Pitching trade against privacy: reconciling EU governance of personal data flows with external trade

Yakovleva, S.; Irion, K.

DOI
10.1093/idpl/ipaa003

Publication date
2020

Document Version
Final published version

Published in
International Data Privacy Law

Pitching trade against privacy: reconciling EU governance of personal data flows with external trade

Svetlana Yakovleva* and Kristina Irion**

Key Points

- Global data flows underpinning cross-border digital trade have moved centre stage in international trade negotiations. New trade law disciplines on the free flow of data are included in a number of international trade deals.
- The European Union (EU) has a key role to play in the global governance of the protection of personal data. The EU's strict data protection regime has sometimes been framed as a digital trade barrier.
- This article juxtaposes the EU's governance of fundamental rights to privacy and data protection with external trade policy on cross-border data flows.
- The process of aligning EU's normative approach to personal data protection with its external trade policy has been, until very recently, riddled with contradictions.
- The article concludes with an assessment of the EU's recent horizontal strategy on cross-border data flows and personal data protection in trade and investment agreements, which aims to align EU external policy.

Introduction

In today's global economy, digital trade is closely linked to cross-border data flows. A 2016 report of McKinsey Global Institute (MGI), a consultancy firm, estimates that cross-border data flows now exert a larger impact on the global gross domestic product (GDP) than trading goods.[1] Because of the overwhelmingly positive feedback loop of global data flows on international trade, growth and welfare, conflicting public interests and policy objectives can easily appear subordinated. As digital trade flourishes with the free flow of data, the role of privacy within international trade law is becoming increasingly controversial.

In the European Union (EU), the privacy and personal data of citizens and residents are protected as fundamental rights, thereby ascribing them the highest normative value.[2] After four years of intense legislative wrangling, the EU legislator in 2016 adopted the General Data Protection Regulation (GDPR) which entered into force in May 2018.[3] The GDPR continues to make the transfer of personal data to third countries subject to requirements, which intend to ensure that the high level of personal data protection not be undermined. Remarkably, the Regulation applies directly to cross-border commercial transactions involving personal data from the EU, even if an organization operates from outside the EU.[4] Such external effect profoundly impacts suppliers of goods and services from outside the EU.

* Institute for Information Law (IViR), University of Amsterdam, Amsterdam, The Netherlands; De Brauw Blackstone Westbroek, Amsterdam, The Netherlands

** Institute for Information Law (IViR), University of Amsterdam, Amsterdam, The Netherlands. E-mail: k.irion@uva.nl.

The research has been carried out in full compliance with the Netherlands Code of Conduct for Research Integrity (2018). No external funding has been received for research and writing this article. The authors would like to thank Colin Bennett and the paper workshop participants of the 10th Annual Privacy Law Scholars Conference (PLSC, June 1-2, 2017, Berkeley), the Editor of International Data Privacy Law as well as the anonynous reviewers for their helpful suggestions and comments.

1 McKinsey Global Institute, 'Digital Globalization: The New Era of Global Flow' (2016) <https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx> accessed 5 March 2020.

2 Arts 7 and 8 of the Charter of Fundamental Rights of the EU; Art 6(1) of the Treaty on EU.

3 Regulation (EU) 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) (2016) OJ L119/1, *hereinafter* GDPR.

4 Art 3(2) GDPR.

Numerous authors have flagged the potential of international trade law to conflict with a sovereign party's measures to protect privacy.[5] This verdict is derived from the 1994 General Agreement on Trade in Services (GATS),[6] so far the only multilateral international trade agreement concerning international trade in services. A number of authors who have contrasted EU rules on cross-border transfer of personal data against the provisions of the GATS trade liberalization disciplines have found probable inconsistencies between the two.[7] In particular, GATS Article XIV, which defines the scope of a World Trade Organization (WTO) member's autonomy to regulate in the interest of privacy, can be difficult to satisfy.[8] The forthcoming legal challenge for privacy regulation is GATS-plus trade liberalization and the digital trade agenda, which aim to take trade liberalization commitments further than the GATS.

Meanwhile, proposals to liberalize the cross-border flow of data abound in the literature on international trade law.[9] Trade pundits and think tanks that frame the discourse on global data flow frequently single out EU data protection law as an impediment to digital trade.[10] Proponents of global data flows label the EU approach to personal data protection as 'overly restrictive', 'onerous', and 'protectionist'.[11] Intergovernmental organizations with an economic mandate also call to balance concerns over privacy with facilitating global flows of data.[12] As a result, the forum for personal data exports has been masterfully shifted to international trade law, where national measures disruptive to free data flows ought to be justified in light of the trade objective.[13]

Personal data is peculiar in the way it combines the dignity of a human being with economic properties valuable for commercial activity.[14] Aaronson argues

5 See, eg Susan 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' (2015) 14(4) World Trade Review 671; William J Drake and Kalypso Nicolaidis, 'Global Electronic Commerce and GATS: The Millenium Round and Beyond' in Pierre Sauve and Robert M Stern (eds), *GATS 2000: New Directions in Services Trade Liberalization* (The Brookings Institution Press, Washington, DC 1999); Rolf H Weber, 'Regulatory Autonomy and Privacy Standards under the GATS' (2012) 7(1) Asian Journal of WTO and International Health Law and Policy 25; Lee A Bygrave, *Data Privacy Law: An International Perspective* (OUP, Oxford 2014) 199; Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (OUP, Oxford 2013) 52; Perry Keller, *European and International Media Law: Liberal Democracy, Trade and New Media* (OUP, Oxford 2011) 353; Yi-Hsuan Chen, 'The EU Data Protection Law Reform: Challenges for Service Trade Liberalization and Possible Approaches for Harmonizing Privacy Standards into the Context of GATS' (2015) 19 Spanish Yearbook of International Law 211, 211, Joel R Reidenberg, 'E-commerce and Transatlantic Privacy' (2001–2002) 38 Houston Law Review 717, 736–37.

6 GATS, Annex 1B to the 1994 Marrakesh Agreement on Establishing the World Trade Organization (WTO Agreement). Both the EU and its Member States are founding members of the WTO and parties to the GATS.

7 Carla L Reyes, 'WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive' (2011) 12(1) Melbourne Journal of International Law 141; Eric Shapiro, 'All Is Not Fair in the Privacy Trade: The Safe Harbor Agreement and the World Trade Organization' (2003) 71(6) Fordham Law Review 2781; Maria V Perez Asinari, 'Is There Any Room for Privacy and Data Protection within the WTO Rules?' (2002) 9 Electronic Communication Law Review 249.

8 Markus Krajewski, *National Regulation and Trade Liberalization in Services: The Legal Impact of the General Agreement on Trade in Services (GATS) on National Regulatory Autonomy* (Kluwer Law International, The Hague 2003); Jan Wouters and Dominic Coppens, 'GATS and Domestic Regulation: Balancing the Right to Regulate and Trade Liberalization' in Kern Alexander and Mads Adenas (eds), *The World Trade Organization and Trade in Services* (Martinus Nijhoff Publishers, Leiden 2008) 205–64.

9 Hosuk Lee-Makiyama, 'The Political Economy of Data: EU Privacy Regulation and the International Redistribution of Costs' in Luciano Floridi (ed), *Protection of Information and the Right to Privacy - A New Equilibrium?* (Springer International, Cham 2014) 85–94; Joshua P Meltzer, 'The Internet, Cross-border Data Flows and International Trade' (2015) 2 Asia & the Pacific Policy Studies 90; Andrew D Mitchell and Jarrod Hepburn, 'Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-border Data Transfer' (2017) 19(1) Yale Journal of Law and Technology 182, Lee Tuthill, 'Cross-border Data Flows: What Role for Trade Rules?' in Pierre Sauvé and Martin Roy (eds), *Research Handbook on Trade in Services* (Edgar Elger, Cheltenham 2016) 357–82; Margaret B Sedgewick, 'Transborder Data Privacy as Trade' (2017) 105 California Law Review 1513, 1514–15.

10 ECIPE, 'The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce' (2013) <https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf> accessed 5 March 2020; Edward Gresser, 'Lines of Light: Data Flows as a Trade Policy Concept' (*Progressive Economy*, 2012) <http://www.progressive-economy.org/wp-content/uploads/2012/05/05082012-LinesOfLight1.pdf> accessed 5 March 2020; 'Business Without Borders: The Importance of Cross-border Data Transfers to Global Prosperity' (*U.S. Chamber of Commerce, Hunton&Williams*, 2014) <https://www.huntonak.com/images/content/3/0/v3/3086/Business-without-Borders.pdf> accessed 5 March 2020, Michael Mandel, 'Data, Trade and Growth' (*Progressive Policy Institute*, 2014) <http://www.progressivepolicy.org/wp-content/uploads/2014/04/2014.04-Mandel_Data-Trade-and-Growth.pdf> accessed 5 March 2020; McKinsey Global Institute (n 1).

11 Cf Peter P Swire and Robert E Litan, 'None of You Business: World Data Flows, Electronic Commerce, and the European Privacy Directive' (*Brookings Institution Press*, 1998) 76ff; Susan A Aaronson, 'The Digital Trade Imbalance and Its Implications for Internet Governance' (2016) Global Commission on Internet Governance, Paper Series No 25, 7–8, 17 <https://www.cigionline.org/sites/default/files/gcig_no25_web_0.pdf> accessed 4 March 2020; Economics and Statistics Administration and National Telecommunications and Information Administration, 'Measuring the Value of Cross-border Data Flows' (*US Department of Commerce*, 2016) 1 <https://www.ntia.doc.gov/files/ntia/publications/measuring_cross_border_data_flows.pdf> accessed 5 March 2020; UNCTAD, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' (*United Nations Publications*, 2016) 106 <http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf> accessed 5 March 2020.

12 UNCTAD, ibid; OECD, 'Economic and Social Benefits of Internet Openness' (2016) OECD Digital Economy Papers No 257, 10, 23–24 <https://www.oecd-ilibrary.org/economic-and-social-benefits-of-internet-openness_5jlwqf2r97g5.pdf?itemId=%2Fcontent%2Fpaper%2F5jlwqf2r97g5-en&mimeType=pdf> accessed 4 March 2020.

13 Graham Greenleaf, 'The TPP & Other Free Trade Agreements: Faustian Bargains for Privacy?' (2016) UNSW Law Research Paper No 8 <http://classic.austlii.edu.au/au/journals/UNSWLRS/2016/8.pdf> accessed 4 March 2020.

14 Beate Roessler, 'Should Personal Data Be a Tradable Good? On the Moral Limits of Markets in Privacy' in Beate Roessler and Dorota Mokrosinska (eds), *Social Dimensions of Privacy: Interdisciplinary Perspective* (CUP, Cambridge 2015).

that those who say the EU fundamental rights' approach to the protection of privacy and personal data is failing the data-intensive industries are often self-serving.[15] Both, Aaronson and Kaminski cast doubt that trade deals are the right venue to solve the divergences over privacy protection between the USA and the EU.[16] Concurring, Greenleaf invokes a quote attributed to Spiros Simitis when discussing EU/US tensions over the 1995 EU Privacy Directive: 'This is not bananas we are talking about.'[17] To Breining-Kaufmann the 'economization of human rights' other than privacy leads to human rights being instrumentalized for economic ends such as market access.[18] Such reverberations permeate scholarship on the dysfunctional relationship between international trade and human rights law.[19]

Although several of the EU's future trading partners, such as Australia and New Zealand,[20] would like to introduce free data flow provisions in their trade agreements, it is the USA that has traditionally voiced concerns about the trade-restrictive effect of EU's data protection framework most vociferously.[21] Since the late 1990s, the Clinton and then Obama administrations have been harnessing their foreign relations to eliminate what they deem 'digital protectionism'.[22] During the negotiations for the EU–US Transatlantic Trade and Investment Partnership (TTIP) and for a multilateral Trade in Services Agreement (TiSA), the EU and others have been under pressure to bargain over new commitments on free data flow.[23] These commitments were present in the earlier drafts of EU's Economic Partnership Agreement (EPA) with Japan[24] and the revision of the trade agreement with Mexico.[25] This is how international trade law became a new frontier for privacy and data protection in the EU.

