Asian Journal of International Law (2024), **14**, 154–179
doi:10.1017/S204425132300036X

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Trade in the Digital Age: Agreements to Mitigate Fragmentation

Felicity DEANE, Emily WOOLMER, Shoufeng CAO and Kieran TRANTER

Queensland University of Technology, Brisbane, Australia
Corresponding author: Felicity DEANE; felicity.deane@qut.edu.au

(First published online 14 August 2023)

Abstract

Cross-border data flow is essential to contemporary international trade. However, transitioning from paper to digital in international trade has benefits and concerns. Concerns have led to an upsurge in data regulation as nations and regions impose restrictions on data flows and storage. This paper argues that, with increasing concerns about data sovereignty, the reconciliation of differing positions will be necessary to ensure that the benefits of digitization can be realized equally. At present, the objective of "data free flow with trust" is aspirational at best, with emerging trade barriers that unfairly threaten opportunities for small to medium enterprises and development within the Global South. This paper supports new knowledge and demonstrates that discriminatory regulation of data flow and disproportionately prioritizing national interests will be a trade barrier that impacts private entities and consumers in all nations. To avoid unintended externalities, cooperation is needed at a global level.

Keywords: cross-border data flows; international trade; data sovereignty; data free flow with trust; WTO

International trade has always been an informatic exchange, from the grand exchange of culture and knowledge of the world to the tedious exchange of papers, bills of lading, customs certificates, and contracts in triplicate. Consistent with the epochal transition from paper as the informatic medium to digital,[1] contemporary international trade has become increasingly digitalized. Indeed, data has become the medium for international transactions. Consequently, cross-border data flow is essential to contemporary international trade (even when the goods or services are not traded in a digital form).[2] Supplementary to this, the volume of data flow is increasing through negotiated processes. For instance, in February 2021, the *Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific* entered into force.[3] The agreement aimed to progress efficiency in transactions and improve transparency and regulatory

[1] Cornelia VISMANN, *Files: Law and Media Technology* (Stanford: Stanford University Press, 2008), 163–4.

[2] Susan LUND and Laura TYSON, "Globalization is Not in Retreat: Digital Technology and the Future of Trade Essays" (2018) 97(3) Foreign Affairs 130 at 131–3; Robert WOLFE, "Learning about Digital Trade: Privacy and E-Commerce in CETA and TPP" (2019) 18(S1) World Trade Review S63 at S64.

[3] *Framework Agreement on Facilitation of Cross-Border Paperless Trade in Asia and the Pacific*, 19 May 2016 (entered into force 20 February 2021), online: https://treaties.un.org/doc/Treaties/2016/05/20160519%2012-16%20PM/Ch_X-20.pdf.

compliance.[4] These negotiations highlight that the transition from paper to digital in international trade brought benefits and concerns. The benefits of immediacy, automation, and accessibility from the digital are realized through facilitating and reducing the costs of international trade. However, digital trade raises concerns about data security and personal privacy.[5] These concerns and the regulation associated with them have led to risks of digital fragmentation in the global market.[6] In this sense, fragmentation effectively means that the digital environment will be a series of smaller parts rather than one connected system that causes disruptions and unwelcome externalities on trade.

Concerns around data security and privacy are (at times) connected to the global recognition that data has value. For instance, Yakovleva argues that personal data is both a trade commodity and an asset.[7] Chinese documentation recently referred to data as one of the five factors of production, alongside capital, labour, land, and technology.[8] Other commentators have labelled data as "capital" and, as such, its value is increasingly recognized by corporate and governmental entities.[9] As consumption does not decrease the value of data, it can be classified as a non-rival asset; hence, economic theory suggests that social welfare will increase where data is openly shared.[10] However, that recognition of value has been accompanied by an upsurge in data regulation as nations impose restrictions on data flows and storage. As digital transactions become increasingly regulated by nations, there is a corresponding need for global cooperation to avoid laws and policies that lead to digital fragmentation, which in some instances can pose barriers to trade.[11] Fragmentation in this sense can lead to negative economic impacts, market access limitations, and restrictions on the rights of individuals.[12] Alternatively, cooperation may ensure that the benefits of trade facilitated by cross-border data flows can be realized within a policy setting that supports data security and personal privacy.[13]

In World Trade Organization (WTO) e-commerce negotiations, some parties targeted the objective of "data free flow with trust" (DFFT).[14] Although the negotiations in this

[4] United Kingdom Law Commission, "Digital Assets: Electronic Trade Documents", Consultation Paper No 254, 30 April 2021, online: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/04/Electronic-trade-documents-CP.pdf.

[5] Emily LAIDLAW, "Privacy and Cybersecurity in Digital Trade: The Challenge of Cross-Border Data Flows" (22 February 2021) Social Science Research Network, online: SSRN https://ssrn.com/abstract=3790936 at 3. Data security is the safeguarding of information from corruption and external threats; data protection supports replication of the data through backups and other means where the data may be lost, and data privacy is a subset of data security, which supports an individual's right to control their personal information.

[6] Simon J EVENETT and Johannes FRITZ, "Emergent Digital Fragmentation: The Perils of Unilateralism", Centre for Economic Policy Research, Report, 2022 at 46.

[7] 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 477 at 478.

[8] Jathan SADOWSKI, "When Data Is Capital: Datafication, Accumulation, and Extraction" (2019) 6(1) Big Data & Society 2053951718820549, 1–7.

[9] *Ibid.*

[10] Organization for Economic Co-operation and Development (OECD), *Data-Driven Innovation: Big Data for Growth and Well-Being* (Paris: OECD Publishing, 2015) at 196.

[11] Vanya RAKESH, "Regulating Cross-Border Data Flow Between EU and India Using Digital Trade Agreement: An Explorative Analysis" in Stefan SCHIFFNER, Sebastien ZIEGLER, and Adrian Quesada RODRIGUEZ, eds., *Privacy Symposium 2022* (Cham: Springer International Publishing, 2022), 106.

[12] Evenett and Fritz, *supra* note 6 at 17.

[13] Susan A. AARONSON, "Data Is Different, and That's Why the World Needs a New Approach to Governing Cross-Border Data Flows" (2019) 21(5) Digital Policy, Regulation and Governance 13 at 17; Usman AHMED, "The Importance of Cross-Border Regulatory Cooperation in an Era of Digital Trade" (2019) 18 World Trade Review S99.

[14] World Trade Organization (WTO), "E-Commerce Co-Convenors Welcome Substantial Progress in Negotiations" (14 December 2021), online: WTO News https://www.wto.org/english/news_e/news21_e/ecom_14dec21_e.htm [*WTO News*].

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

forum have been slow, they have allowed trade theorists to consider the many issues raised by this goal. In this respect, there are two key components that must be resolved by state parties in order to achieve DFFT. First, the data must be capable of being shared meaningfully. This requires data portability and interoperability, which has been cited as one of the most "challenging barriers to data reuse".[15] Data portability is the right to personally access your own data and reuse that data with another company.[16] This could be considered one of the components of individual data rights. In contrast, interoperability requires corporations to support "interfaces" that "allow users to interact fluidly with users on other services",[17] which will protect individual data rights. The second challenge of DFFT is building a solid and stable shield of trust, much needed in the process of sharing data. This is a sizeable problem that ultimately requires global concerns about data security and privacy to be alleviated through technical standards and international agreements (enacted by private entities). These challenges can be addressed (in part) by negotiation, regulation, and corporate compliance; however, reconciling competing needs and interests is not a simple process.

This paper is a study of the challenges that arise in the pursuit of international DFFT. The key contribution of this paper is to identify actions needed to support this critical objective. Realizing this objective will be a way to avoid the externalities of digital fragmentation, the barriers to global cooperation are significant. The first section of this paper identifies how concerns about cross-border data flows have led to data sovereignty policies and national (and regional) data regulation. This section is both descriptive and analytical as it examines how data regulation, such as those enacted by the European Union (EU) and the People's Republic of China (China), has effectively created forms of trade barriers. The second section adds to the literature on the WTO in regulating global issues in the public-private nexus. Within this part, this paper provides evidence to show that the WTO has not yet been an effective forum for establishing a global consensus on cross-border data flows; nevertheless, negotiations continue and progress has been made through the joint statement on e-commerce, where parties have been promoting the objective of DFFT.[18] The third section identifies the emergence of Preferential Trade Agreements (PTAs) as establishing some international norms in relation to the regulation of cross-border data flows; however, these agreements have not been effective in resolving data flow concerns, nor will they address the fragmentation issue. Hence, the final section is prescriptive and provides some initial steps to avoid fragmentation in the digital era.[19] This paper supports new knowledge and demonstrates that discriminatory regulation of data flow and disproportionately prioritizing national interests will be a trade barrier that ultimately impacts on private entities and consumers. As such, cooperation on this matter is needed at a global level to avoid unintended externalities. For a digital future, this will include continued negotiations at the WTO alongside support for the Global South.

