate under the EU standards.[95] This has led to intense politization of the topic and to the creation of an ingenious set of legal mechanisms that permit transatlantic data transfers while providing certain safeguards. The hybrid mechanisms, under the 'Safe Harbor'[96] and later under the 'Privacy Shield'[97] schemes, have been however under substantial pressure, both politically and in courts and have been adjusted over time due to this pressure. Indeed, these schemes have until now not survived the scrutiny of the CJEU, which found in its *Schrems I*[98] and *Schrems II* decisions[99] that level of protection of EU citizens' data was not adequate and up to the EU standards and invalidated the respective Commission's decisions.[100] This despite certain upgrades subsequent to the first *Schrems* judgment, including stronger obligations upon US companies to protect the personal data of European citizens according to a set of clearly defined principles;[101] stronger monitoring and

---

Loyola of Los Angeles International and Comparative Law Review 38 (2016), 101–182.

[91] 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.

[92] This may be changing with new geopolitics online, especially with regard to China. The US has started in this sense to impose certain restrictions to cross-border flows of personal data invoking its national security authority. See E. Rosenbach and K. Mansted, 'The Geopolitics of Information', *Belfer Center for Science and International Affairs* (2019).

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

[94] A. Chander, M.E. Kaminski and W. McGeveran, 'Catalyzing Privacy Law', *University of Colorado Law Legal Studies Research Paper* No 19-25 (2019).

[95] *See* Shaffer (2000), *supra* note 10, at 26; *see* also Schwartz, *supra* note 89, at 1980; B. Petkova, 'Privacy as Europe's First Amendment', *European Law Journal* 25 (2019), 140–154. For a different perspective, *see* K.A. Bamberger and D.K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (Cambridge: MIT Press, 2015).

[96] 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.

[97] 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.

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

[99] Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (Shrems II),* judgment of 16 July 2020, ECLI:EU:C:2020:559.

[100] See supra notes 96 and 97.

[101] European Commission's Implementing Decision, *supra* note 97, paras. 19–29 refer to the Notice Principle,

enforcement mechanisms;[102] enhanced individual safeguard mechanisms and an explicit assurance from the US that any access of public authorities to personal data will be subject to clear limitations, safeguards, and oversight mechanisms.[103] Despite these additional safeguards, in the judgment of *Schrems II* the CJEU still found 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;[104] the lack of necessary limitations on the power of the US authorities, particularly in light of proportionality requirements;[105] and the lack of remedies for EU data subjects,[106] including deficiencies in the ombudsman mechanism.[107] The *Schrems II* judgment had an immediate effect and the standard contractual clauses became the common way to allow transatlantic data transfers, however with additional burden placed on data exporters and importers and the demand for additional organizational and technological measures. The newly agreed upon Trans-Atlantic Data Privacy Framework,[108] whose text is to be finalized until the end of the year, would certainly offer certain improvements to the system but its standing under the scrutiny of the CJEU remains uncertain and might 'meet the same ignoble end before the CJEU as its predecessors'.[109]

III. Evaluating the different reconciliation mechanisms

Each of the existing models does come with certain pros and cons. The regimes under the OECD and APEC, whereas 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[110] and for some countries, like the EU Member States, that demand treating privacy as a fundamental right with priority over economic interests as well as appropriate checks and balances for the protection of individual rights, they may plainly be not enough. In the area of international trade law, 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. Indeed, we do not know much yet on how these tailored general exception clauses would work on the ground and whether they are adequately designed to tread

---

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.

[102] Organizations could choose independent recourse mechanisms in either the EU or in the US, including the possibility to voluntarily cooperate with the EU data protection authorities (DPAs). Where organizations process human resources data, the cooperation with the DPAs was mandatory. Other recourse alternatives included independent Alternative Dispute Resolution or private-sector developed privacy programmes that committed to the Privacy Principles. 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.

[103] European Commission, ibid., at paras. 64–90. For a great analysis of the EU-US Privacy Shield, *see* Deckelboim, supra note 91.

[104] Ibid., para. 164.

[105] Ibid., paras. 168–185.

[106] Ibid., paras. 191–192.

[107] Ibid., paras. 193–197.

[108] See European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework, Press Release, 25 March 2022, available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087

[109] A. Chander and P.M. Schwartz, 'Privacy and/or Trade', *University of Chicago Law Review* 90:1 (forthcoming 2023), available at: http://dx.doi.org/10.2139/ssrn.4038531

[110] See Chander and Schwatz, ibid.

the fine line between curbing data protectionism and protecting legitimate public interests, even for a pro-digital trade oriented and a CPTPP-member country as New Zealand.[111] Coupled with the low privacy protection guarantees that these trade 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 affirm data protection as a fundamental human right in its FTAs and carve out policy space for current and future measures that secure effective safeguards, as a reflection of the provided protection of EU citizens.[112] The EU also exports its high standards of protection through an extension of the territorial application of the GDPR and unilateral or mutual recognition adequacy decisions that short of international harmonization provide for an adequate level of protection of EU citizens' data. This EU approach, which only fuels the 'Brussels effect', whereby firms are under pressure to conform with the EU domestic standards, so that they can access the market,[113] while justified on the side of the EU, may be linked to higher costs of compliance for foreign (and local) firms and countries and may have negative implications even for the EU's economy and its innovation capabilities in the era of Big Data and AI. The EU itself may be in a hot spot, as on the one hand the GDPR framework may be found in violation of WTO law and the adequacy decisions may fail the test of the EU Charter of Fundamental Rights.[114] Down the road, the EU maximalist approach can also be viewed as a hurdle to finding any global solutions[115] and linked to legal uncertainty, as the repeated invalidation of the EU–US transatlantic data flows schemes shows.