The EU is not unique in restricting cross-border data flows, and privacy and data protection are not the sole policy interests behind these restrictions. For example, China has adopted an even more restrictive approach, which applies to both personal and non-personal data, claiming to assert its cybersecurity interests.[26] In its draft National E-Commerce Policy, India's government has called for restrictions on cross-border data flows to ensure that Indian citizens benefit from the monetization of their personal data.[27] Along similar lines, the United Nations Conference on Trade and Development (UNCTAD) argues that 'the only way for developing countries to exercise effective economic "ownership" of and control over the data generated in their territories may be to restrict cross-border flows of important personal and community data'.[28] This article, however, will focus solely on how the

15 Susan A Aaronson, 'Digital Protectionism? Or Label the U.S. Government Uses to Criticize Policy It Doesn't Like?' (*Council on Foreign Relations*, 3 March 2016) <http://blogs.cfr.org/cyber/2016/03/03/digital-protectionism-or-label-the-u-s-government-uses-to-criticize-policy-it-doesnt-like/> accessed 5 March 2020.

16 Margot Kaminski, 'Why Trade Is Not the Place for the EU to Negotiate Privacy' (*Internet Policy Review*, 23 January 2015) <https://policyreview.info/articles/news/why-trade-not-place-eu-negotiate-privacy/354> accessed 5 March 2020; Aaronson (n 11) 21. In a most recent article, however, Aaronson and Leblond suggest that WTO forum could be used to create interoperability between divergent regimes for cross-border data flows (Susan A Aaronson and Patrick Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO' (2018) 21 Journal of International Economic Law 245, 248).

17 Greenleaf (n 13) 3.

18 Christine Breining-Kaufmann, 'The Legal Matrix of Human Rights and Trade Law: State Obligations Versus Private Rights and Obligations' in Thomas Cottier, Joost Pauwelyn and Elisabeth Bürgi (eds), *Human Rights and International Trade* (Oxford: OUP, 2005) 104.

19 Lorand Bartels, 'Trade and Human Rights' in Rüdiger Wolfrum (ed), *Max Planck Encyclopedia of Public International Law* (OUP, Oxford 2012); Cottier, Pauwlyn and Bürgi, ibid; Svetlana Yakovleva, 'Should Fundamental Rights to Privacy and Data Protection Be a Part of the EU's International Trade "Deals"?' (2018) 17(3) World Trade Review, 499–508.

20 See, eg Jyoti Panday, 'E-commerce RCEP Chapter: Have Big Tech's Demands Fizzled?' (*Electronic Frontier Foundation*, 4 August 2017) <https://www.eff.org/deeplinks/2017/08/e-commerce-rcep-chapter-have-big-techs-demands-fizzled> accessed 5 March 2020.

21 See Susan A Aaronson, 'Redefining Protectionism: The New Challenge in the Digital Age' IIEP Working Paper, 2016, 87 <https://www2.gwu.edu/~iiep/assets/docs/papers/2016WP/AaronsonIIEPWP2016-30.pdf> accessed 5 March 2020; Aaronson (n 15).

22 Cf Aaronson (n 11) 6.

23 Cf 'Note-Tactical State of Play of the TTIP Negotiations' (March 2016) 7 <https://wikileaks.org/ttip/Tactical-State-of-Play/Tactical-State-of-Play.pdf> accessed 5 March 2020; Adam Behsudi, 'A Swan Song for TISA Talks' (*Politico*, 14 November 2016) <http://www.politico.com/tipsheets/morning-trade/2016/11/a-swan-song-for-tisa-217394> accessed 5 March 2020.

24 Alberto Mucci, Laurens Cerulus and Hans von der Burchard, 'Data Fight Emerges as Last Big Hurdle to EU-Japan Trade Deal. Brussels Closes in on Its Biggest Trade Agreement' (*Politico*, 12 August 2016) <http://www.politico.eu/article/eu-japan-trade-deal-caught-up-in-data-flow-row-cecilia-malmstrom/> accessed 5 March 2020; European Commission, Statement: Joint Declaration by Mr. Shinzo Abe, Prime Minister of Japan, and Mr. Jean-Claude Juncker, President of the European Commission, 6 July 2017, <http://europa.eu/rapid/press-release_STATEMENT-17-5182_en.htm> accessed 5 March 2020; Marija Bartl and Kristina Irion, 'The Japan EU Economic Partnership Agreement: Flows of Personal Data to the Land of the Rising Sun' (*University of Amsterdam*, 25 October 2017) <https://www.ivir.nl/publicaties/download/Transfer-of-personal-data-to-the-land-of-the-rising-sun-FINAL.pdf> accessed 5 March 2020.

25 The EU Proposal for Chapter on Digital Trade as of April 2017 contained a placeholder for provision on data flows/data localization in art 14 <http://trade.ec.europa.eu/doclib/docs/2017/may/tradoc_155518.pdf> accessed 5 March 2020.

26 For a summary of China's restrictions on cross-border data flows, see Francesca Casalini and Javier López González, 'Trade and Cross-Border Data Flows' (OECD Publishing, Paris, 23 January 2019) OECD Trade Policy Papers, No 220, 22 <https://www.oecd-ilibrary.org/docserver/b2023a47-en.pdf?expires=1575651497&id=id&accname=guest&checksum=A9E4AF04E8F810E54C1A414ED35E32ED> accessed 5 March 2020.

27 IAPP, Indian Government Calls for Cross-border Data Flow Regulation' (25 February 2019) <https://iapp.org/news/a/indian-government-calls-for-cross-border-data-flow-regulation/> accessed 5 March 2020.

28 UNCTAD, Digital Economy Report 2019, 'Value Creation and Capture: Implications for Developing Countries' (2019) 89.

EU's restrictions on data flows play out in international trade context and on the interplay between the goals of protecting privacy and personal data as fundamental rights and digital trade liberalization.

At this moment, the trade and privacy interface has yet to be fully formed, both doctrinally and normatively. The negotiations of TTIP and TiSA are momentarily stalled due to the uncertainties about the new US government's trade policy's strategic directions. Both the final draft version of the EU–Japan EPA and the latest version of the Digital Trade Chapter in trade negotiations with Mexico contain a placeholder for a cross-border data flow provision in the form of a '*rendez-vous*' clause that will allow the parties to reconsider the issue three years after the agreement enters into force.[29] However, the tension between the commitment to free data flows and the regulation protecting privacy and personal data is unlikely to go away. Now that the EU has defined its position on horizontal provisions on cross-border data flows and personal data protection,[30] it is both timely and essential to reassess its strategy on the international transfers of personal data in the purview of its future trade agreements.

This article positions EU's external governance of personal data flows against the backdrop of the international controversy on digital trade versus strict privacy laws. For its own normative approach and regulatory autonomy, the EU has a pivotal role to play in shaping the interface between trade and privacy before the 'free trade leviathan'[31] can restrict the policy choices not only of individual states but also of the EU itself. Our contribution aims to break through the present compartmentalization of privacy scholarship and trade lawyers because it situates personal data flows in both disciplines.

The article is structured as follows. In section 'Framing the controversy on digital trade versus data privacy protection', we critically review the economic narrative underpinning free data flows which have put domestic measures on privacy and personal data protection that affect cross-border digital trade in a defensive position. Next, in section 'Free data flows and the digital trade agenda', we show how international trade diplomacy has been progressively embarking on free data flows first under the auspice of the WTO, and then as a part of the digital trade agenda. The section 'EU external policies: between normative values and economic relations' turns to EU affairs and discusses the internal confrontation between its normative approach to privacy and personal data and its economic approach to international governance of cross-border data transfers. In conclusion, we introduce and evaluate the EU's recent horizontal strategy on cross-border data flows and personal data protection in EU trade and investment agreements.

Framing the controversy on digital trade versus data privacy protection

In the last decades, international trade has shifted towards international trade in digital services. Cross-border information flows now exert a larger impact on the global GDP than the trading of goods.[32] The MGI report estimates that global data flows raised the world GDP by $2.8 trillion in 2014.[33] These overwhelming numbers, although approximate at best, as will be discussed below, create an unprecedented pressure on governments worldwide to open up cross-border data flows.

Data privacy protection as an impediment to digital trade

The intuitive positive feedback loop between cross-border data flows and economic growth has put sovereign states and the EU in a defensive position regarding domestic measures on privacy and personal data protection that affect cross-border digital trade. Foregrounding the added value of data flows to world GDP over privacy protections, the UNCTAD warns that data protection regulation 'must carefully correspond to the evolving needs and possibilities' associated with the value of cross-border data flows in order to facilitate potential benefits.[34] A variety of other policy documents by trade pundits and think tanks rely on the estimates from the above-mentioned MGI report in order to buttress the logic of pursuing trade interests ahead of data privacy.[35]

29 Art 8.81 E-commerce chapter of EU–Japan Economic Partnership Agreement, Text of the Digital Trade Chapter in draft EU–Mexico Agreement announced on 21 April 2018 <http://trade.ec.europa.eu/doclib/docs/2018/april/tradoc_156811.pdf> accessed 5 March 2020.

30 European Commission, 'Horizontal Provisions on Cross-border Data Flows and Personal Data Protection' (news release of 18 May 2018) <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=627665> accessed 13 August 2018.

31 Gráinne de Búrca and Joanne Scott, 'The Impact of the WTO on EU Decision-making' in Gráinne de Búrca and Joanne Scott (eds), *The EU and the WTO Legal and Constitutional Issues* (Hart Publishing, Oxford 2002) 25.

32 McKinsey Global Institute (n 1) at 73.

33 Ibid 10, 73–75.

34 UNCTAD (n 11) Executive Summary, xi.

35 See, eg Peter Chase, Sudha David-Wilp and Tim Ridout, 'Transatlantic Digital Economy and Data Protection: State-of-play and Future Implications for the EU's External Policies' (*Study for the European Parliament*, 2016) 11–13 <http://www.europarl.europa.eu/RegData/etudes/STUD/2016/535006/EXPO_STU(2016)535006_EN.pdf> accessed 5 March 2020.

The proponents of this position argue along at least two lines of reasoning. The first and more traditional argument focuses on the lack of harmonization of data privacy rules across the globe, as well as on the lack of interoperability between these rules. In a connected world, these inconsistencies raise a host of complicated questions over the transnational protection of privacy.[36] The MGI report notes that this lack of uniformity leads to additional compliance costs for companies and thus 'could limit the economic benefits of cross-border data flows'.[37] This issue has been articulated sharply in the context of transatlantic relations between the EU and the USA, whose trade link remains the most important economic link in the world.[38] Trade in digitally deliverable services amounts to a substantial proportion of it.[39] The EU and the USA adhere to radically different normative models of informational privacy, in particular in the field of commerce.[40] A 2014 survey among US firms in 'digitally intensive industries' produced the not very surprising outcome that businesses perceive data protection requirements in the EU as the top obstacle to doing business online for large firms (79 per cent) and the third highest obstacle for small and medium sized enterprizes (51 per cent).[41] To be clear, EU businesses have reported similar concerns since they have to obey the same rules on cross-border transfers of personal data.[42]

The second line of reasoning focuses specifically on EU data protection rules. The GDPR, for example, has been said to 'create[s] barriers to cross-border data transfers to such an extent that they are effectively data localization requirements'.[43] The hypothetical consequences for the EU, by frightening estimations, could lead to a 3.9-per cent loss of EU's GDP, or up to $193 billion in absolute numbers.[44] Chander and Lê contend that such data localization rules threaten the major new advances in information technology, such as cloud computing, the Internet of Things, and big data.[45] Policy research predicts that the 'data gap' between Europe and the USA is likely to grow wider and 'the costs will be felt most profoundly in Europe itself'.[46] The bias towards liberalizing data flows at the expense of rigorous privacy protections is inherent to these claims. However, the premise of these claims is faulty because they do not incorporate a thorough legal analysis of EU law. For instance, EU data protection law does not obstruct cross-border electronic commerce with consumers because it generally permits the transfer of personal data that is necessary for the performance of a contract.[47]

The weak link between measuring data flows and personal data

There are at least three problems with the discourse putting digital trade ahead of domestic data privacy regimes. First, there are no reliable measurements of data flows as yet, and the assessments of their contribution to value creation lack solid methodological grounds. Secondly, wholesale extrapolations from estimations of data flows and their value to the effect of domestic privacy regulation result in a skewed picture. Thirdly, framing the protection of personal data as a barrier to trade focuses only on the cost side of things ignoring the individual and societal benefits of stronger data protection. Ultimately, this approach generates a bipolar landscape that ignores the possibility of a win–win between the protection of privacy and personal data and cross-border data flows. We argue that the numbers that lie at the heart of the quantitative arguments on the economic importance of cross-border data flows and the economic costs of personal data protection should be treated with caution.