I. Cross-border data flows and data sovereignty

The phrase "digital globalization" has been termed to describe a new era of digitally facilitated trade.[20] Through e-commerce and the adoption of digital formats to facilitate

[15] OECD, *supra* note 10 at 198.

[16] Sophie KUEBLER-WACHENDORFF et al., "The Right to Data Portability: Conception, Status Quo, and Future Directions" (2021) 44 Informatik Spektrum 264.

[17] Bennett CYPHERS and Cory DOCTOROW, "Privacy Without Monopoly: Data Protection and Interoperability", Electronic Frontier Foundation, Report, 12 February 2021 at 2 and 40.

[18] *WTO News, supra* note 14.

[19] *Ibid*.

[20] See Peter VAN DEN BOSSCHE and Werner ZDOUC, *The Law and Policy of the World Trade Organization,* 4th ed. (Cambridge: Cambridge University Press, 2017) at 7.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

paperless trade,[21] the transfer of data across borders is becoming a significant global issue. This intensification of data flows is disrupting the established trading landscape and the long-recognized national and international norms of laws of trade and how information is regulated. Specifically, national concerns with data security, privacy, data portability, and interoperability have led to increasing volumes of national regulation of cross-border data flows. Some of these national regulations are starting to impact global trade,[22] which mobilizes interest and action from the private sector.

Cross-border data flows occur when data is sent between parties that reside in different national jurisdictions. The rise of e-commerce has been one of the reasons for increased data flow (although by no means the only reason). In 1998, the WTO defined "e-commerce" to mean "the production, distribution, marketing, sale or delivery of goods and services by electronic means".[23] Since 1998, e-commerce has changed both in scale and in nature. As Mitchell and Mishra suggest, it remains a "broad and evolving activity".[24] Importantly, digital globalized trade extends beyond e-commerce platforms and retailers. The Australian Department of Foreign Affairs and Trade emphasizes that:

> Digital trade is not just about buying and selling goods and services online, it is also the transmission of information and data across borders. It relies on the use of digital technologies to facilitate trade and improve productivity, for example through simplified customs procedures.[25]

In short, cross-border data flows need to be understood, not just in the narrow e-commerce sense, but in the way these flows form the primary informatic engine for the global economy: "it is becoming clearer by the day that data flows are the heart and soul of digital trade".[26] In particular, the era of digitalization has enabled trade where the absence of proximity previously made it impossible.[27] The increase in trade volumes has not just occurred in developed economies, developing countries have also benefit from easier access and distribution that digitization supports.[28]

In addition, data has value beyond facilitating international trade. Indeed, data has been described as an asset,[29] as one of the five factors of production (as already stated),[30] and as capital.[31] As noted, "[d]ata and connectivity are not just important tools to access

[21] United Kingdom Law Commission, "Digital Assets: Electronic Trade Documents", Summary of Consultation Paper, 2021, online: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/04/6.7434_LC_Digital-assets-consultation-summary_web3.pdf.

[22] Andrew MITCHELL and Jarrod HEPBURN, "Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer" (2017) 19 Yale Journal of Law and Technology 182 at 196–7; Andrew MITCHELL and Neha MISHRA, "Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute" (2019) 22(3) Journal of International Economic Law 389 at 390–1.

[23] *Work Programme on Electronic Commerce*, WTO Doc. WT/L/274 (30 September 1998) [*WPE*].

[24] Andrew MITCHELL and Neha MISHRA, "Data at the Docks: Modernizing International Trade Law for the Digital Economy" (2018) 20(4) Vanderbilt Journal of Entertainment and Technology Law 1073 at 1110.

[25] Australian Government, Department of Foreign Affairs and Trade (DFAT), "International Services Trade & the WTO" *DFAT*, online: DFAT https://www.dfat.gov.au/trade/services-and-digital-trade/services-trade-and-the-wto.

[26] Jan A. MICALLEF, "Digital Trade in EU FTAs: Are EU FTAs Allowing Cross Border Digital Trade to Reach Its Full Potential?" (2019) 53 Journal of World Trade 855 at 865.

[27] Ahmed, *supra* note 13 at S103.

[28] World Economic Forum (WEF), "Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows", White Paper, May 2020 at 8.

[29] Yakovleva, *supra* note 7 at 478.

[30] Sadowski, *supra* note 8.

[31] *Ibid.*

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

overseas markets and customers but are also key ingredients for industrial production".[32] At the same time, the value of data is dependent upon the uses for which it is employed.[33] This means that not all data will lead to value creation, although much of it will.[34] Where it does generate value, as a non-rivalrous good (that is, its use by one person will not affect the use by another), open sharing of data should enhance social welfare.[35] Conversely, where barriers are erected to data sharing, costs will be imposed upon private entities that can potentially have detrimental flow-on consequences.

For these reasons, striking the right balance in data security requirements represents a substantial challenge in the era of digital globalization.[36] Regulation of cross-border data flows is often introduced to ensure the safe movement of personal data and metadata around the world.[37] Indeed, data security to support data privacy, which is considered in many countries to be a fundamental human right,[38] is critical to ensure consumer confidence. In addition, data and system security is needed to combat cybercrimes. The Budapest Convention, which was opened for signature in 2001, was conceptualized with a view to minimize cybercrimes through harmonized domestic legislative measures and to promote security through "greater unity" between the signatories.[39] This convention recognized that harmonization can lead to better security for all nations and, although it will not prevent digital fragmentation, it is one element needed in a global framework that supports data flow.

The movement of data has become a critical issue in the global trading landscape. Aligned with this, nations are trying to find an equilibrium between data security and international economic cooperation, which requires some policy alignment at an international level to address competing concerns.[40] Despite the need for cooperation and alignment in an era characterized by economic statecraft,[41] coupled with amplified data security risks (and fear),[42] data sovereignty has become a policy objective within some nations. Enforcing sovereignty over data could be considered a way of exercising control over data subjects[43] and those entities that need data to engage in commerce. Data sovereignty is a phrase which indicates that nations can restrict the movement of data, prevent data transfer across borders, or at the very least, set minimum standards for

[32] WEF, *supra* note 28 at 8.

[33] OECD, *supra* note 10 at 193.

[34] See, for example, WEF, *supra* note 28 at 12.

[35] OECD, *supra* note 10 at 187.

[36] Digital Sense User, "Data Security or Data Protection: What's the Difference?" (28 June 2018), online: Digital Sense http://digitalsense.com.au/to-protect-or-secure-that-is-the-question/.

[37] Samuel ABU, "Right to Privacy, Data Protection and IOTs: An Appraisal of Legal Issues Covering Cross-Border Data Transfer" (November 2019) Social Science Research Network, online: SSRN https://ssrn.com/abstract=3848782.

[38] Oliver DIGGELMANN and Maria Nicole CLEIS, "How the Right to Privacy Became a Human Right" (2014) 14 (3) Human Rights Law Review 441; Australian Government, Office of the Australian Information Commissioner (OAIC), "What is Privacy?", online: OAIC https://www.oaic.gov.au/privacy/your-privacy-rights/what-is-privacy/.

[39] *Convention on Cybercrime*, 23 November 2001, CETS No 185 (entered into force on 1 July 2004), online: Council of Europe https://rm.coe.int/1680081561.

[40] *Ibid.*

[41] Vinod K. AGGARWAL and Andrew W. REDDIE, "Economic Statecraft in the 21st Century: Implications for the Future of the Global Trade Regime" (2021) 20 World Trade Review 137 at 137.

[42] Helena CARRAPICO and Benjamin FARRAND, "Discursive Continuity and Change in the Time of Covid-19: The Case of EU Cybersecurity Policy" (2020) 42(8) Journal of European Integration 1111 at 1112.

[43] Konstantinos KOMAITIS, "The "Wicked Problem" of Data Localization" (2017) 2(3) Journal of Cyber Policy 355 at 356.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

the storage of that data.[44] Asserting data sovereignty can support multiple policy objectives that include: the security of personal data and the privacy of citizens, national security, censorship, and population control.[45] However, this is also an objective that challenges traditional notions of sovereignty, particularly in those countries that extend their legal reach into cyberspace and necessarily beyond their own borders.[46] The uncertainty posed by digital transfer may also mean that control is not possible (or desirable in some instances).[47]

Globally, there are increasing numbers of laws that impact the digital domain, introduced at a national level.[48] Data policies often focus on data localization (or restrictions on cross-border data transfers), use, storage, and other data transfer requirements.[49] Each of these presents challenges and arguably increases the risk of digital fragmentation.[50] For instance, data localization rules attempt to stop personal data or metadata from flowing beyond a nation's borders,[51] which is a measure that some countries employ to support both cybersecurity and privacy requirements. Komaitis describes "forced data localization" as a "conscious governance decision under which the storage of data takes place on a device that is physically located within the country where the data were created".[52] Indeed, data localization requirements often necessitate operators to provide *within jurisdiction storage facilities* to conduct business or trade within a nation.[53] This, of course, increases the costs of trade, which ultimately impacts consumers.