D. Different speeds of legal adaptation: has trade law trumped data protection?

The particularly dynamic landscape of digital trade rule-making, of which this article captures only a small portion,[116] may lead one to think that the FTA provisions agreed upon may be going too fast and too deep in a way that encroaches upon the developments in domestic privacy protection regimes, which tend to conventionally develop at a much slower pace due to constitutional, political and cultural constraints. This concern about the different speeds of legal adaptation is then often linked to the discussion on whether trade venues are in the first place suitable to address all issues of data governance, which considering some of the drawbacks of trade law-making, which remains opaque, state-centric, top-down with no proper stakeholder participation[117] but lobbyist influence, is probably not the case.[118] Yet, the real picture with

---

[111] See in this sense New Zealand's Waitangi Tribunal, Report on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, supra note 64 (the report concluded that the risks to Māori interests arising from the e-commerce provisions of the CPTPP are significant, and that reliance on the exceptions and exclusions to mitigate that risk falls short of the Crown's duty of active protection).

[112] S. Yakovleva, 'Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade "Deals"?', *World Trade Review* 17 (2018), 477–508.

[113] 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).

[114] S. Yakovleva, 'Personal Data Transfers in International Trade and EU Law: A Tale of Two "Necessities"', *Journal of World Investment and Trade* 21 (2020), 881–919.

[115] Such as those suggested for instance by Chander and Schwartz, *s*upra note 109.

[116] See e.g. Burri and Polanco, supra note 22; Burri (2022), supra note 21.

[117] For suggestions for broader stakeholder involvement and alignment with the principles of Internet Governance, see N. Mishra, 'Building Bridges: International Trade Law, Internet Governance and the Regulation of Data Flows', *Vanderbilt Journal of Transnational Law* 52 (2019), 463–509.

[118] The discussion on the boundaries of the WTO and trade law in general is not new. See e.g. A. Bradford, 'When the WTO Works, and How It Fails', *Virginia Journal of International Law* 51 (2010), 1–56; S. Cho and C.R. Kelly, 'Are World Trading Rules Passé?', *Virginia Journal of International Law* 53 (2013), 623–666; with regard to data protection, *see* Yakovleva, supra note 60.

regard to the contestation between free data flows and privacy protection may be more complex and less clear-cut than one expects, since while the US-led model has placed trade before privacy and does enjoy some diffusion across other agreements, the EU has also successfully pushed the adoption of its high standards of personal data protection and secured dependencies of multiple trade partners through its adequacy decisions. The GDPR itself has become a powerful model that has been replicated in a great number of jurisdictions, either through the adoption of new domestic acts or the revision of older ones,[119] which naturally fuels the 'Brussels effect'. In this sense, both major actors have been able to preserve and exert their regulatory preferences and only the difficulty of finding suitable mechanisms for transatlantic data flows still remains a preoccupation linked on the one hand to worries amongst EU institutions and citizens and to higher costs of compliance for US businesses, on the other. A question that then becomes pertinent and has been as yet largely unexplored by scholars is firstly, what happens to countries caught under the regulatory drive of either the US or the EU, which translates into rule-making that may not reflect the country's own preferences and secondly, what happens to countries caught somewhere between the two competing trends. In the former situation, there is a danger in particular for smaller developing countries with weaker regulatory capacities that may enter into US-like FTAs and hard commitments implicating data governance issues under these. In the latter situation, which appears to be common for instance for a number of countries in Latin America (such as Argentina, Uruguay, Mexico, Peru, Paraguay and Columbia), which have both entered into CPTPP-like commitments in FTAs and in GDPR-like domestic regimes, the question is whether conflicts will follow and how governments will manage such conflicts between national laws and international commitments.[120] Overall, the picture is fluid with multiple developments underway, both domestically and on the international scene. There is certainly room for experimentation and learning, to which the evolution of both the digital trade and privacy-related rule-making so far significantly contribute, and as of now both the paths of divergence and convergence remain open.

[119] *See* G. Greenleaf, 'Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance', *Privacy Laws and Business International Report* 169 (2021), 1–5; G. Greenleaf, 'Global Data Privacy Laws 2021: Uncertain Paths for International Standards', *Privacy Laws and Business International Report* 169 (2021), 23–27.

[120] Own research; in the same line, see R. Polanco, 'Regulatory Convergence of Data Rules in Latin America', in M. Burri (ed), *Big Data and Global Trade Law* (Cambridge: Cambridge University Press, 2021), 268–300.