36 Dan JB Svantesson, 'The Regulation of Cross-border Data Flows' (2011) 1(3) International Data Privacy Law 180; Gehan Gunasekara, 'The "Final" Privacy Frontier? Regulating Trans-border Data Flows' (2009) 17(2) International Journal of Law and Information Technology 147.

37 McKinsey Global Institute (n 1) 101.

38 European Commission, 'Countries and Regions – United States' <http://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/> accessed 5 March 2020; US International Trade Commission, 'Digital Trade in the U.S. and Global Economies' (July 2013) Part 1, USITC Publication 4415, 4-4.

39 Meltzer (n 9) 4; Chase, David-Wilp and Ridout (n 35) 13ff, US International Trade Commission, 'Digital Trade in the U.S. and Global Economies' (August 2014) Part 2, USITC Publication 4485, 48–49.

40 See James Q Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 Yale Law Journal 1151, 1189ff, Joel R Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (2000) 52 Stanford Law Review 1315, 3120ff.

41 US International Trade Commission (n 39) 83.

42 Kommerskollegium (Swedish National Board of Trade), 'No Transfer , No Trade – the Importance of Cross-border Data Transfers for Companies Based in Sweden' (2014) <https://unctad.org/meetings/en/Contribution/dtl_ict4d2016c01_Kommerskollegium_en.pdf> accessed 5 March 2020.

43 Matthias Bauer and others, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery', ECIPE Occasional Paper No 3/2014, 2014 <https://ecipe.org/wp-content/uploads/2014/12/OCC32014__1.pdf> accessed 5 March 2020.

44 Ibid 2, 3 and 5.

45 Anupam Chander and Uyen P Lê, 'Breaking the Web: Data Localization vs. the Global Internet' (March 2014) UC Davis Working Paper 2014-1, 40ff.

46 Paul Hofheinz and Michael Mandel, 'Bridging the Data Gap: How Digital Innovation Can Drive Growth and Create Jobs' Progressive Policy Institute, Issue 15/2014, 2014, 13 <http://www.progressivepolicy.org/wp-content/uploads/2014/04/LISBON_COUNCIL_PPI_Bridging_the_Data_Gap.pdf> accessed 5 March 2020.

47 Art 49(1) GDPR.

Turning to the first critique, measuring the positive effects of data flows on digital trade is prone to several methodological difficulties.[48] As the above-mentioned reports acknowledge, existing measurements of data flows are derived from proxies and are not necessarily accurate. For example, the 2016 MGI report estimates data flows on the basis of overall use of cross-border bandwidth, a sum of all capacity deployed for Internet backbones, private networks, and switched voice networks.[49] Although claimed as the most precise,[50] this methodology only allows an estimate of the capacity of infrastructure and does not inform of *actual* data flows.[51] Internet traffic, another, even less precise proxy, always suffers from double counting because Internet protocol traffic is not linear and can be routed through several countries.[52] Using cross-border trade in 'digitally enabled services' or 'ICT-enabled services' as a measurement of cross-border data flows leads to even vaguer approximations. 'Data moves' do not correspond to the value of international digital trade, as not all 'digitally enabled' commercial transactions coincide with transfer of data.[53] Similarly, not all information and communications technology (ICT)-enabled trade is digital.[54]

The necessity of using proxies to measure cross-border data flows is dictated by the absence of an agreed definition of digital economy, comprehensive statistics for international digital trade and of reliable metrics to measure digital trade or cross-border data flows.[55] Cross-border data flows are not tracked as a separate category in trade statistics,[56] which are 'mostly uninformative and even misleading' about the magnitude of cross-border data flows.[57] This issue has only recently come to the focus of governments and international organizations, and the initiatives on developing internationally comparable metrics and tools to measure digital trade and cross-border flows of (personal) data are only starting to shape.[58]

When it comes to the value of data flows—the second line of reasoning[59]—it is crucial that the *scale* of data flows does not necessarily correlate with their underlying *economic value*.[60] To be fair, the reported value of data flows can be both under- or overstated.[61] Besides data flows, cross-border trade also generates flows of goods, services, and people. As a result, the effects of other types of flows can be mistakenly attributed to flows of data: according to the above-cited MGI report, one type of flow considered separately may capture more than 60 per cent of value of all flows.[62]

Even if reliable, the measurements of volume and value of cross-border data flows may be misleading in the trade and data privacy discourse, unless it could be clearly established how much of *cross-border data flows* are attributed to flows of *personal data*. In the studies discussed in this article, the link between the value of data flows and the value of personal data among these data flows is weak.[63] Wholesale extrapolation from the estimated benefits of global data flows to the negative effect of domestic privacy and data protection regulation on trade may grossly overstate the magnitude of the effect. Without denying that such regulation can generate substantial compliance costs, there is no sound methodology to attribute the unrealized potential of personal data flows to data protection. Even more importantly, compliance costs cannot be in themselves an argument against regulation imposing them, as long as they serve an important public policy interest, such as

48 Georgios Alaveras and Bertin Martens, 'International Trade in Online Services' (2015) Institute for Prospective Technological Studies Digital Economy Working Paper (2015-08), 6–10 <https://ec.europa.eu/jrc/sites/jrcsh/files/JRC97233_Workingpaper_Alaveras_Martens_InternationalTrade_Online_services_191015.pdf> accessed 5 March 2020; Economics and Statistics Administration and National Telecommunications and Information Administration (n 11) 1–3; OECD (n 12) 33ff.

49 Excluding capacity is used for restoration and redundancy purposes. McKinsey Global Institute (n 1) 111.

50 McKinsey Global Institute (n 1) 32, 75–78.

51 OECD (n 12) 78.

52 Mandel (n 10) 9–10; OECD (n 12) 78.

53 US International Trade Commission (n 38) I, 1-4, 4-3; Mandel (n 10) 5–7; Meltzer (n 9) 4.

54 US International Trade Commission, ibid 4-3.

55 US International Trade Commission (n 38) 4-1; Gresser (n 10) 5; Mandel (n 10) 2–3; UNCTAD Digital Economy Report (n 28) 49–51, 89.

56 Mandel (n 10) 2–3.

57 Ibid.

58 See, eg APEC Privacy Framework (2015) para 61; 'Resolution on Developing New Metrics of Data Protection Regulation' (38th International Data Protection and Privacy Commissioners Conference, Marrakesh, 18 October 2016) <https://edps.europa.eu/sites/edp/files/publication/16-10-18_resolution-developing-new-metrics-of-data-protection-regulation_en_0.pdf> accessed 5 March 2020. An Expert Group created by an inter-agency Task Force on International Trade Statistics is currently working on an OECD-WTO Handbook on Measuring Digital Trade. The first draft of 6 March 2019 is available at <http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=SDD/CSSP/WPTGS(2019)4&docLanguage=En> accessed 5 March 2020.

59 Economics and Statistics Administration and National Telecommunications and Information Administration (n 11)

60 Lee Branstetter, 'TPP and Digital Trade' in Effrey J Schott and Cathleen Cimino-Isaacs (eds), *Assessing the Trans-Pacific Partnership, Volume 2: Innovations in Trading Rules*, PIIE Briefing 16-4 (PIIE, Washington, DC 2016) 74 <https://piie.com/system/files/documents/piieb16-4.pdf> accessed 5 March 2020.

61 Mandel (n 10) 5–7.

62 McKinsey Global Institute (n 1) 78.

63 It is quite plausible that it is mostly not export of personal data but rather of machine-generated data (including jet engines, lifts, and cars) that is responsible for the impressive scale of international data flows. See Annegret Bendiek and Evita Schmieg, 'European Union Data Protection and External Trade. Having the Best of Both Worlds?' (*SWP Comments*, 2016) 2 <https://www.swp-berlin.org/fileadmin/contents/products/comments/2016C11_bdk_scm.pdf> accessed 5 March 2020.

data privacy. On the contrary, these compliance costs could spur innovation by prompting the development and wider use of technologies based on anonymization and differential privacy algorithms, so that less personal data are involved in international transfers.

The positive effects of protecting data privacy

Studies that make far-reaching conclusions about potential negative effects of EU data protection on digital trade often overlook the other side of the data privacy equation. Focusing almost exclusively on the compliance costs that accrue to EU data protection rules, they ignore the costs of insufficient privacy and personal data protection for businesses and consumers, and the broader societal benefits of protecting privacy and personal data as fundamental rights. The OECD rightly notes that 'information on global data flows alone says little about the value of that data, i.e. it cannot describe the respect of fundamental rights'.[64]

Generalized conclusions about the wholesale benefits of free data flows, albeit tempting, are not possible because this would presuppose that an optimal level of privacy and data protection has already been realized. Owing to the multifaceted concept of privacy Acquisti, Taylor and Wagman conclude their extant review of the literature on privacy economics and empirical studies by asserting that both the sharing and the protecting of personal data can have positive and negative consequences at both the individual and societal levels.[65]

Data privacy protections are considered an important ingredient to build up consumer trust in electronic commerce and online transactions. Several surveys conducted in Europe show that protection of personal data and online behaviour is very important to Europeans, regardless of the location of the company or public authority that handles their data or offers the service.[66] According to the 2017 survey, the majority of individuals consider privacy and security when purchasing IT products. Although only slightly more than one-quarter of Europeans (27 per cent) were willing to pay for better privacy and security features, this share was much higher in Germany, Denmark, and Ireland (43, 44, and 37 per cent, respectively).[67] A 2019 survey shows that more than six in 10 individuals are concerned about not having complete control over their personal data online.[68] Consumers on the other side of the Atlantic have developed even stronger concerns about Data privacy and security online.[69] The lack of data privacy may lead to the misuse of personal data and result in costs for both businesses and individuals. Identity theft may not only cost users billions of dollars[70] but also cause a variety of non-economic costs, ranging from physical and emotional harm to negative effects on relationships and life opportunities.[71] As a result of exploitation of their personal data by companies, some consumers may end up paying higher prices, buying goods and services of inferior quality, and incur transaction costs of handling unsolicited communications.[72] Businesses may also suffer losses in online retail due to consumers' privacy concerns, negative publicity, administrative fines or sanctions, and massive class action claims.[73]

64 OECD (n 12) 51, endnote 10.

65 Alessandro Acquisti, Curtis Taylor and Liad Wagman, 'The Economics of Privacy' (2016) 54(2) Journal of Economic Literature 442, 483.

66 European Commission, Special Eurobarometer 431, 'Data Protection' (2015) <http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf> accessed 5 March 2020; European Commission, Flash Eurobarometer 443, 'e-Privacy' (2016) <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/82290> accessed 5 March 2020; European Commission, Special Eurobarometer 460, 'Attitudes Towards the Impact of Digitisation and Automation on Daily Life' (2017) <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/78997> accessed 5 March 2020.