As data localization rules decrease productivity and increase the cost of doing business within a nation, they can be categorized as protectionist measures.[54] For this reason, they are (sometimes) considered an "extreme" response to two categories of real or perceived risks arising from cross-border data flow.[55] First, that cross-border data flow exposes the data to interception and appropriation by hostile entities – foreign powers, commercial rivals, or cyber criminals.[56] Second, transmitting data beyond the nation's borders means that a desired level of security of personal privacy (or other sensitive information)

[44] European Union Agency for Network and Information Security (ENISA), "Technical Guidelines for the Implementation of Minimum Security Measures for Digital Service Providers", European Union Agency for Cybersecurity, Report, 2016, online: ENISA https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers.

[45] Stéphane COUTURE and Sophie TOUPIN, "What does the Notion of 'Sovereignty' Mean When Referring to the Digital" (2019) 21(10) News Media and Society 2305 at 2360; Yudhistira NUGRAHA and Ashwin Sasongko SASTROSUBROTO, "Towards Data Sovereignty in Cyberspace" (2015) 3rd International Conference on Information and Communication Technology 465 at 466.

[46] Islam JUSUFI, "Uncertainty, Fragmentation, and International Obligations as Shaping Influences: Cyber Security Policy Development in Albania" in Myriam DUNN CAVELTY and Andreas WENGER, eds., *Cyber Security Politics* (London: Routledge, 2022), 172.

[47] *Ibid.*, at 173.

[48] Evenett and Fritz, *supra* note 6.

[49] *Ibid.*

[50] *Ibid.*

[51] Abu, *supra* note 37.

[52] Komaitis, *supra* note 43 at 356.

[53] Anupam CHANDER and Uyen LE, "Breaking the Web: Data Localization vs. the Global Internet" (2014) Emory Law Journal 1 at 35–7.

[54] Iva MIHAYLOVA, "Could the Recently Enacted Data Localization Requirements in Russia Backfire?" (2016) 50 (2) Journal of World Trade 313; Nigel CORY and Luke DASCOLI, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them" *Information Technology and Innovation Foundation* (19 July 2021), online: Information Technology and Innovation Foundation https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost.

[55] Mihaylova, *supra* note 54 at 326; Laidlaw, *supra* note 5.

[56] Seyed Ebrahim DORRAJI and Mantas BARČYS, "Privacy in Digital Age: Dead or Alive?! Regarding the New EU Data Protection Regulations" (2014) 4(2) Socialinės Technologijos 306 at 307; "New Technology Has Enabled

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

in the nation of origin might not apply to the data once it arrives in a different jurisdiction. Analysis of these risks demonstrates that it is not the location of the data that will assure its security (after all, most information will inevitably need to be transmitted even within a nation's borders); rather, it is the method of storage and/or data sharing that creates data vulnerabilities. However, this does not stop nations from requiring that their data be stored locally and, in some instances, these localization requirements are encapsulated within the legal framework.

Governments from most larger economies are in the process of "deploying a wide range of tools to shape and nurture the digital domain".[57] One of the most well-known examples of regulation of cross-border data flow is the strict measures introduced by the EU through the General Data Protection Regulation (GDPR).[58] While the scope of the GDPR is limited to personal data,[59] the security level required once this threshold condition is met is significant. The extraterritorial scope was drafted to ensure that any personal data transferred out of the EU would be subject to the same level of security that would be offered within its borders. Although one of the EU's core objectives is to facilitate cooperation between nations (at least, within the EU),[60] the security of personal data has become one of the region's policy imperatives. In contrast to the objectives of the EU, China has also proposed laws that provide security of personal data for its citizens while maintaining national data sovereignty. Although the laws of these two jurisdictions align, the national security priority within China is far more prominent.[61] Indeed, the objective of data sovereignty is far more pronounced in the Chinese requirements than those in the EU. These are, of course, just two examples of jurisdictions where such provisions have been enacted. There are many more. It is this bottom-up approach, supporting national and regional self-interest, that has led to fears of global digital fragmentation.

A. Regulation of Cross-Border Data Flows

Data security laws have been increasingly implemented around the world, particularly in G20 countries.[62] Although a degree of homogeneity is demonstrated in these laws, digital fragmentation may be an undesirable outcome of small differences in the requirements. The EU has led the way with its regional GDPR.[63] The GDPR was enacted in 2018 with the objective of protecting the fundamental right to the security of personal data.[64] It prescribes a high level of personal data security in cross-border data flow with the aim of ensuring that all data transferred within and outside of the EU is protected. The GDPR provides a clear definition of what is meant by personal data and includes "any

Cyber-Crime on an Industrial Scale" *The Economist* (6 May 2021), online: The Economist https://www.economist.com/international/2021/05/06/new-technology-has-enabled-cyber-crime-on-an-industrial-scale.

[57] Evenett and Fritz, *supra* note 6 at 21.

[58] *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*, Official Journal of the EU L 119/1 [*GDPR*].

[59] *Ibid*., art. 1.

[60] Dimitra MARKOPOULOU, Vagelis PAPAKONSTANTINOU, and Paul DE HERT, "The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation" (2019) 35(6) Computer Law and Security Review 105336 at 105344.

[61] Aimin QI, Guosong SHAO, and Wentong ZHENG, "Assessing China's Cybersecurity Law" (2018) 34 Computer Law & Security Review 1342 at 1344–5.

[62] Evenett and Fritz, *supra* note 6 at 47.

[63] Matthias BAUER et al., "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localization Measures in the EU Member States" ECIPE Policy Brief, Research Report No. 3/2016, 2016.

[64] *GDPR*, *supra* note 58, art. 1.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

information relating to an identified or identifiable natural person".[65] Further, the GDPR applies in circumstances where the data is processed by automated means or forms part of a filing system.[66] While these restrictions limit some of the applications of the GDPR, commentators have labelled the GDPR as the gold standard in data security.[67]

The consequence of the GDPR's high level of security is that it often requires personal information to remain in the territory (specific localization),[68] prohibiting the transfer of data to a third-party nation unless an exemption applies.[69] There are three main exceptions to this within the GDPR. For instance, Article 45 allows transfers to a nation outside the EU where that nation's own data security laws provide an adequate level of security.[70] However, few countries have been recognized as having an adequate standard of security hence[71] this exemption does little to eliminate the trade barrier erected by the restriction provision.[72] Article 46 also provides an exemption where adequate safeguards are provided by the controllers of personal data.[73] This exemption places costs on the corporations that handle personal data of EU origin to ensure that adequate data security is maintained.[74] However, this exception is only supported for intra-company transfers, which significantly limits its application.[75] Finally, Article 49 outlines derogations for specific situations such as a public interest reason or where the data is necessary for the performance of a contract.[76] Chander summarizes Article 49 exception as "consent or necessity".[77] Both consent and necessity are difficult to satisfy in the context of the GDPR. Consent is onerous and can be revoked, and the necessity exception is "narrowly construed".[78] The end result is that the GDPR could be described as trade restrictive[79] by coaxing rather than mandating localization through extensive limitations on cross-border data transfer.

[65] *Ibid*., art. 4(1). Article 4(1) states:

> "[P]ersonal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[66] *Ibid*., art. 2.

[67] Giovanni BUTTARELLI, "The EU GDPR as a Clarion Call for a New Global Digital Gold Standard" (2016) 6(2) International Data Privacy Law 77; Alessandro MANTELERO, "The Future of Data Protection: Gold Standard vs. Global Standard" (2021) 40 Computer Law and Security Review 105500.

[68] Elisabeth MEDDIN, "The Cost of Ensuring Privacy: How the General Data Protection Regulation Acts as a Barrier to Trade in Violation of Articles XVI and XVII of The General Agreement on Trade Services" (2020) 35 (4) American University International Law Review 997 at 1007.

[69] *GDPR*, *supra* note 58, Chapter 5.

[70] *Ibid*., art. 45.

[71] Anupam CHANDER, "Is Data Localization a Solution for Schrems II?" (2020) 23 Journal of International Economic Law 771 at 774.

[72] Aaditya MATTOO and Joshua MELTZER, "International Data Flows and Privacy: The Conflict and its Resolution" (2019) 21(4) Journal of International Economic Law 769 at 788.

[73] *GDPR*, *supra* note 58, art. 46.

[74] Ioannis NTOUVAS, "Exporting Personal Data to EU-Based International Organizations under the GDPR" (2019) 9(4) International Data Privacy Law 272 at 277 and 280.

[75] Chander, *supra* note 71 at 775.

[76] *Ibid*., at 277; *GDPR*, *supra* note 58, art. 49.

[77] Chander, *supra* note 71 at 775.

[78] *Ibid*., at 776.

[79] Meddin, *supra* note 68 at 1036.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

Although most countries in the world have introduced data security legislation,[80] the examination of the GDPR remains important as it was "designed to be a flagship of the user-centred approach".[81] For the purposes of this paper, consideration of this regional framework demonstrates that limitations on cross-border data transfer are not the same as strict data localization requirements. Both policy approaches will lead to data fragmentation; however, while restrictions on cross-border data transfer are relatively common,[82] data localization requirements have featured in relatively few data security regimes.[83] One such example exists in China. In November 2016, China passed its first Cybersecurity Law,[84] and in 2021, the Data Security Law (DSL) and the Personal Information Protection Law (PIPL) have added to the framework. The DSL and the PIPL reflect some features of the GDPR, despite the policy differences that underpin them.[85] One point of contention is that of data localization requirements.

The 2016 Cybersecurity Law introduced strict data security standards on private operators. This legislation prescribed that network operators were not permitted to collect data unrelated to the service they provided,[86] and the collection and usage of private information was only permitted with the user's consent.[87] The data collected was not to be disclosed, damaged, tampered with, or shared with others unless the user gave permission.[88] Further, network operators were required to take security measures to ensure the safety of private information and in the event of an information breach or loss, notification was required to be sent to the relevant authority and users.[89]

The Cybersecurity Law were extended in December 2019 with the Cybersecurity Multi-Level Protection Scheme (MLPS) imposing hierarchical obligations on network operators.[90] The level of obligation correlated with the scope of the damage caused to the Chinese people or their government that would result from any breach of the system.[91] The Cybersecurity MLPS also placed an increased burden on Chinese companies to protect data and extended the compliance mechanisms to all companies that stored data in China. Further, more onerous requirements were imposed where the data was considered to fall within a "security sensitive" category. Combined, the cybersecurity laws mandate that companies which have access to and store Chinese data must store it in China in compliance with the requirements specified in the cybersecurity laws. As a

[80] United Nations Conference on Trade and Development (UNCTAD), "Data Protection and Privacy Legislation Worldwide" (14 December 2021), online: UNCTAD https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[81] Evenett and Fritz, *supra* note 6 at 48.

[82] *Ibid*., at 49. Limitations on cross-border data transfer have featured in the EU, China, Brazil, South Africa, Saudi Arabia, India (proposed – now withdrawn), and Japan.

[83] *Ibid.*

[84] Qi, Shao, and Zheng, *supra* note 61 at 1342.

[85] *Ibid*., at 1342. The *Cybersecurity Law of the People's Republic of China*, 7 November 2016 (entered into force 1 June 2017) [*Cybersecurity Law of the People's Republic of China 2016*] states that one of its purposes is to "safeguard cyberspace sovereignty".

[86] *Cybersecurity Law of the People's Republic of China 2016*, *supra* note 85, art. 41.

[87] *Ibid.*

[88] *Ibid.*, art. 42.

[89] *Ibid*.

[90] *The Cybersecurity Multi-Level Protection Scheme* (2019) National Information Security Standardization Technical Committee of the People's Republic of China, online: The People's Government of Beijing Municipality http://banshi.beijing.gov.cn/pubtask/task/1/110000000000/c22ab389-19b8-4e5f-b0ba-49d4776cac94.html?locationCode=110000000000 [*Cybersecurity Multi-Level Protection Scheme 2019*] will apply to all "networks" operating in China. This defines "network" as a system that protects computers or related equipment that "gathers, stores, transmits or processes information". This is broad enough to cover any computer operation or company storage as being a "network".

[91] *Ibid.*; Qi, Shao, and Zheng, *supra* note 61 at 1346.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

point of difference (and potential concern), the laws provide that any data could be copied and kept by the Chinese government.[92] This feature has been recognized as unique to Chinese law. Indeed, no technology that blocks access by the Ministry of Public Security is permitted. As noted:

> China is creating a system to achieve two ultimately contradictory objectives: the system will be closed against intrusion by "bad actors" (foreigners and internal dissidents), but completely transparent to the Ministry of Public Security and other internet security agencies of the PRC government and the Chinese Communist Party (CCP).[93]

Following the introduction of the 2019 Cybersecurity MLPS, the DSL was implemented.[94] Although the DSL provides no additional guarantee of data security against the state, it does demonstrate a commitment to protect "[Comprehensive Trans-Pacific Partnership] users against cyber criminals".[95] Under Article 21 of the DSL, data is categorized according to its perceived importance and security risks. Data that is categorized as either the "core data of the state" or "important data" will have stricter security requirements over what is referred to as "general data".[96] The DSL prohibits any entity from furnishing data to an external entity unless specific permission is granted by the Chinese government.[97] Article 31 reserves certain cross-border transfers of data to the Cybersecurity Law and provides additional requirements for cross-border flow. The DSL divides cross-border data flow into two areas: localization and outbound security assessment.[98] Article 37 of the Cybersecurity Law contains localization requirements: "[p]ersonal information and important data collected and generated by operators of critical information infrastructure during operations within the territory of the People's Republic of China shall be stored within the territory".[99]

In August 2021, the National People's Congress adopted the PIPL,[100] which is intended to form the third pillar of China's data security regime.[101] It entered into effect on 1 November 2021 with the aim to: "protect the rights and interests of individuals; regulate personal information processing activities; safeguard the lawful and 'orderly flow' of data; and facilitate reasonable use of personal information."[102] With these aims there is clear

[92] Qi, Shao, and Zheng, *supra* note 61 at 1351.

[93] Steve DICKINSON, "China's New Cybersecurity System: There Is NO Place to Hide" *Harris Bricken* (7 October 2019), online: Harris Bricken http://harrisbricken.com/chinalawblog/chinas-new-cybersecurity-system-there-is-no-place-to-hide/.

[94] Jihong CHEN and Jiabin SUN, "Understanding the Chinese Data Security Law" (2021) 2(3) International Cybersecurity Law Review 1; Jenny SHENG, Chunbin XU, and Esther TAO, "China Adopts New Data Security Law" *Pillsbury Law* (7 September 2021), online: Pillsbury Law https://www.pillsburylaw.com/en/news-and-insights/china-adopts-new-data-security-law.html.

[95] Lorand LASKAI and Segal ADAM, "The Encryption Debate in China: 2021 Update" *Carnegie Endowment for International Peace* (31 March 2021), online: Carnegie Endowment for International Peace https://carnegieendowment.org/2021/03/31/encryption-debate-in-china-2021-update-pub-84218.

[96] *Ibid.*

[97] Dickinson, *supra* note 93.

[98] *Cybersecurity Law of the People's Republic of China 2016*, *supra* note 85.

[99] *Ibid.*, art. 37.

[100] Josh HORWITZ, "China Passes New Personal Data Privacy Law, to Take Effect Nov. 1" *Reuters* (20 August 2021), online: Reuters https://www.reuters.com/world/china/china-passes-new-personal-data-privacy-law-take-effect-nov-1-2021-08-20/.

[101] Sheng, Xu, and Tao, *supra* note 94.

[102] Hunter FORWART, Gabriela ZANFIR-FORTUNA, and Clarisse GIROT, "China's New Comprehensive Data Protection Law: Context, Stated Objectives, Key Provisions" *Future of Privacy Forum* (20 August 2021), online:

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

similarity between the PIPL and the GDPR. First, the definition of "personal information" as "various kinds of information related to identified or identifiable natural persons" other than that which is processed anonymously, is similar to the definition in the GDPR.[103] Second, the PIPL, together with the DSL, requires corporations to closely consider their own policies regarding collecting, processing, and storing information.[104] Third, the PIPL has extraterritorial reach, which requires that any company collecting Chinese citizens data must comply with the regulations.[105] Therefore, if compliance is difficult or not possible, the Chinese laws are *de facto* localization requirements.