67 Special Eurobarometer 460, ibid 110.

68 Special Eurobarometer 487a, 'Summary' (June 2019) 14 <https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/86881> accessed 5 March 2020.

69 See, eg Brooke Auxier, 'Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information' (*Pew Research Center*, 15 November 2019) <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/> accessed 5 March 2020.

70 According to a study by Javelin Strategy & Research, identity fraud affected 16.7 million US consumers causing losses of $16.8 billion (see Al Pascual, Kyle Marchini and Sarah Miller, '2018 Identity Fraud: Fraud Enters a New Era of Complexity' (2018) <https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity> accessed 5 March 2020.

71 Eva Velasquez and others, 'Identity Theft: The Aftermath 2017' (Identity Theft Resource Center for U.S. Federal Trade Commission), 2017 <https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf> accessed 5 March 2020; Nathan Newman, 'The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google' (2014) 40 William Mitchell Law Review 849.

72 Acquisti, Taylor and Wagman (n 65) 464, Chris J Hoofnagle and Kerry E Smith, 'Comments of the Electronic Privacy Information Center to the Federal Trade Commission Workshop on Information Flows' (2003) FTC File No P034102 <https://epic.org/privacy/profiling/infoflows.html> accessed 5 March 2020; Robert Gellman, 'How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs Are Biased and Incomplete' (*EPIC*, 2002) <http://www.epic.org/reports/dmfprivacy.html> accessed 5 March 2020.

73 Gellman (n 73); Sasha Romanoski and Alessandro Acquisti, 'Privacy Costs and Personal Data Protection: Economic and Legal Perspectives' (2009) 24(3) Berkeley Technology Law Journal, 1064–1101; France24, 'French Consumer Group Launches Class Action Against Google' (26 June 2019) <https://www.france24.com/en/20190626-french-consumer-group-launches-class-action-against-google-0> accessed 5 March 2020.

More importantly, the economic approach to personal data protection does not capture the broader societal value of privacy and personal data protection as fundamental rights, and ignores broader societal risks. 'Economic analysis', as Kerber rightly argues, 'usually focusses on welfare effects alone, which might not always grasp sufficiently the normative dimension of privacy as a fundamental right'.[74] Accumulating vast amounts of personal data from different sources and reselling these data for any purpose to almost any business on a global scale can deprive individuals of privacy and effective remedies.[75] Zuboff advocates that the unprecedented accumulation of personal data leads to 'surveillance capitalism' that 'threatens the existential and political canon of the modern liberal order defined by principles of self-determination'.[76] Ultimately, she notes, not just consumers' costs or individual rights to privacy are at stake, but:

> the sanctity of the individual and the ideals of social equality, the development of identity, autonomy, and moral reasoning; the integrity of contract, the freedom that accrues to the making and fulfilling of promises; norms and rules of collective agreement; the functions of market democracy; the political integrity of societies; and the future of democratic sovereignty.[77]

Viewed in this perspective, this protection contributes to the preservation of individual and societal values, such as democracy, civil society, fairness, and individual self-determination to name just a few.[78] Revelations of how profiling combined with political micro-targeting on social media may have affected the 2016 presidential election in the USA and the Facebook–Cambridge Analytica scandal are good examples of the risks that the erosion of privacy poses to Western electoral democracies.[79]

In light of the aforementioned, we offer an alternative, more cautious narrative in which global data flows should be construed to serve individuals' interests and societal values. The reasoning underpinning this alternate narrative is certainly not less compelling than extrapolating from total bandwidth to the value of free data flow to the need to liberalize cross-border data flows including individuals' personal data.

Free data flows and the digital trade agenda

Theoretically, international trade law is the result of reciprocal—and arguably, mutually advantageous—arrangements between sovereign parties. Trade law forms a subset of public international law, centred around the law of the WTO, and a vast network of bilateral trade agreements.[80] The recent discourse on the importance of data flows for digital trade is not an entirely new but rather a twist to the ongoing discussions about trade-related aspects of electronic commerce in the WTO multilateral trade law system.[81] Therefore, it cannot be viewed in isolation from the relevant WTO rules which can help to understand the evolution of the trade discourse from electronic commerce to digital trade.

This section traces how free data flows entered international trade diplomacy. After a historical glance at the regulation of data flows in 1994 GATS and the ensuing WTO work programme on electronic commerce, it will introduce a more elaborate discussion on cross-border data flows and counterbalancing provisions for the protection of personal data that took place in the decades after the adoption of the GATS. It is worth keeping in mind that the EU adopted the Data Protection Directive (DPD)[82]—the core of the data protection framework before the GDPR—just one year after the adoption of the GATS.

74 Wolfgang Kerber, 'Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection' (2016) 11(11) Journal of Intellectual Property Law & Practice 856, 857.

75 Chris J Hoofnagle, 'US Regulatory Values and Privacy Consequences: Implications for the European Citizen' (2016) 2(2) European Data Protection Law Review 169, 170–71.

76 Shoshana Zuboff, 'The Secrets of Surveillance Capitalism' *Frankfurter Algemeine Zeitung* (5 March 2016) <http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html> accessed 5 March 2020; Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology 75, 77.

77 Zuboff, 'The Secrets of Surveillance Capitalism' ibid.

78 Cécile de Terwangne, 'Is a Global Data Protection Regulatory Model Possible?' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer, Dordrecht 2009) 55; Julie E Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stanford Law Review 1373, 1423–28; Jonathan Cinnamon, 'Social Injustice in Surveillance Capitalism' (2017) 15(5) Surveillance & Society 609, 610–11; Paul M Schwartz, 'Privacy and Democracy in Cyberspace' (1999) 52 Vanderbilt Law Review 1609, 1647ff.

79 See, eg Alexis C Madrigal, 'What Facebook Did to American Democracy' *The Atlantic* (17 October 2017) <https://www.theatlantic.com/technology/archive/2017/10/what-facebook-did/542502/> accessed 5 March 2020.

80 Steve Charnovitz, 'The Field of International Economic Law' (2014) 17(3) Journal of International Economic Law 607.

81 See Jane Kelsey, 'How a TPP-style E-commerce Outcome in the WTO Would Endanger the Development Dimension of the GATS Acquis (and Potentially the WTO)' (2018) 21 Journal of International Economic Law 273; Svetlana Yakovleva, 'Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy' (2020) 74 University of Miami Law Review 416, 2020, <https://ssrn.com/abstract=3463076> accessed 5 March 2020.

82 Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L281 31–50.

From the WTO e-commerce work programme to the digital trade agenda

The primary goal of the GATS, as its preamble states, was the expansion of international trade in services through the elimination of trade barriers. Negotiated between 1986 and 1994, the text of the GATS does not explicitly refer to electronic commerce, cross-border data flows, or digital delivery of services. However, the GATS defines its scope and disciplines in a broad and flexible manner. The growth of electronic commerce in the late 1990s put pressure on the GATS disciplines to include the provision of electronically delivered services within the scope of the agreement. To address this problem, in 1998 the WTO launched a Global Work Programme on Electronic Commerce ('the Work Programme on E-commerce').[83]

The first 1999 progress report on the WTO Work Programme[84] clarified the WTO members' informal consensus that:

> the Agreement applies to all services regardless of the means by which they are delivered, and that electronic delivery can take place under any of the four modes of supply. Measures affecting the electronic delivery of services are measures affecting trade in services in the sense of Article I of the GATS and are therefore covered by GATS obligations. . . . It was also the general view that the GATS is technologically neutral in the sense that it does not contain any provisions that distinguish between the different technological means through which a service may be supplied.[85]

The Work Programme contributed to the interpretation of the WTO agreements in the WTO jurisprudence, which eventually confirmed the applicability of the GATS to services delivered electronically.[86] Put differently, the GATS provisions have been flexible enough to accommodate the proliferation of electronic commerce, at least as far as the electronic delivery of goods and services is concerned. Whether the GATS, and the WTO in general, apply to digital services and are resilient to meet the challenges of digital trade is a separate question.

Cross-border data flows under GATS and WTO trade diplomacy

The main body of GATS does not contain a horizontal provision on cross-border data flows. This issue first emerged in GATS-annexed sector-specific provisions. In particular, under the 1994 Understanding on Commitments in Financial Services (Understanding),[87] one of the market access obligations in the financial services sector is the requirement to abstain from taking measures preventing the transfer of data by electronic means.[88] Article 5(c) of the Annex on Telecommunications obliges the WTO members to allow the use of public telecommunications infrastructure and services for the movement of information within and across borders, and for access to information contained in databases or otherwise stored in machine-readable form in the territory of any party. Both commitments were subject to counterbalancing provisions on privacy and confidentiality, respectively, as will be explained below.

In the WTO, the discussion on cross-border information flows emerged in 2011, when the EU and the USA jointly submitted to the WTO Council for Trade in Services a set of Trade Principles for Information and Communication Technology Services (the so-called ICT Principles).[89] Two of the principles are relevant in the context of this article. The first prohibits governments from preventing cross-border electronic transfers of information. The second obliges the parties to refrain from imposing ICT localization requirements. Initially, the ICT Principles did not include a full-fledged counterbalancing provision on the protection of privacy and personal data.

Consumer privacy entered the discussion in 2012 at the initiative of the Australian delegation. It proposed

83 Geneva Ministerial Declaration on global electronic commerce, 20 May 1998, WT/MIN(98)/DEC/2.

84 It is worth mentioning that the Progress Report does not constitute an official clarification of the GATS, as the Council for Trade in Services is not authorized to give authoritative interpretations of WTO law. It only reflected the views on the issues mentioned in the Work Programme, and the discussion of these issues continued in the years to come.

85 WTO Council for Trade in Services WTO, Progress Report on the Work Programme on Electronic Commerce, 19 July 1999, S/L/74, para. 4.

86 Appellate Body Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/AB/R, adopted 20 April 2005, para 180ff; Panel Report, *United States – Measures Affecting the Cross-border Supply of Gambling and Betting Services*, WT/DS285/R, adopted 20 April 2005, para 6.285; Appellate Body Report, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, WT/DS363/AB/R, adopted 19 January 2010, para 377; Panel Report, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, WT/DS363/R and Corr.1, adopted 19 January 2010, paras 7.1220 and 7.1265. For analysis, see Mira Burri, 'The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation' (2017) 51(65) UC Davis Law Review, 94–97; Sacha Wunsch-Vincent, 'The Internet, Cross-border Trade in Services and the GATS: Lessons from US-Gambling' (2006) 5(3) World Trade Review 319–355.

87 The understanding is not a part of the GATS but an appendix to the Final Act of the Uruguay Round.

88 Art B.8 of the Understanding.

89 Communication from the European Union and the United States, Contribution to the Work Programme on Electronic Commerce, 13 July 2011, S/C/W/338.

to complement the ICT Principles with three additional principles in order to enhance 'consumer and business confidence in electronic commerce'.[90] 'Online Personal Data Protection' was one of them; it required members to 'adopt or maintain a domestic legal framework which ensures the protection of the personal data of the users of electronic commerce'.[91] The absence of a counterbalancing provision in the initial ICT Principles, arguably, exemplifies the EU's ultimate reliance on the robustness of the GATS Article XIV exception (discussed in section 'Parties right to regulate under the GATS' below) to preserve its autonomy to regulate privacy and personal data protection.