The main difference between the Chinese regime and the GDPR is the very clear declaration of Chinese data sovereignty.[106] Within Chinese law, there are clear allowances for barriers to cross-border data flow due to national security. This is similar to the Indian Personal Data Protection Bill 2018,[107] which, at the time of writing, had been withdrawn by the Indian government.[108] The Chinese laws, in particular, "has a distinct 'national security' flavour, particularly around its provisions on localization and cross-border transfers".[109] The PIPL, for instance, requires that there is content and risk assessment prior to the cross-border transfer of personal information.[110] However, the differences in objectives have not necessarily resulted in substantive differences between the regimes and both impose restrictions on trade through cross-border data flow.

In sum, differences between newly introduced data security laws could have significant flow-on consequences for market access and international trade. In China, the restrictions imposed through the DSL and the PIPL manifest a formal agenda of personal privacy for Chinese citizens. However, with the Chinese laws, the sovereignty of the Chinese state over Chinese data is particularly emphasized by the myriad of provisions that allow for state entities to access data. Although the GDPR does not support state access to data in the same way as the Chinese framework, it does introduce onerous requirements upon all companies who collect personal information. Putting the virtues of these laws aside, both impose a non-tariff barrier to trade by mandating standards and processes in how personal data can be transferred, stored, and used.[111] This is not an unusual situation for world trade. Nations often introduce domestic laws and regulations that impact trade relationships at the cost of international commerce.[112] While the digitalization of trade and the intensification of cross-border data flows present novel and emerging problems, the need for forums to cooperate on "trade impacting" national laws and

Future of Privacy Forum https://fpf.org/blog/chinas-new-comprehensive-data-protection-law-context-stated-objectives-key-provisions/.

[103] KPMG Cybersecurity, "Overview of Draft Personal Information Protection Law in China", Report, 10 November 2020, online: KPMG https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2020/11/overview-of-draft-personal-information-protection-law-in-china.pdf.

[104] Horwitz, *supra* note 100.

[105] *Ibid.*

[106] Jyh-An LEE, "Hacking into China's Cybersecurity Law" (2018) 53(1) Wake Forest Law Review 57 at 89; Sarah WANG HAN and Abu Bakar MUNIR, "Information Security Technology – Personal Information Security Specification: China's Version of the GDPR Reports: Practitioner's Corner" (2018) 4(4) European Data Protection Law Review 535.

[107] Evenett and Fritz, *supra* note 6 at 49.

[108] Manish SINGH, "India Withdraws Personal Data Bill that Alarmed Tech Giants" *TechCrunch* (4 August 2022), online: Tech Crunch https://techcrunch.com/2022/08/03/india-government-to-withdraw-personal-data-protection-bill/.

[109] Lee, *supra* note 106; Wang Han and Munir, *supra* note 106.

[110] *Personal Information Protection Law*, 20 August 2021, (entered into force 1 November 2021) [*PIPL*], arts. 39 and 54.

[111] Mattoo and Meltzer, *supra* note 72.

[112] Aggarwal and Reddie, *supra* note 41 at 137.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

regulations is an evergreen concern. However, the particular challenge of DFFT has proven a difficult one to address using existing negotiation arrangements. Although analysis of different regulatory regimes indicates that barriers already exist,[113] cooperation will be needed in order to avoid exacerbating the economic and social pitfalls of data fragmentation. Unfortunately, cooperation in the current era is elusive.

II. The world trade organization and the digitalization of trade

The WTO is the only international institutional body governing global trade.[114] It should have a significant role in the globalized economy and should be the forum where tensions between data sovereignty and data free flow are resolved. The WTO framework has some clear strengths. Within this forum, there have been successful negotiations on many complex matters borne out of the common interest of negotiating parties. Further, it is an international setting where member nations should negotiate common values and principles, such as rules aligned with societal values and interests. The common recognized values include (*inter alia*): protecting human, animal, or plant life or health; protecting natural resources; protecting public morals; and protecting privacy.[115] In addition, there are also rules designed to promote the harmonization of national regulations. For instance, the agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) lays down the minimum requirements for the protection of intellectual property rights. This is a point of difference from other WTO agreements; they are considered to be beyond-the-border measures. These forms of agreement are generally considered to be more troublesome to negotiate. As noted, "[t]he rules in these ... agreements ... go far beyond the usual trade liberalization rules and venture into behind-the-border regulatory areas to a greater extent than other WTO agreements dealing with other non-tariff barriers to trade".[116]

In such instances, finding an appropriate balance between the right to regulate and enforcing the rules-based order of the world trading system is a challenge that is increasing rather than decreasing. This challenge is exacerbated by the growing interconnectedness of economies. There are different theories on what the balance should be. For instance, Rigod suggests that it is only where domestic (or regional) policies cause unnecessary externalities that they should be subject to the rigours of WTO dispute settlement.[117] Although there are merits in this approach, providing rules and adjudication in support of this standard could present difficulties. Data fragmentation will cause disruptions to trade in the form of externalities. Thus, in this respect, data fragmentation could cause unnecessary tensions between nations.[118] Consequently, the negotiations and, ideally, the rules of the WTO should legitimately extend to matters of data security in the hope of avoiding the costs associated with these increasing trade barriers. For these reasons, the WTO should prioritize discussions to foster cooperation in this policy space.

[113] Evenett and Fritz, *supra* note 6 at 55.

[114] Mary FOOTER, *An Institutional and Normative Analysis of the World Trade Organization* (Leiden: Brill, 2005) at 24; Robert KOOPMAN et al., "The Value of the WTO" (2020) 42(4) Journal of Policy Modelling 829 at 830–1; WTO, "What is the WTO?" *WTO*, online: WTO https://www.wto.org/english/thewto_e/thewto_e.htm.

[115] *General Agreement on Trade in Services,* 15 April 1994, 1869 U.N.T.S. 183, 33 I.L.M. 1167 (entered into force 1 January 1995) [*GATS*], arts. XX and XXI.

[116] Peter VAN DEN BOSSCHE, *The Law and Policy of the World Trade Organization,* 2nd ed. (Cambridge: Cambridge University Press, 2008) at 41.

[117] Boris RIGOD, "Optimal Regulation and the Law of International Trade: A Law & Economics Analysis of the WTO Law on Domestic Regulation", Department of Law, European University Institute (EUI), Thesis, 15 January 2014, online: EUI https://cadmus.eui.eu/handle/1814/32095.

[118] Evenett and Fritz, *supra* note 6 at 55.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

Unfortunately, the current rules of international trade do not address or protect data flow in a way that is "consistent, comprehensible and predictable".[119] In addition, there are challenges in applying the existing rules to laws and regulations that reflect data sovereigntist stances. Although some restrictive data flow practices, such as in the GDPR or the Chinese laws, arguably constitute a violation or breach of obligations under the current trade rules, there is considerable uncertainty in the application of the WTO framework to these matters.[120] While there has been some deliberation about the applicability of the current framework, members generally agree that the best way forward will require new rules that specifically address cross-border data flows.[121] Indeed, it is the existing gaps in the WTO rules that have enabled members to unilaterally impose data localization requirements and other trade-restrictive measures.[122] However, due to the current state of disorder in the WTO's dispute settlement system, enforcement of even the strictest measures is difficult. Despite this, a new agreement or amendments to existing agreements could potentially support a smoother transition for existing or revised exception provisions. [123] However, at this stage, members appear to be aligned on keeping data flow as a matter of state sovereignty, which means that a state of digital fragmentation will continue.

Members within the WTO have debated digital enabled trade over the past three decades.[124] A specific point of contention is categorizing cross-border data flows, which, as identified, can be both the end objective of trade (trade of digital or virtual goods and services) and a side-effect of a transaction between parties (with digital communication the norm for international trade). In the absence of explicit definitions and categorization, several scholars have argued that digital trade should logically fall under the General Agreement of Trade in Services (GATS);[125] however, the application of the GATS in these instances would be limited in scope and would only be inclusive of traditional digitally transmitted products (or services),[126] leaving other data flow questions unanswered.[127] Of course, the GATS is just one possible agreement for dealing with cross-border data flows. The Information Technology Agreement removes tariffs on information

[119] Mitchell and Hepburn, *supra* note 22 at 187.

[120] *Ibid.*, at 221–2.

[121] *Joint Statement on Electronic Commerce*, WTO Doc. WT/L/1056 (25 January 2019) [*E-Commerce Joint Statement*]; Rajan NEERAJ, "Trade Rules for the Digital Economy: Charting New Waters at the WTO" (2019) 18(S1) World Trade Review S121 at S140.

[122] Simon ABENDIN and Pingfang DUAN, "Global E-Commerce Talks at the WTO: Positions on Selected Issues of the United States, European Union, China, and Japan" (2021) World Trade Review 1 at 2.