The ICT Principles, which were never adopted, marked an important turn in the discussions of cross-border information flows. For once these principles formulated the overarching and highly compelling premise of cross-border data flows as desirable trade law disciplines. Privacy and personal data protection were discussed not merely as an exception, but as a positive obligation counterbalancing the parties' possible commitments to cross-border information flows. Perhaps as a result of this, the WTO Committee of Ministers in its 2013 Bali Ministerial decision for the first time mentioned the protection of confidential data, privacy, and consumer protection as trade-related aspects.[92]

Besides the informal agreement not to impose customs duties on electronic transmissions, that has been continuously extended since its inception (the last time was in 2019[93]), the WTO Work Programme did not yield any conclusive results. Trying to get out of this gridlock, in 2017 a smaller group of 71 WTO members, including the EU, Australia, Japan, Mexico, New Zealand, and USA, initiated 'exploratory work . . . toward future WTO negotiations on trade-related aspects of electronic commerce'.[94] In a communication to the participants of the group, the USA outlined what it considers to represent the 'highest standard in safeguarding and promoting digital trade'.[95] The rules on cross-border transfer of data—'the life blood of international trade'—were at the top of the list. In 2019, 76 WTO members announced their intention to launch WTO negotiations on electronic commerce to create multilateral rules regulating digital trade.[96] Digital trade, we argue, is a broader notion than mere electronic commerce, and hence the digital trade agenda, as we explain below, is bound to have much wider repercussions on domestic privacy frameworks. There is no universal definition of electronic commerce or digital trade. The OECD, for example, has defined an electronic commerce transaction as 'the sale or purchase of goods or services, conducted over computer networks by methods specifically designed for the purpose of receiving or placing orders'.[97] Against this backdrop, digital trade constitutes a qualitative shift:

> [t]his new era of hyperconnectivity is not just about digitally delivered trade, it is also about more physical, traditional or [global value chains], trade enabled by growing digital connectivity increasing access to foreign markets for firms in a way that would previously have been unimaginable.[98]

Whereas in electronic commerce flows of personal data were understood as auxiliary to the provision of services, in digital trade personal data itself can be the subject of trade, as in the business of data brokers and the trading of big data troves. The overview above is an illustration of the mindset that evolved in relation to cross-border data flows and the protection of privacy and personal data in the WTO. The provisions on cross-border data flows, the position of the USA, and the ultimate reliance of the EU on the GATS Article XIV-type general exceptions have almost verbatim resurrected in the negotiations of new generation trade agreements addressed in section 'EU external policies: between normative values and economic relations' of this article. Prior to that, to make the overview complete, the following section illustrates why the autonomy to regulate granted to the parties under the GATS in the form of general exceptions likely does not suffice to accommodate today's EU measures on privacy and personal data protection.

Parties right to regulate under the GATS

The GATS recognizes the autonomy of parties to pursue their national policy objectives, referred to as the right to regulate.[99] In effect, it allows a party to adopt

90 Communication from Australia, Suggestions on ICT Principles, Contribution to the Work Programme on Electronic Commerce, 26 September 2012, S/C/W/349.

91 Ibid.

92 WTO Ministerial decision of 7 December 2013, WT/MIN(13)/32, WT/L/907.

93 WTO General Council Decision of 11 December 2019, WT/L/1079.

94 WTO Ministerial Conference, Joint Statement on Electronic Commerce, 13 December 2017, WT/MIN(17)/60.

95 Joint Statement on Electronic Commerce Initiative, Communication from the United States of 12 April 2018, JOB/GC/178.

96 European Commission, 76 WTO partners launch talks on e-commerce, 25 January 2019 <http://trade.ec.europa.eu/doclib/press/index.cfm?id=1974> accessed 5 March 2020.

97 Javier López González and Marie-Agnes Jouanjean, 'Digital Trade: Developing a Framework for Analysis' (2017) OECD Policy Papers No 205, 12, fn 13 <http://dx.doi.org/10.1787/524c8c83-en> accessed 5 March 2020.

98 Ibid 7.

99 Recital 3 of the Preamble to the GATS.

domestic measures which are either from the outset compliant with its commitments under the GATS, or, in the event of a violation of its GATS commitments, are justifiable under the general exceptions provided for in Article XIV.[100] The general exceptions apply horizontally to all sectors liberalized under the GATS.

The protection of the privacy of individuals in relation to the processing and dissemination of personal data is one of the policy objectives that is explicitly mentioned in paragraph (c)(ii) of Article XIV. Under this provision, the WTO members may adopt and enforce a GATS-inconsistent measure if it is:

> necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to . . . the protection of the privacy of individuals in relation to the processing and dissemination of personal data . . ..

The core element of the Article XIV(c)(ii) exception is the so-called 'necessity' test that requires 'weighing and balancing' between several factors.[101] First, it should be established whether a measure contributes to the enforcement of domestic laws and regulations that pursue a public policy objective,[102] which in itself is 'not inconsistent' with the provisions of the GATS. Secondly, the restrictive effect of the measure on international trade in services should be assessed. The less restrictive the measure, and the greater the contribution to the enforcement of public interest, the more likely it is that the measure in question will meet the necessity test. If the party whose measure is being challenged demonstrates the *prima facie* 'necessity' of its measure, the claimant can rebut the 'necessity' by demonstrating that a less trade-restrictive alternative to the measure has been 'reasonably available', meaning that it allows the defending party to achieve the pursued public policy objective without prohibitive costs or substantial technical difficulties to that party.[103]

A measure that has been provisionally justified under the material requirements of Article XIV(c)(ii) is further tested against the so-called *chapeau* of Article XIV, which requires that a measure should have been applied in a manner that does not constitute:

> . . . a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services.

Interpreted by the WTO adjudicating bodies as an open norm,[104] the *chapeau* aims to prevent abuses or misuses of the right to invoke the exception.[105] On its face, this does not seem to be an unreasonable requirement. However, the way it is applied in WTO jurisprudence requires almost absolute 'consistency of enforcement', which is in practice arguably prone to some failure.[106] As a result, any inconsistency creates the risk of precluding the justification of a GATS-inconsistent measure.

To date no case law has clarified the application of Article XIV(c)(ii) to privacy and personal data protection measures. Scholars and pundits note a high level of uncertainty and unpredictability in relation to the application and interpretation of the general exceptions.[107] The main point of concern is that such application may not be favourable for the protection of privacy and personal data as fundamental rights, given the low overall success rate in the reliance on GATS Article XIV in general.[108] In an earlier article, the authors subjected EU rules on cross-border transfers of personal data to a hypothetical challenge under the GATS and applied WTO adjudicating bodies' jurisprudence.[109] Concurring with other authors, we concluded that if these EU measures qualify as a GATS violation, they may not be capable of meeting all the prongs of this exception.[110]

Indeed, when it comes to regional privacy and data protection standards, there are several of them, in particular, the 2013 OECD Guidelines and the 2015 APEC Privacy Framework,[111] that hold a purely economic

100 Appellate Body Report, *Argentina – Measures Relating to Trade in Goods and Services*, WT/DS453/AB/R and Add.1, adopted 9 May 2016, para 6.114.

101 Appellate Body Report, *US – Gambling* (n 86) para 306; Panel Report, *Argentina – Measures Relating to Trade in Goods and Services*, WT/DS453/R and Add.1, adopted 9 May 2016, para 7.684.

102 This is not to be confused with the contribution of the measure to the protected interest itself.

103 Panel Report, *Argentina – Financial Services* (n 101) para 7.729; Appellate Body Report, *US – Gambling* (n 86) para 308.

104 The unwillingness of the WTO adjudicating bodies to develop general rules on the basis of the *chapeau* was criticized, as this creates uncertainty in the future interpretation of the exceptions. See Reyes (n 7) 27.

105 Panel Report, *Argentina– Financial Services* (n 101) para 7.743, Appellate Body Report, *United States – Standards for Reformulated and Conventional Gasoline*, WT/DS2/AB/R, adopted 20 May 1996, 22.

106 Appellate Body Report, *US – Gambling* (n 86) para 351.

107 Reyes (n 7) 25, 34; Weber (n 5) 40.

108 Citizen.org, 'Only One of 40 Attempts to Use the GATT Article XX/GATS Article XIV "General Exception" Has Ever Succeeded: Replicating the WTO Exception Construct Will Not Provide for an Effective TPP General Exception' (2015) <www.citizen.org/documents/general-exception.pdf> accessed 5 March 2020.

109 Svetlana Yakovleva and Kristina Irion, 'The Best of Both Worlds - Free Trade in Services and EU Law on Privacy and Data Protection' (2016) 2 European Data Protection Law Review 191.

110 Yakovleva and Irion, ibid 206; Reyes (n 7) 25, 34; Shapiro (n 7) 2812; Diane Macdonald and Christine Streatfeild, 'Personal Data Privacy and the WTO' (2004) 36(3) Houston Journal of International Law 625, 646ff; Shin-yi Peng, 'Digitalization of Services, the GATS and the Protection of Personal Data' in Rolf Sethe and others (eds), *Kommunikation: Festschrift für Rolf H. Weber zum 60. Geburtstag* (Stämpfli Verlag, Bern 2011) 753.

111 OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013); APEC Privacy Framework (2015).

stance on the issue. The existence of these arguably less trade-restrictive approaches puts the EU fundamental rights-based privacy and data protection framework at risk of not passing the necessity test; the fundamental rights approach requires a higher level of protection of privacy and personal data, transcending the economic interests of cross-border data flows and liberalization of international trade.[112] As a result, the regulatory architecture and methods used by EU law to ensure a high level of privacy and data protection (in particular, the country-by-country adequacy approach) may not be considered as the least trade-restrictive by WTO adjudicators.

International trade law knows other techniques besides the general exceptions that are used to counterbalance a commitment. Such have entered the sector-specific cross-border information flow commitments in financial services and telecommunications. Provisions related to cross-border data flows—paragraph B8 of the Understanding and Article 5(d) of the Annex on Telecommunications—contain counterbalancing provision mentioning privacy and/or the protection of personal data. These provisions are, arguably, rooted in the principles of financial secrecy and confidentiality of telecommunications that are widely recognized across jurisdictions. Paragraph B8 of the Understanding provides that:

> [n]othing in this paragraph restricts the right of a Member to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is *not used to circumvent the provisions of the Agreement*. (emphasis added)

According to Article 5(d) of the Annex on Telecommunications:

> [n]otwithstanding the preceding paragraph, a Member may take such measures as are *necessary* to ensure the security and confidentiality of messages, *subject to* the requirement that such measures are *not applied* in a manner which would constitute a means of *arbitrary or unjustifiable discrimination or a disguised restriction on trade* in services. (emphasis added)

While the counterbalancing provision in the financial sector gives comparatively more leeway to protect privacy and personal data as fundamental rights, than does the telecommunications sector, both provisions carry requirements similar to those contained in the general exceptions.

To sum up, although the GATS recognizes some autonomy to adopt regulation protecting privacy and personal data even if inconsistent with its disciplines, this autonomy is quite narrow given that it is subject to a number of trade-conforming conditions. From the outset, it should be noted that while trying to expand the scope of the GATS to include electronic commerce, a number of participants of the WTO Work Programme simultaneously tried to limit the regulatory autonomy of the parties to the GATS in this area; in particular, as the 1999 Progress Report illustrates, the framers cautioned that the general exception 'should be interpreted narrowly'.[113] In the view of UNCTAD, it is plausible that in the future data privacy law will also be influenced by international trade disputes.[114]

Besides, the tendency to convert privacy and data protection from a matter of conditional regulatory autonomy into the subject matter of international trade agreements (regulating, among other things, digital trade) is similar to the case of intellectual property. Initially, in GATT 1947 intellectual property rights were mentioned in a general exception of Article XX. In 1994, they became the subject matter of a separate WTO trade agreement—the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).[115] Even if provisions on data flows are inevitable, a more important question is thus how they will be framed and what carve-outs or exceptions for privacy and data protection will counterbalance the negative effects of such provisions on human rights.

Free data flows in GATS-plus Free Trade Agreements

Thanks to its powerful enforcement mechanism and institutional structure, international trade law has an enormous potential to influence national laws.[116] A new generation of trade and investment agreements which have been concluded or are presently being negotiated endeavours to secure service liberalization beyond what has been achieved under the GATS (the so-called 'GATS-plus' criteria). GATS-plus trade relations aim to deepen commitments in existing service chapters, as well as to introduce additional service chapters covering

112 Yakovleva (n 19) 483ff.

113 WTO Council for Trade in Services WTO, Progress Report on the Work Programme on Electronic Commerce (n 85) para 14.

114 UNCTAD (n 11) 37.

115 For a discussion, see Laurence R Helfer, 'Regime Shifting. The TRIPS Agreement and New Dynamics of International Intellectual Property Lawmaking' (2004) 29 Yale Journal of International Law 1.