[123] Tatiana LACERDA PRAZERES, "Trade and National Security: Rising Risks for the WTO" (2020) 19(1) World Trade Review 137.

[124] For example, at the Ministerial Conference (M.C.) in Geneva in 1998, the *Declaration of Global Electronic Commerce*, Declaration No. 98-2148, WTO Doc. WT/MIN(98)/DEC/2 (25 May 1998) was adopted and, more recently, at the M.C. in Buenos Aries in 2017, the *E-Commerce Joint Statement, supra* note 121, was established.

[125] Farrokh FARROKHNIA and Cameron RICHARDS, "E-Commerce Products Under the World Trade Organization Agreements: Goods, Services, Both or Neither?" (2016) 50(5) Journal of World Trade 793 at 796–7. See also John-Ren CHEN and Christian SMEKAL, "Should the WTO Deal with E-Trade Taxation Issues?" (2009) 9(4) Progress in Development Studies 339; Sam FLEUTER, "The Role of Digital Products Under the WTO: A New Framework for GATT and GATS Classification" (2016) 17(1) Chicago Journal of International Law 26; Ignatius YORDAN NUGRAHA, "Is Tangibility a Prerequisite? Digital Products as Goods" (2020) 15(2) Asian Journal of WTO and International Health Law and Policy 691.

[126] Fleuter, *supra* note 125 at 160; Lee TUTHILL and Martin ROY, "GATS Classification Issues for Information and Communication Technology Services" in Mira BURRI and Thomas COTTIER, eds., *Trade Governance in the Digital Age: World Trade Forum* (Cambridge: Cambridge University Press, 2012), 157–79.

[127] Chen and Smekal, *supra* note 125; *The Work Programme on Electronic Commerce: Note by the Secretariat*, WTO Doc. S/C/W/68 (16 November 1998), at 10, paras. 37–8.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

technology products (hardware products)[128] and the TRIPS agreement protects intellectual property including trade secrets.[129] Both agreements complement the GATS provisions, which include annexes like those on financial services or telecommunication, designed to take into account the circumstances of specific sectors.[130] Together, these agreements and annexes establish a broad framework that collectively sets some standards for technology transfer and some level of data security.[131] However, despite several agreements intended to address areas related to digital technologies, cross-border data flow represents a vast chasm in the WTO rules landscape.[132]

There are some elements of existing agreements that could spark a future agreement on privacy and data flows; for instance, in the GATS exception provisions. Article XIV(c)(ii) of the GATS permits trade restrictions that are necessary for the "protection of privacy of individuals in relation to the processing and dissemination of personal data".[133] Although this indicates that members agree that privacy is essential, this provision was drafted in the early days of digitalization (of the global economy) before many of the complexities of the digital trade environment were identified. As a result, the rules were not designed to deal with the volume of data transfer from cross-border transactions that subsequently arose.[134] As Tuthill and Roy identified, digital advances moved many services to online supply, where this was once impractical (if not impossible).[135] Further, the question of what the exception allows has not been tested through the dispute settlement procedures.[136] Hence, there is a risk that members could attempt to rely on the "right to privacy" to excuse disguised restrictions on international trade, much like some members have attempted to do through the invocation of the national security exception.

While this exception provision points to the agreed values of WTO members, it does nothing to fill the gap that exists in relation to the digitization of trade and cross-border data flows. At the same time, the specific matters have not been completely overlooked by members, but it has certainly not been "comprehensively" addressed.[137] The Work Programme on Electronic Commerce (WPE), commissioned in 1998, was the first attempt to develop minimal standards on the legal structures surrounding e-commerce.[138] The Work Programme has been on the WTO negotiation agenda since this time, with the only substantive issue resolved (and repeatedly revisited) being the moratorium on customs duties on electronic transmissions. The agreement not to impose customs duties on electronic transmissions has been reaffirmed every two years since the establishment of

[128] *Ministerial Declaration on Trade in Information Technology Products*, WTO Doc. WT/MIN(96)/16 (13 December 1996).

[129] *Agreement on Trade-Related Aspects of Intellectual Property Rights*, 15 April 1994, 1869 U.N.T.S. 299 (entered into force 1 January 1995) [*TRIPS*], art. 39, provides protection against undisclosed information.

[130] *GATS, supra* note 115.

[131] Mira BURRI and Thomas COTTIER, "Introduction: Digital Technologies and International Trade Regulation" in Mira BURRI and Thomas COTTIER, eds., *Trade Governance in the Digital Age: World Trade Forum* (Cambridge: Cambridge University Press 2012), 1 at 1 and 4.

[132] Susan A. AARONSON and Patrick LEBLOND, "Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO" (2018) 21(2) Journal of International Economic Law 245 at 251.

[133] *GATS, supra* note 115, art. XIVI(ii).

[134] Tuthill and Roy, *supra* note 126 at 157.

[135] *Ibid*., at 158.

[136] Rolf WEBER, "Regulatory Autonomy and Privacy Standards under the GATS" (2012) 7(1) Asian Journal of WTO and International Health Law and Policy 25 at 27.

[137] Merit JANOW and Petros MAVROIDIS, "Digital Trade, E-Commerce, the WTO and Regional Frameworks" (2019) 18(S1) World Trade Review S1 at S3.

[138] C. SATAPATHY, "WTO Work Programme on Electronic Commerce: A Developing Country Perspective" (1999) 34(39) Economic and Political Weekly 2771; Biswajit DHAR, "Electronic Commerce and the WTO: The Changing Contours of Engagement" Madhyam, Briefing Paper 21, November 2017 at 2–3.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

the WPE.[139] The WPE was not established to deal with matters that have since arisen in relation to data security and localization rules, with the exception of the requirement to consider the GATS privacy exception provisions.[140] Indeed, the national security exception provisions were excluded from reference in the WPE documentation.[141] Therefore, as one would expect, the WPE has not been a forum where data localization and other protectionist policies have been raised.

Interestingly, the decade-long negotiation "deadlock" that followed the Doha negotiations has led members to pursue alternatives to traditional agreements. In particular, plurilateral "discussions" have been pursued as a tangential approach.[142] Referred to as joint statement initiatives (JSIs), this plurilateral *approach* to negotiations is recognized by the WTO rules.[143] It is through this medium that e-commerce has been addressed by a growing number of nations.[144] In 2021, the participation in the e-commerce discussions, labelled *Trade Related Aspects of Electronic Commerce*, increased to eighty-six members.[145] This is unsurprising given the importance of e-commerce, and the regulation of it, to the private sector. The scope of discussions in this JSI are far broader than matters of e-commerce and include data localization requirements,[146] cybersecurity threats, and online consumer protection.[147] Although these issues must be considered, it is uncertain whether this JSI (or any other) will have a broader impact on WTO rules or even on the commitments made by participating nations. Although the process of negotiations is supported, the legal status of the *outcomes* of the talks is not addressed by the WTO Agreements.[148] The uncertain status is unlikely to be resolved by consensus as the process of JSI negotiations has been criticized by some nations for lacking transparency[149] and resisted for being contrary to consensus-based decision-making.[150] Other commentators recognize that although JSIs may not solve the problems created by the WTO negotiation deadlock, they have been seen as a partial solution that could address the stalemates created through the consensus approach.[151]

To conclude, the WTO should be the forum where nations develop global rules for cross-border data flows that facilitate international trade and provide basic standards in relation to personal data privacy and data security. The issues of data localization and cross-border restriction requirements (which are a part of most cybersecurity and privacy strategies)[152] is one that should be discussed within this setting. It should be

[139] Abendin and Duan, *supra* note 122 at 5.

[140] *WPE, supra* note 23.

[141] *Ibid.*

[142] Bernard HOEKMAN, Xinquan TU, and Dong WANG, eds., *Rebooting Multilateral Trade Cooperation: Perspectives from China and Europe* (London: CEPR Press, 2021), online: CEPR https://cepr.org/chapters/introduction-rebooting-multilateral-trade-cooperation, at 11.

[143] Hamid MAMDOUH, "Plurilateral Negotiations and Outcomes in the WTO" *King & Spalding LLP* (16 April 2021), online: Friends of Multilateralism https://fmg-geneva.org/7-plurilateral-negotiations-and-outcomes-in-the-wto/.

[144] Hoekman, Tu, and Wang, *supra* note 142 at 11.

[145] WTO, "Further progress cited in e-commerce negotiations" *WTO* (22 July 2021), online: WTO E-Commerce https://www.wto.org/english/news_e/news21_e/jsec_22jul21_e.htm.

[146] Burri and Cottier, *supra* note 131 at 97; Hoekman, Tu, and Wang, *supra* note 142 at 11.

[147] *Ibid.*

[148] Mamdouh, *supra* note 143.

[149] Hoekman, Tu, and Wang, *supra* note 142 at 36–7.

[150] Institute for International Trade (IIT), University of Adelaide "'Joint Statement Initiatives' and Progress in the WTO System" *IIT* (2021), online: IIT https://iit.adelaide.edu.au/news/list/2021/05/21/joint-statement-initiatives-and-progress-in-the-wto-system.

[151] Hoekman, Tu, and Wang, *supra* note 142 at 12.

[152] Markopoulou, Papakonstantinou, and De Hert, *supra* note 60 at 105347.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

where a consensus between the data sovereignty of nations and the benefit of an open global digital economy is forged. There are some signs that the WTO is facilitating this mission with the JSI on *Trade Related Aspects of Electronic Commerce*. However, progress has been slow. Reflecting a broader malaise within the WTO, which has not seen new agreements since the halcyon days of its formation, it is doubtful whether the JSI process will provide the needed framework in a timely manner. Furthermore, the digitalization of national economies and the global economy continue apace. Data and data flows across national borders is becoming more significant to the lives and wellbeing of all humans on the planet. Within this context, nations are using other international arrangements to address some of the challenges from digitalization. In particular, provisions on cross-border data flows are becoming a feature of PTAs. These negotiations show a desire to eliminate barriers to data flows and reduce the risk of digital fragmentation, but at the same time, there is a distinct weakness in that there is a reluctance to enforce these arrangements. Despite this, the provisions from PTAs may be critical to provide something of a path forward for progress within the multilateral trading system.[153]

III. A preferential trade approach to data free flows

PTAs provide an alternative platform to negotiate on challenges left unaddressed by the multilateral system.[154] In particular, PTAs are becoming the preferred instrument that some nations are using to provide standards and regulation of cross-border data flows.[155] This section highlights some of the key developments in newly negotiated PTAs and, in doing so, recognizes the weaknesses within these agreements. In this section, this paper demonstrates that PTAs could lead to cooperation on matters related to data security, cross-border data transfer, and privacy. Alternatively, it may further assure a fragmented future.

PTAs exist outside of the complexities of the WTO and represent a smaller grouping of nations agreeing to shared rules and processes relating to intra-group trade. PTAs are considered to be an alternative to pursuing agreements through the WTO process, with some members suggesting this is preferred to the JSI process.[156] Many countries have used PTA negotiation processes to agree on matters that are currently without guidance under the multilateral rules framework.[157] For instance, there are currently over seventy PTAs that incorporate an e-commerce chapter, including the United States - Mexico - Canada Agreement (USMCA, previously the North American Free Trade Agreement); the Comprehensive Trans-Pacific Partnership (CPTPP);[158] and the dedicated digital trade agreements, the Digital Economy Partnership Agreement (DEPA) and the Digital Economy Agreement (DEA).[159] Interestingly, not all agreements have included cross-border data flow commitments. The Japan-EU Economic Partnership Agreement shelved the matter for three years post-entry into force of the agreement,[160] based on

[153] Petros MAVROIDIS and André SAPIR, *China and the WTO: Why Multilateralism Still Matters* (Princeton: Princeton University Press 2021) at 175.

[154] Deborah ELMS, "Getting RCEP across the Line" (2021) 20(3) World Trade Review 373 at 380; Leon TRAKMAN, "The Proliferation of Free Trade Agreements: Bane or Beauty?" (2008) 42(2) Journal of World Trade 367.

[155] Mitchell and Hepburn, *supra* note 22 at 406 and 409.

[156] *The Legal Status of 'Joint Statement Initiatives' and Their Negotiated Outcomes*, Communication from India and South Africa, Communication No. 21-1421, WTO Doc. WT/GC/W/8 (19 February 2021) [*Legal Status of JSIs*] at 3.

[157] Mavroidis and Sapir, *supra* note 153.

[158] Joshua MELTZER, "Governing Digital Trade" (2019) 18(S1) World Trade Review S23 at S43.

[159] Marta SOPRANA, "The Digital Economy Partnership Agreement (DEPA): Assessing the Significance of the New Trade Agreement on the Block" (2021) XIII Trade, Law and Development 143 at 148–9. The DEPA was signed by Chile, New Zealand, and Singapore, and the DEA was an agreement between Australia and Singapore.

[160] *Ibid.*

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

the premise that parties will consider domestic legislative strategies on data flow and data security.[161]

In contrast to this, the Comprehensive and Progressive Treatment for Trans-Pacific Partnership (CPTPP)[162] and the Regional Comprehensive Economic Partnership (RCEP) both include specific e-commerce chapters.[163] Both agreements include sections that deal with cross-border data flow and localization with what appears to be, at first glance, a (somewhat) liberalized approach to data. The CPTPP Agreement was signed by eleven countries: Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, Peru, New Zealand, Singapore, and Vietnam, with the Australian government considering it a breakthrough in the promotion of the free flow of data across international borders for business activities.[164] Although the CPTPP suspended some provisions from the original Trans-Pacific Partnership text, Chapter 14, which focuses on "electronic commerce", was adopted in its entirety.[165]

Two provisions outlined within Article 14 have particular significance in indicating support for a liberalized approach to cross-border data flow and preventing digital fragmentation.[166] The first prescribes an obligation on all signatories to allow cross-border data flows, including personal data, for the purpose of business transactions or operation.[167] The second restricts a nation from applying localization requirements within its borders as a condition for conducting business or operating within that nation.[168] Both of these provisions are subject to exceptions, which are contained within Articles 14.11(3) and 14.13(3). These exceptions provide that any national measure inconsistent with its obligations must not be arbitrary, unjustifiable, or a disguised restriction on trade.[169] The exemptions make it essential that any national law or regulation does not restrict the transfer of cross-border data flow or impose localization requirements beyond what is required to achieve the permitted objective.[170] Hence, the CPTPP does not leave the exemptions to the fiat of individual nations. Rather, exception claims can be referred to the dispute resolution system outlined in the text.[171]

The purpose of Chapter 14 is to encourage open cross-border trade and limit exercises of data sovereignty to agreed zones of legitimate national interest. Furthermore, it provides for a dispute resolution mechanism to scrutinize and ensure that national measures that affect cross-border data flows remain within the agreed exemptions. This is a substantial improvement over the WTO in that issues relating to data flows,[172] personal data privacy,[173] minimal standards for cooperation on electronic

[161] Abendin and Duan, *supra* note 122 at 15.

[162] *Comprehensive and Progressive Trans-Pacific Partnership*, 8 March 2018, [2018] Australian Treaty Series (A.T.S.) 23 (entered into force 30 December 2018).

[163] *Regional Comprehensive Economic Partnership*, 15 November 2020, [2022] A.T.S. 1 (entered into force 1 January 2022) [*RCEP*].

[164] Australian Government, DFAT, "CPTPP Outcomes: Trade in the Digital Age" *DFAT* (2019), online: DFAT https://www.dfat.gov.au/trade/agreements/in-force/cptpp/outcomes-documents/Pages/cptpp-digital.

[165] *Trans-Pacific Partnership*, 4 February 2016 (treaty has not entered into force) [*TPP*], Chapter 14, online: DFAT https://www.dfat.gov.au/sites/default/files/14-electronic-commerce.pdf.

[166] *Ibid.*, arts. 14.11(3) and 14.13(3).

[167] *Ibid.*, art. 14.11(2).

[168] *Ibid.*, art. 14.13(2); Burri and Cottier, *supra* note 131 at 85.

[169] *TPP*, *supra* note 165, arts. 14.11(3) and 14.13(3); Yoshinori ABE, "Data Localization Measures and International Economic Law: How Do WTO and TPP/CPTPP Disciplines Apply to These Measures?" (2021) Public Policy Review 1 at 22.

[170] *TPP, supra* note 165, art. 14.11(3)(b) does not impose restrictions on transfers of information greater than are required to achieve the objective. See also Abe; supra note 169 at 22.

[171] *TPP*, *supra* note 165, art. 14.18.

[172] *Ibid.*, art. 14.11.

[173] *Ibid.*, art. 14.8.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

commerce,[174] online consumer protection,[175] cybersecurity cooperation,[176] and prohibiting localization requirements[177] are addressed. Furthermore, the dispute resolution process allows scrutiny of national data restrictions to determine whether those restrictions are supported by the agreed exemption for a "legitimate public policy objective".[178] These provisions in the CPTPP show promise for future multilateral agreements that facilitate DFFT, albeit with the shadow of a broad "legitimate public policy objective" exemption jeopardizing the provisions' enforceability. Indeed, the wording and form of the CPTPP provisions have been largely replicated in other agreements, specifically the DEPA and DEA.[179] This could be seen as a convergence of nations agreeing to the form of DFFT articulated within the CPTPP. However, there is an exception to this convergence.