116 With direct effects, such as a party lifting tariffs, and more subtle and indirect effects, see, eg Emily Lydgate, 'Is It Rational and Consistent? The WTO's Surprising Role in Shaping Domestic Public Policy' (2017) 20(3) Journal of International Economic Law 561.

the so-called 'new and enhanced disciplines'. Such new generation trade agreements endorse digital trade broadly by proposing provisions on cross-border data flows while keeping privacy and data protection relegated to an exception modelled after GATS Article XIV.[117]

The USA and Korea were the first states to include a (non-binding) provision on cross-border free flow of information in their bilateral trade agreement.[118] This approach has culminated in a horizontal provision on data flows in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) signed in March 2018, which incorporates by reference the original Trans-Pacific Partnership (TPP) signed in 2016 and later abandoned by the new US administration. The CPTPP includes Article 14.11, paragraph 2 requiring that:

> [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.[119]

Unlike the above-mentioned WTO provisions related to cross-border data flows in financial and telecommunications services, this CPTPP clause is formulated as a positive obligation and is not sector-specific. The purposes of cross-border transfers are formulated broadly, which means that any slight connection of transfers to the conducting of business may be enough to trigger this provision. Furthermore, the provision seems to intentionally exclude the 'necessity' of the transfers for the purposes of conducting business. It is worth recalling, that necessity of data processing is an important factor in assessing the legitimacy of data processing under many domestic data protection regimes. As a result, even limitations on transfers of personal data in cases where such transfers are merely incidental for the companies' business might lead to a violation of Article 14.11, paragraph 2.

Remarkably, although Article 29.1 CPTPP incorporates general exceptions familiar from the GATS Article XIV, Article 14.11(3) provides for a specific exception:

> Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 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 required to achieve the objective.

The structure of this specific exception strongly resembles that of GATS Article XIV(c), with two important differences. First, the Article 14.11(3) exception does not name the legitimate public policy objectives that could justify limitations on transfers, and is, in this sense, broader than the general exception for privacy and data protection. Secondly, the so-called 'necessity test' discussed above is replaced by the condition that limitations on cross-border transfers should not 'impose restrictions ... greater than are required to achieve the objective'. While the purpose of incorporating a specific exception for data transfers, in addition to a general exception, is unclear, the authors believe that this could have been done to avoid the application of WTO jurisprudence from GATS Article XIV to this particular context and to broaden the range of public policy objectives that could justify a restriction on data flows.

Furthermore, one of the Trump administration's objectives for the renegotiation of the North American Free Trade Agreement (NAFTA) has been to ensure that NAFTA countries do not impose restrictions on cross-border data flows.[120] The meanwhile concluded United States–Mexico–Canada Agreement (USMCA) comprises a chapter on Digital Trade requiring 'that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented'.[121] USMCA moreover endorses the APEC Cross-Border Privacy Rules as 'a valid mechanism to facilitate cross-border information transfers while protecting personal information',[122] thereby defining what is deemed necessary and proportionate under the agreement. The USMCA digital trade provisions have become the model for future US-led trade agreements: they have already been, almost verbatim, included in the US–Japan Digital Trade Agreement[123] and are included in the US proposal for the recently relaunched electronic commerce negotiations at the WTO.[124]

The issue of cross-border data flows has been persistent in bilateral and multilateral trade agreements the

117 Burri (n 86) 99ff.

118 Aaronson (n 11) 8.

119 Comprehensive and Progressive Agreement for Trans-Pacific Partnership between Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam, March 2018.

120 Office of the United States Trade Representative, Summary of Objectives for the NAFTA Renegotiation, 17 July 2017, 8–9.

121 USMCA, signed 30 November 2018, art 19.8(3) <https://ustr.gov/usmca> accessed 5 March 2020.

122 Ibid, art 19.8(6).

123 US–Japan Digital Trade Agreement, signed on 7 October 2019 <https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf> accessed 5 March 2020.

124 Inu Manak, 'U.S. WTO E-commerce Proposal Reads Like USMCA' (*International Economic Law and Policy Blog*, 8 May 2019) <https://worldtradelaw.typepad.com/ielpblog/2019/05/us-wto-e-commerce-proposal-reads-like-usmca.html> accessed 5 March 2020.

EU has negotiated or is currently negotiating, such as the TTIP, TiSA, the 2016 Comprehensive Economic and Trade Agreement (CETA),[125] the Japan–EU EPA, and the envisaged trade deals with Australia, Chile, Indonesia, Mexico, New Zealand, and Tunisia. Although the fate of TTIP and TiSA is unclear, their negotiating history exemplifies how data privacy protection has been contentious in the negotiations of trade agreements with the EU.[126] In 2015, removal of discriminatory and protectionist barriers to cross-border data flows was one of the US Trade Representative's 12 priorities at the time of the negotiations of TTIP and TiSA.[127] It was suggested that in relation to the EU, TTIP is 'one of the best opportunities to institute cutting-edge data transfer protections ... by including three key features: (1) a commitment to allowing cross-border transfers; (2) a prohibition on data localization requirements; and (3) a non-exhaustive list of data transfer mechanisms'.[128] If such provisions were included in TTIP, it was hoped, they might serve 'as a template and baseline for the TiSA negotiations'.[129] Since negotiations stalled at the end of 2016, however, no visible progress has been reached on international data flows or data protection in either TTIP or TiSA.

In this respect, CETA is still comparatively innocuous, provided that Canada is one of the countries being recognized by the EU as affording an adequate level of personal data protection.[130] Only Chapter 13 of CETA on Financial Services incorporates in Article 13.15 a commitment on the transfer and processing of information that permits:

> ... a financial institution or a cross-border financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing if processing is required in the ordinary course of business of the financial institution or the cross-border financial service supplier.

The second paragraph of Article 13.15 calls for 'adequate safeguards to protect privacy'. The subsequent carve-out for the protection of personal information reads:

> If the transfer of financial information involves personal information, such transfers should be in accordance with the legislation governing the protection of personal information of the territory of the Party where the transfer has originated.

In other words, the EU can maintain its rules on the transfer of personal data to a third country in relation to financial services, and there is no dependency on a European Commission (Commission) decision conferring to Canada an adequate level of protection in the meaning of Article 45 GDPR. This provision exempts EU data protection law from the scope of Chapter 13 of CETA on Financial Services, without any conditions that it must be consistent with other commitments in that chapter. As a prudential measure, it would have been unnecessary were the general exceptions in CETA, which are modelled after GATS Article XIV, fully sufficient to achieve the same outcome.

Although the present US administration's actions do more harm than good to the rule-based multilateral trading system, cross-border data flow issues will continue to feature high on the digital trade agenda across the globe. Ultimately, the extent to which parties commit to free data flows in trade deals will determine the relative strength of privacy vis-à-vis trade and whether data privacy is to be protected by sovereign countries and the EU or is pulled into a supranational legal order on trade.

EU external policies: between normative values and economic relations

The EU has been characterized as a normative power that conducts its international relations through a professed rule-of-law based multilateralism.[131] The founding Treaties, as amended by the Lisbon Treaty, explicitly state the values, principles, and objectives that the EU shall pursue in its international relations: the universality and indivisibility of human rights and fundamental freedoms and contribution to their protection, respect for human dignity and for the principles of the United Nations and international law (Articles 3(5) and 21 TEU). The Charter of Fundamental Rights of the EU (Charter), in its Articles 7 and 8, guarantees both the right to privacy

125 Comprehensive Economic and Trade Agreement (CETA) between Canada, of the one part, and the European Union and its Member States, of the other part, 14 September 2014 (2017) OJ L11/23.

126 Elina Viilup, 'The Trade in Services Agreement (TISA): An End to Negotiations in Sight?' (*Study for the European Parliament*, 2015) 22ff <http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/570448/EXPO_IDA%282015%29570448_EN.pdf> accessed 5 March 2020.

127 'Remarks by Deputy US Trade Representative Robert Holleyman to the New Democrat Network' (Washington, DC, 1 May 2015) <https://ustr.gov/about-us/policy-offices/press-office/speechestranscripts/2015/may/remarks-deputy-us-trade> accessed 5 March 2020.

128 US Chamber of Commerce and Hunton&Williams LLP (n 10) 30.

129 Ibid.

130 Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (2001) OJ L2/13.

131 Bart Van Vooren, Steven Blockmans and Jan Wouters, 'The Legal Dimension of Global Governance: What Role for the European Union? An Introduction' in Bart Van Vooren, Steven Blockmans and Jan Wouters (eds), *The EU's Role in Global Governance The Legal Dimension* (OUP, Oxford 2013) 1–4, 2.

and the right to the protection of personal data as fundamental rights.

Extrapolating from this, the EU has a key role to play in the global governance of privacy and in particular regarding the protection of personal data. This role accrues to the EU by virtue of its external relations with third countries stretching over two policy areas for which it has exclusive competences: international transfers of personal data and external commercial policy. The EU has a preference for institutionalized relationships with third countries, emulating strategies that 'developed internally as part of its original project of European transnational integration'.[132] This may explain why the EU strives for regulatory convergence, mutual recognition, and ongoing dialogue in both policy areas,[133] which are closing in on each other in an increasingly connected and data-driven society. The EU's 2014-2019 Digital Single Market strategy, which has also been the umbrella for unifying data protection law in the GDPR, and the recently announced European Digital Strategy illustrate the point.[134]

Stating that EU external policies should be fully aligned with its normative approach to privacy and the protection of personal data would seem like preaching to the converted. But EU governance in this area has been erratic to a stunning degree, even to the detriment of individuals' fundamental rights. This troubling state of affairs can be attributed to EU internal divisions of competences and goal conflicts between normative levels of protection and external trade objectives. Below we revisit EU external policies in the field of data protection and external trade and discuss the EU's horizontal strategy which aligns its normative approach to privacy and the protection of personal data with future international trade law commitments the EU will enter into.

Administrating international transfers of personal data

In the last two decades, EU policy focused on ensuring that a sufficient privacy and data protection framework was established in order to guarantee a robust information society.[135] The GDPR preserved the regulatory approach, first adopted in the DPD, tying-in the high level of protection of personal data with the free movement thereof in the internal single market. The very legal basis for passing legislation relating to the protection of individuals with regard to the processing of personal data is connected to the rules relating to the free movement of such data.[136]

At the heart of the EU fundamental rights approach and the cross-border transfers controversy is the set of rules on transfer of personal data from the EU to third countries. This mechanism differentiates between third countries that ensure an adequate level of protection and third countries without an adequate level of protection.[137] To be recognized as a country ensuring an adequate level of protection, the country in question must undergo an assessment of its privacy and data protection rules and receive a positive assessment from the Commission (the so-called adequacy decision). As clarified by CJEU, this approach aims to prevent circumvention of the high level of personal data protection in the EU by transferring personal data to a third country.[138]

Surprisingly, the success with which third countries embraced the EU data protection principles in their own legislation did not result in many adequacy decisions in relation to foreign data protection systems. In relation to third countries, however, findings of adequacy are not automatic, and the intricate procedure to apply for recognition has been identified as a bottleneck that may effectively discriminate amongst third countries. As of December 2019, the Commission granted adequacy status to only 13 countries. Besides a few islands and small territories with strong ties to EU Member States,[139] Argentina, Canada, Israel, Japan, Switzerland, Uruguay, and the USA pursuant to the 2016 'EU-US Privacy Shield' are recognized. After 'Brexit', the UK will no longer be able to freely exchange personal data with other EU members,[140] while an adequacy procedure with South Korea[141] is in progress.

132 Gráinne De Búrca, 'EU External Relations: The Governance Mode of Foreign Policy' in Vooren, Blockmans and Wouters, ibid 39–57, 40.

133 Billy A Melo Araujo, *The EU Deep Trade Agenda* (OUP, Oxford 2016) 88.

134 Communication from the European Commission, A Digital Single Market Strategy for Europe, COM(2015) 192 final, 6 May 2015, para. 4.1, Communication from the European Commission, A European Strategy for Data, COM(2020) 66 final, 19 FEbruary 2020, p. 4. For an overview of the European Digital Strategy, see European Commission, Shaping Europe's Digital Future: European Digital Strategy <https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy> accessed 5 March 2020.

135 Abraham L Newman, *Protectors of Privacy: Regulating Personal Data in the Global Economy* (Cornell University Press, Ithaca 2008) 12ff.

136 Art 16(2) of the Treaty on the Functioning of EU.

137 Ch V GDPR.

138 CJEU, Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* (2015) ECLI:EU:C:2015:650, para 73.

139 Andorra, the Faeroe Islands, Guernsey, the Isle of Man, Jersey.

140 European Commission, 'Notice to Stakeholders. Withdrawal of the United Kingdom from the Union and EU Rules in the Field of Data Protection' (Brussels, 9 January 2018) <http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245> accessed 5 March 2020.

141 European Commission, 'Adequacy of the Protection of Personal Data in Non-EU Countries' <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en> accessed 5 March 2020.

Without an adequacy finding, transfers of personal data to other countries are only possible subject to 'appropriate safeguards', such as standard contractual clauses, binding corporate rules, and certification mechanisms, or one of the derogations, including where this is necessary for the performance of a contract, the use of adequate contractual safeguards, or reliance on the consent of data subjects and other special cases.[142] In other words, wholesale transfers of personal data to third countries not ensuring adequate levels of protection are sufficiently restricted while consent and contractual safeguards can substitute up to a certain extent for bilateral incongruences.

While these mechanisms have been criticized for being overly formalistic,[143] the justices at the CJEU seem determined to restrict the international transfer of personal data when necessary to protect the fundamental rights of individuals. In 2015, the CJEU in its landmark *Schrems* ruling struck down a significant legal basis for transferring personal data from the EU to the USA.[144] In two other decisions, the Court ruled that private-sector datasets carrying sensitive citizens' personal data must be retained inside EU territory in order to ensure independent supervision.[145]

Transatlantic transfers of personal data and blanket surveillance

Notably, transatlantic relations have proved to be a test for *de jure* compliance with EU rules on transfer of personal data. Here, the 2013 Snowden revelations on mass surveillance by the US government unsettled both transatlantic relations and trust in the digital economy. When in 2013 the 'Safe Harbour' was revealed to be a farce,[146] it was only the Court of Justice in its 2015 *Schrems* ruling[147] that invalidated the 'Safe Harbour' decision providing for the personal data of EU residents to be transferred to the USA. Whereas the justices did not examine the content of the safe harbour principles, they could still invalidate the Commission's adequacy decision because it did not satisfy the requirements for concluding that a third country ensures an adequate level of protection. The Court found that the Commission's obligation when rendering an adequacy decision is to:

> find, duly stating reasons, that a third country concerned in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order. . ..[148]

The Court argued that a third country's domestic law must limit interferences with the rights to privacy and the protection of personal data to what is strictly necessary, and that the right to effective judicial protection must be observed. Since the CJEU's reasoning is directly based on Articles 7 and 8 of the Charter, the ruling implicates more than the particular adequacy decision because it formulates a horizontal expectation for international transfers of personal data originating from EU individuals.

The *Schrems* ruling laid bare how far the EU executive—through the legal fiction of adequacy—had allowed the actual situation (*de facto*) to depart from the law (*de jure*). This troubling state of affairs can be attributed to internal struggles between EU institutions to adopt an approach capable of protecting fundamental rights when this has a bearing on the Union's first ally and trade partner.

The confrontation that arises at the triangular interface between privacy, trade, and surveillance has become emblematic for EU's external relations with the USA. In order to replace the invalidated 'Safe Harbor', the 'Privacy Shield', was hastily negotiated between the US government and the Commission and enacted in 2016.[149] Although the 'Privacy Shield' has passed the

142 Arts 46–49 GDPR.

143 Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) 18 German Law Journal 881, 917.

144 *Schrems* (n 138). For analysis, see Loic Azoulai and Marijn van der Sluis, 'Institutionalizing Personal Data Protection in Times of Global Institutional Distrust: Schrems' (2016) 53 Common Market Law Review 1343.

145 CJEU, Joined Cases C-203/15 and C-698/15 *Tele2 Sverige v Tom Watson* (2016) ECLI:EU:C:2016:970; Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources* (2014) ECLI:EU:C:2014:238; Marie-Pierre Granger and Kristina Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection' (2014) 39 European Law Review 834.

146 Alexander Dix, *Datenschutz Und Transatlantische Freihandelszone* (KIT Scientific Publishing, Karlsruher 2013); European Parliament Resolution of 12 March 2014 on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs (2013/2188) (2014) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//EN> accessed 5 March 2020.

147 *Schrems* (n 138).

148 Ibid, para 96.

149 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 the Protection Provided by the EU-U.S. Privacy Shield, however, disregarding the European Parliament Resolution of 26 May 2016 on transatlantic data flows (2016/2727(RSP)) <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2016-0233&language=EN&ring=P8-RC-2016-0623> accessed 5 March 2020; The Opinion of the European Data Protection Supervisor 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision (30 May 2016) <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-05-30_Privacy_Shield_EN.pdf> accessed 5 March 2020; and Article 29 Data Protection Working Party Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy

three annual reviews (last time in October 2019),[150] it is the subject of proceedings at the General Court and the CJEU.[151] Being the guardian of the EU Treaties, only the CJEU can reverse slack policy formulation by the EU executive where this puts individuals' fundamental rights at stake.

EU's external trade policy on data flows revisited

In the realm of EU external trade policy, the Commission's 2015 trade and investment strategy recognizes free cross-border data flows as an offensive interest for the EU.[152] The Commission promised that it will seek to use free trade agreements:

> to set rules for e-commerce and cross-border data flows and tackle new forms of digital protectionism, in full compliance with and without prejudice to the EU's data protection and data privacy rules.[153]

Obviously, the EU would not refer to its own data protection framework as 'digital protectionism', but it mainly aims to tackle 'unjustified data localisation and data storage requirements'.[154] The Commission did not anticipate any conflict when it resolved that '[r]ules on the processing of personal data are not negotiated in *or affected by trade agreements*' (emphasis added).[155]

The Commission negotiates international trade agreements on behalf of the EU in accordance with the negotiation directives (mandates) from the Council. Pursuant to Article 207(3) TFEU, both the Council and the Commission are 'responsible for ensuring that the agreements negotiated are compatible with internal Union policies and rules'. In respect to negotiations of both TTIP, TiSA, and the EPA with Japan, the Council's negotiating mandates do not mention privacy or data protection.[156] The negotiating mandates on TTIP and the EPA do require that the agreement not preclude the enforcement of exceptions on the supply of services justifiable under the relevant WTO rules (GATS Articles XIV and XIV*bis*). However, unlike such public interests as protection of environment, labour, consumers, and culture, privacy and data protection are not explicitly listed in the negotiation mandates as public interests to be secured in the course of negotiations.

Evolving trade deals, however, are affecting the EU's ability to afford a high level of protection for individual's personal data and may clash with the multiple external effects of the strengthened EU legislation. In principle, the GDPR applies directly to cross-border commercial transactions involving personal data from the EU.[157] The Court of Justice in the *Google Spain* case has already ruled that local law applies to the search engine's website, which now has to comply with the European *right to be forgotten*.[158] Such external effects are expected to have a profound impact on suppliers of goods and services from outside the EU, who will be required to observe the GDPR in its entirety—complying with EU-style data breach notifications, the right to be forgotten, data portability, and the principle of privacy by design, to name but a few.

Moreover, at the triangular interface between privacy, trade, and surveillance, it is unclear whether a party has the right to sever the flow of personal data in the commercial sector. This is precisely what the Court of Justice would do if it deemed privacy and data protection safeguards in a third country incompatible with the Charter. Inside international trade law, however, also a court judgment is considered a party's measure which could be challenged if it affects cross-border (digital) trade.

Towards an EU horizontal strategy on data flows

How the EU governs cross-border flows of personal data in external trade policy, it turns out, is much more

decision of 13 April 2016 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf> accessed 5 March 2020.

150 'Report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU–U.S. Privacy Shield' COM (2019) 495 final, 23 October 2019 <https://ec.europa.eu/info/sites/info/files/report_on_the_third_annual_review_of_the_eu_us_privacy_shield_2019.pdf> accessed 5 March 2020.

151 General Court, Case T-670/16 *Digital Rights Ireland v Commission* (dismissed) and Case T-738/16 *La Quadrature du Net and Others v Commission* (pending), CJEU, Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, unofficially referred to as *Schrems III*) (pending).

152 European Commission, 'Trade for All: Towards a More Responsible Trade and Investment Policy' COM (2015) 497 final, 14 October 2015.

153 Ibid.

154 Ibid 7.

155 Ibid.

156 The Council of the European Union, Directives for the Negotiation on the Transatlantic Trade and Investment Partnership Between the European Union and the United States of America 11103/13 (17 June 2013) <http://data.consilium.europa.eu/doc/document/ST-11103-2013-DCL-1/en/pdf> accessed 5 March 2020; Council of the European Union, Draft Directives for the Negotiation of a Plurilateral Agreement on Trade in Services (10 March 2015) para 7 <http://data.consilium.europa.eu/doc/document/ST-6891-2013-ADD-1-DCL-1/en/pdf> accessed 5 March 2020; The Council of the European Union, Directives for the Negotiation of a Free Trade Agreement with Japan 15864/12 (29 November 2012) <http://trade.ec.europa.eu/doclib/docs/2017/september/tradoc_156051.en12.pdf> accessed 5 March 2020.

157 Paul de Hert and Michal Czerniawski, 'Expanding the European Data Protection Scope Beyond Territory: Article 3 of the General Data Protection Regulation in Its Wider Context' (2016) 6 International Data Privacy Law 230; Yakovleva and Irion (n 109) 194–95; Cedric Ryngaert, 'Symposium Issue on Extraterritoriality and EU Data Protection' (2015) 5(4) International Data Privacy Law 221.

158 Indra Spiecker gen Döhmann, 'A New Framework for Information Markets: Google Spain' (2015) 52(4) Common Market Law Review 1033.

intricate than perhaps anticipated. The EU had to redefine its strategy to ensure that its trade deals are not undermining its new GDPR specifically designed to protect fundamental rights.

In its 2017 Communication on Exchanging and Protecting Personal Data in a Globalised World, the Commission defined its approach from the perspective of its data protection policy.[159] The Communication was passed after a study was published (to which the authors of this article contributed) which unpacked the potentially conflictual relationship between EU data privacy law and free data flow commitments in GATS-plus free trade agreements.[160] This Communication sets out in detail the mechanisms for international transfers of personal data, emphasizing the new opportunities introduced by the GDPR, such as approved codes of conduct and certification mechanism.

In relation to the adequacy mechanism, the Communication moreover clarifies the criteria which the Commission will take into account when selecting third countries for conducting a dialogue on adequacy:

(i) the extent of the EU's (actual or potential) commercial relations with a given third country, including the existence of a free trade agreement or ongoing negotiations;

(ii) the extent of personal data flows from the EU, reflecting geographical and/or cultural ties;

(iii) the pioneering role that the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region; and

(iv) the overall political relationship with the third country in question, in particular with respect to the promotion of common values and shared objectives at international level.[161]

Based on these considerations, the Communication indicates more agility to engage with key trading partners in East and South-East Asia. It moreover mentions India, depending on its progress in modernizing its data protection laws, countries in Latin America, and in the European neighbourhood. A more proactive approach of the EU in opening adequacy procedures would certainly be necessary in order to offer third countries a fair entry point to the procedure and breathe new life into the adequacy mechanisms championed by the EU.

The interface with external trade policy is also briefly touched upon, falling short, however, of defining a horizontal strategy:

> The EU data protection rules cannot be the subject of negotiations in a free trade agreement. While dialogues on data protection and trade negotiations with third countries have to follow separate tracks, an adequacy decision, including a partial or sector-specific one, is the best avenue to build mutual trust, guaranteeing uninhibited flow of personal data, and thus facilitate commercial exchanges involving transfers of personal data to the third country in question.[162]

Interestingly, it was the European Parliament which underscored the need for better scoped exceptions in free trade agreements. In its 2015 resolution on TTIP and 2016 resolution on TiSA, the European Parliament recommended that the Commission ensure the EU *acquis* on data privacy is not compromised through the liberalization of data flows, in particular in the areas of e-commerce and financial services. [163] The resolution on TiSA states that data protection and the right to privacy are not trade barriers, but fundamental rights.[164] A key point in both resolutions is the demand for a more robust version of GATS Article XIV-type exceptions for privacy and data protection. The European Parliament specifically called for:

> [A] comprehensive, unambiguous, horizontal, self-standing and legally binding provision based on GATS Article XIV which fully exempts the existing and future EU legal framework for the protection of personal data from the scope of this agreement, without any conditions that it must be consistent with other parts of the TiSA; to apply such provisions to all other TiSA annexes; . . ..[165]

159 European Commission, 'Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World' COM (2017) 7 final, s I.3.

160 Kristina Irion, Svetlana Yakovleva and Marija Bartl, 'Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements', independent study commissioned by BEUC et al., 13 July 2016, Amsterdam, Institute for Information Law (IViR) <https://ssrn.com/abstract=2877166> accessed 5 March 2020.

161 European Commission (n 159) para 3.1. Whether these criteria would satisfy Most-Favoured Nation treatment and domestic regulation disciplines in international trade law is already questionable.

162 Ibid.

163 European Parliament, Resolution of 3 February 2016 containing the European Parliament's recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA) (2015/2233(INI), Recital M, paras 1(a)(ii) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0041+0+DOC+XML+V0//EN> accessed 5 March 2020; European Parliament, Resolution of 8 July 2015 containing the European Parliament's recommendations to the European Commission on the negotiations for the Transatlantic Trade and Investment Partnership (TTIP) (2014/2228(INI)) para 2(b)(xii) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0252+0+DOC+XML+V0//EN> accessed 5 March 2020.

164 European Parliament, Resolution of 3 February 2016 (n 163) para 1(c).iii.

165 Ibid.

When it emerged that the Commission did not intend to touch the accepted trade law formula of the general exceptions, members of the European Parliament urged the Commission to put forward its position on cross-border data flows in trade negotiations:

> [N]othing in these trade agreements should prevent the EU from maintaining, improving and applying its data protection rules. Our rules on international transfers of personal data, are crystal clear, well-grounded and must not in any way be diluted.
>
> In other words, data protection should not be subject to trade negotiations. It is a fundamental right, not a trade barrier, and as such, it should be fully excluded from these agreements. Accordingly, any commitments on market access and to international standards on cross-border data flows must be very carefully conditioned. We also believe that the WTO exemption for data protection, known as GATS XIV, should be strengthened.[166]

Meanwhile, the European Parliament adopted a targeted resolution 'Towards a digital trade strategy' which argues for internal consistency of external trade policy with EU data protection regulation and calls on the Commission to come up with a position that takes on board its requirements.[167]

An intense institutional dialogue ensued officially under the lead of First Vice-President Timmermans and involving key members of the European Parliament.[168] In spring 2018, the Commission presented its new position on horizontal provisions on cross-border data flows and personal data protection in EU trade and investment agreement.[169] The accompanying letter has been signed by six commissioners signalling a broad compromise across all affected departments including Justice, Trade, and Digital Single Market, among others. The compromise, however, was only binding on the cabinet of commissioners until the end of their mandate in 2019.[170]

The position consists of three prongs that follow the logic of international trade law: Article A holds a declaratory commitment to enabling cross-border data flows and prohibits restrictions in the form of four concrete data and IT localization requirements.[171] Article B then formulates an unconditional counterbalancing provision for national measures in the interest of the protection of personal data:

> Article B
> Protection of personal data and privacy
>
> 1. 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.
> 2. 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.
> 3. For the purposes of this agreement, 'personal data' means any information relating to an identified or identifiable natural person.
> 4. For greater certainty, the Investment Court System does not apply to the provisions in Articles A and B.[172]

The last prong, Article X on regulatory cooperation with regard to digital trade, carves out issues of cross-border data flows and the protection of personal data from the dialogue on regulatory issues.[173]

In paying attention to devising a proper counterbalancing provision in its new position, the Commission ultimately accepts the delicacy of excepting the EU data protection *acquis* from its commitments under trade and investment law that effectively reverses its early stance. The horizontal exception for a party's respective safeguards on the protection of personal data and privacy is a means to achieve internal consistency when it unties EU data protection measures from EU external trade policy.

Provided that the EU has exclusive competences in the field of external trade, the Commission, after having consulted the Member States in the Trade Policy

166 Jan Albrecht and others, 'MEPs Data Flows Letter to President Juncker', 15 December 2016 <https://marietjeschaake.eu/en/data-flows-letter-to-president-juncker> accessed 5 March 2020.

167 European Parliament Resolution of 12 December 2017, 'Towards a Digital Trade Strategy' (2017/2065(INI)) <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0488+0+DOC+XML+V0//EN> accessed 5 March 2020.

168 Joanna Plucinska and Hans von der Burchard, 'EU Trade, the Martin Selmayr Way' (*Politico*, 18 October 2017) <http://www.politico.eu/article/eu-trade-the-martin-selmayr-way/> accessed 5 March 2020.

169 European Commission, 'Horizontal Provisions for Cross-border Data Flows and for Personal Data Protection (in EU Trade and Investment Agreements),' May 2018 <http://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf> accessed 5 March 2020.

170 Ibid.

171 Parties shall not restrict cross-border data flows by: '(i) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party; (ii) requiring the localisation of data in the Party's territory for storage or processing; (iii) prohibiting storage or processing in the territory of the other Party; (iv) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory'.

172 Ibid.

173 Ibid.

Committee (Services and Investment), started to implement its new position. It submitted the horizontal provisions on cross-border data flows and personal data protection in the trade negotiations with Australia, Chile, Indonesia, Mexico, New Zealand, and Tunisia. The Commission is planning to replace the '*rendez-vous*' clause in the EPA with Japan and the free trade agreement with Mexico with the new position. What is more, the EU has also reproduced its position in its proposal for the ongoing WTO negotiations on trade-related aspects of electronic commerce.[174]

Conclusions

In international trade law, greater attention is being paid to digital trade, cross-border data flows, and the protection of privacy and personal data. The so-called GATS-plus free trade agreements may not only clarify the ambiguities of the WTO framework when it comes to digital trade but also, and most importantly, have a greater bearing on a country's ability to regulate in the field of privacy and data protection, as compared to the 1994 GATS. The GATS, thus far the only multilateral international trade agreement concerning international trade in services, holds very few specific rules on cross-border data transfers confined to specific sectors. Attempts to multilateralize cross-border data flows within the WTO framework have failed so far. However, provision on the free flow of data has been introduced in the CPTPP, USMCA, and the US–Japan Digital Trade Agreement, thereby proliferating the US-led digital trade template.

When the pressure on the EU—due to uncertainties about the new US government's trade policy's strategic directions—momentarily subsided, a precious window opened to reassess its strategy on the international transfer of personal data and to define a position that solidly preserves EU autonomy to regulate privacy and personal data protection in the purview of future trade agreements. From the perspective of the EU, unreservedly committing to free cross-border data flows likely collides with its approach of affording a high level of protection of personal data as is called for by Article 8 of the Charter and as implemented by the GDPR. At this juncture, until recently the EU had been lacking a horizontal strategy to effectively align its normative approach to the protection of privacy and personal data with its external trade policy. This was due to several convolutions in EU policy-making which can be attributed to EU internal divisions of competences, EU institutions' priorities and mandates which exhibited goal conflicts over normative levels of protection and external trade objectives.

In this article, we have traced the process of policy learning and EU institutional dynamics that led to reversing the Commission's approach to its external trade policy from solely relying for its regulatory autonomy in the field of privacy and data protection on the type of general exceptions modelled after GATS Article XIV to a broad horizontal provision containing an almost blank exception for data privacy. The Commission's new position on horizontal provisions on cross-border data flows and personal data protection in EU trade and investment agreements is the product of an intense institutional dialogue between different branches of the Commission and with the involvement of the European Parliament and Member States. The Commission's position is, in our view, capable of sustaining the integrity of its approach to the transnational protection of individuals' fundamental rights because it unconditionally preserves its autonomy to regulate in the interest of data privacy. It is, moreover, prudent to make an exception for domestic privacy and data protection measures from the scope of application of investment protection and regulatory cooperation.

By trade law standards, the Commission's new approach to reconciling cross-border data flows with its personal data protection framework must be considered positively bold. The wording goes beyond the existing counterbalancing provisions in the financial and telecommunications sectors in the GATS and as replicated elsewhere, which are subject to a 'necessity' criterion or an anti-circumvention clause. Aspiring a horizontal provision that excepts data protection and privacy across the entire agreement would effectively overwrite the more narrow exceptions in these service sectors. Remarkably, the new EU approach to privacy and data protection even exceeds normative counterbalancing provisions in favour of labour standards, environmental protection, and sustainable development in a number of post-GATS trade agreements.

As a negotiation position of the EU in trade talks with third countries, the new approach of unconditionally excepting a party's safeguards to ensure the protection of personal data and privacy needs to be agreed to by the other party. A party to the negotiation would likely argue that the EU's proposal amounts to 'GATS-minus' because it demands total regulatory autonomy for domestic rules protecting privacy and personal data vis-a-vis all trade law disciplines. They

174 Communication from the European Union, EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, 26 April 2019, INF/ECOM/22 <https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf> accessed 5 March 2020.

would certainly highlight that such an unconditional exception could be abused as a pretext for otherwise unjustifiable IT and data localization requirements. The Commission, on the other hand, could not deviate significantly from its position without sacrificing EU regulatory autonomy that in turn would risk consistency with the EU privacy and data protection framework.

The diffusion of free data flow commitments in free trade and investments agreements can have hazardous consequences for the regulatory consistency of a third country's data protection framework. If a third country commits to free cross-border data flows in a free trade agreement with yet other countries, it is risking its strategic ability to obtain a finding of adequacy by the Commission in order to freely receive personal data from the EU or risk losing the earlier afforded adequacy status. Pursuant to Article 45(2)(a) of the GDPR, the Commission would assess the rules for onward transfer of personal data to another third country. For example, the Commission's finding that Japan ensures an adequate level of protection does not extend to onward transfers of personal data pursuant to the APEC Cross-Border Privacy Rules. Through the backdoor, the strategy to liberalize free data flows is starting to upset approaches based on mutual recognition of data privacy laws, as practised in the EU and many other countries.

In the interest of EU law consistency, the Commission's position on personal data protection in its external trade policy and the preference given to the regulatory mechanisms of the GDPR must be welcomed. This starkly contrasts with the perceived 'gold standard' for digital trade as championed by the USA and other developed countries prioritizing trade liberalization and the removal of 'unnecessary' restrictions of cross-border data flows. What is certain is that the confrontation between cross-border flows of personal data in a connected world and the fundamental rights to the protection of personal data and privacy in the EU will not subside anytime soon. Future directions in international trade diplomacy should aim to establish realistic coordinates for digital trust in cross-border trade in services, which cannot realistically be parted from individuals' positions of rights as guaranteed in their countries.

doi:10.1093/idpl/ipaa003
Advance Access Publication 30 March 2020