Parallel to the ratification of the CPTPP, RECEP negotiations, which included China as a party, have been ongoing.[180] In 2020, the RCEP agreement was signed by all parties and entered into force 1 January 2022.[181] The agreement has fifteen signatories: Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, Vietnam, Australia, China, Japan, New Zealand, and South Korea, with India withdrawing from negotiations in the final stages.[182] Clearly, there is overlap between the parties to the RCEP agreement and the CPTPP, with Singapore, Vietnam, Malaysia, Japan, Australia, and New Zealand participating in both. This overlap in parties could in part explain the similarities evident in the two PTAs.[183] However, disparities that some commentators attribute to China's presence in the RCEP remain between the agreements.[184]

The RCEP agreement is one of the largest PTAs and includes multilateral rules that aim to liberalize cross-border data flow and set requirements for privacy and consumer protection regulations for member nations. In this regard, the RCEP echoes similar provisions to the CPTPP. For example, Chapter 12 prevents parties from restricting the cross-border transfer of information and prohibiting data localization conditions.[185] However, some commentators have noted that the substantive provisions of the RCEP's "electronic commerce", Chapter 12, has been pared back from what the nations agreed to in the CPTPP.[186] For instance, a footnote to Provision 12.14.3(a), which is the "legitimate public policy objective" exception, states:

[174] *Ibid*., art. 14.15.
[175] *Ibid*., art. 14.7.
[176] *Ibid*., art. 14.16.
[177] *Ibid*., art. 14.13.
[178] *Ibid*., art. 14.11(3).
[179] Soprana, *supra* note 159 at 157.
[180] Elms, *supra* note 154.
[181] Australian Government, DFAT, "Regional Comprehensive Economic Partnership (RCEP)" *DFAT*, online: DFAT https://www.dfat.gov.au/trade/agreements/in-force/rcep.
[182] Elms, *supra* note 154 at 374; Chao WANG and Vinay SHARMA, "India's RCEP Dilemma with China: Beyond the Legal Texts" (2021) 36(1) Pacific Focus 40.
[183] Chien-Huei WU, "ASEAN at the Crossroads: Trap and Track between CPTPP and RCEP" (2020) 23(1) Journal of International Economic Law 97. See also the differences identified in Collins AJIBO et al., "RCEP, CPTPP and the Changing Dynamics in International Trade Standard-Setting" (2019) 16(3) Manchester Journal of International Economic Law 425 at 432.
[184] Ajibo et al., *supra* note 183 at 432.
[185] *RCEP*, *supra* note 163, arts. 12.14(1) and 12.15(1).
[186] Matthew RIMMER, "A Submission to the Joint Standing Committee on Treaties on the Regional Comprehensive Economic Partnership (RCEP)", Joint Standing Committee on Treaties, Parliament of Australia, Parliament Submission, 16 April 2021 at 49; Patrick LEBLOND, "Digital Trade: Is RCEP the WTO's Future?" *Centre for International Governance Innovation* (23 November 2020), online: CIGI https://www.cigionline.org/articles/digital-trade-rcep-wtos-future/.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

> "[f]or the purposes of this subparagraph, the Parties affirm that the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party." This footnote has the effect of allowing any party to determine when the exception should apply, thus excusing data localization requirements whenever desired.[187] Hence, parties may operate outside the provisions if they choose to.

Chapter 12 of the RCEP also includes provisions to cooperate with other signatories on matters of cybersecurity in the interests of capacity building.[188] The Australian government has identified the importance of these provisions in terms of future trade and data flows. Notably, suggesting that:

> By including commitments to support the flow of data, promote privacy and consumer protection and enable electronic authentication and electronic signature, [the] RCEP will help to facilitate digital trade in the region and support consumer confidence in the online environment.[189]

Despite the positive comments of the Australian Government, there are some limitations to these conditions. First, as noted, the agreement differs from the CPTPP by incorporating additional exception provisions. In addition to the "legitimate public policy objective" exception and the environmental exceptions of the GATS and the GATT,[190] the RCEP follows the WTO in acknowledging the importance of national security through its "essential security interests" exception.[191] This was an interesting inclusion, particularly in light of the so-called "abuse" of the national security exception in WTO disputes since 2016.[192]

The second point of limitation in Chapter 12 is the specific exclusion of dispute mechanisms, unlike the CPTPP. In particular, under Article 12.14 members are not able to dispute the location of computing facilities when such actions have been taken for essential security interests.[193] The position on security interests is the same with respect to the cross-border transfer of information by electronic means.[194] However, at this stage, the exemption from dispute settlement is unnecessary as Article 12.17 precludes all of Chapter 12 from the dispute settlement mechanism contained in Chapter 19.[195] Paragraph 3 of this Article states:

> No Party shall have recourse to dispute settlement under Chapter 19 (Dispute Settlement) for any matter arising under this Chapter. As part of any general review of this Agreement undertaken in accordance with Article 20.8 (General Review), the Parties shall review the application of Chapter 19 (Dispute Settlement) to this

[187] Leblond, *supra* note 186.

[188] Australian Government, "Regional Comprehensive Economic Partnership – Outcomes: Electronic Commerce" *Australian Government* (15 November 2020), online: DFAT RCEP https://www.dfat.gov.au/sites/default/files/rcep-outcomes-ecommerce.pdf.

[189] *Ibid.*

[190] *General Agreement on Tariffs and Trade*, 30 October 1947, 58 U.N.T.S. 187 (entered into force 1 January 1948), art. XX; *GATS, supra* note 115, art. XIV.

[191] *GATS, supra* note 115, arts. 12.14(2) and 12.15(2).

[192] Peter VAN DEN BOSSCHE and Sarah AKPOFURE, "The Use and Abuse of the National Security Exception under Article XXI(b)(iii) of the GATT 1994", Universität Bern, WTI Working Paper No 03/2020, September 2019.

[193] *Ibid.*; *GATS, supra* note 115, art. 12.14(3).

[194] *RCEP, supra* note 163, chapter 12, art. 12.15.

[195] *Ibid.*, chapter 12, art. 12.17.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

> Chapter. Following the completion of the review, Chapter 19 (Dispute Settlement) shall apply to this Chapter between those Parties that have agreed to its application.[196]

The exclusion from dispute settlement is significant. This exclusion indicates that although parties agree to the requirements for cross-border data flow, privacy, and localization requirements, they are not willing to be held to account by other parties. In this, RCEP goes against the general trend, noted by Froese, of increased enforceability of e-commerce chapters.[197] In this regard, Chapter 12 of the agreement is seemingly unique. Without recourse to a dispute mechanism, the substantive commitments in Chapter 12, to open cross-border data flows, can only be read as aspirational. Given the data sovereignty objectives of recent Chinese laws, it could be suggested that this provision was a condition of China's participation.[198] Whatever the reasoning of the parties to exempt Chapter 12 from the dispute resolution procedures, the effect is that they will have to rely on good faith that measures will not be enacted which interfere with cross-border data flows. Extensive national regulation of data, such as seen within the Chinese laws, possibly goes beyond the boundaries of the "legitimate public policy objective" or the "essential national security" exemptions of the RCEP. However, as these exemptions, coupled with the exemption from the dispute resolution processes, allow for the parties to determine the boundaries themselves,[199] whether any other party exceeds those boundaries is irrelevant.

The RCEP negotiations provide some insight into what nations are willing to agree to in principle. This agreement does demonstrate that nations regard e-commerce and data flows as important. However, at the same time, the inability to enforce the provisions leaves open questions in terms of the commitment to genuine cooperation on DFFT. The discretion afforded indicates that parties could still be on a trajectory of fragmentation.[200] Although the CPTPP set a standard of liberalization in terms of localization requirements,[201] it is also apparent that this is a standard that may only be acceptable to some nations in principle rather than practice. PTAs are indicative of progress towards DFFT, but the requirement to avoid localization is not the same as finding common ground and cooperation. As such, more is needed to avoid fragmentation in the global economy.

IV. Global data framework for a digital future

It has been identified that the interdependence created by digital globalization has resulted in a "transformation of global politics", which means privacy, cross-border data flows, and data security are matters that unquestionably extend beyond national borders.[202] As noted above, restrictions on cross-border data flows result in costs to industry and to national economies.[203] These restrictions may have other negative flow-on

[196] *Ibid*.

[197] Marc FROESE, "Digital Trade and Dispute Settlement in RTAs: An Evolving Standard?" (2019) 53(5) Journal of World Trade 783 at 804.

[198] Wang and Sharma, *supra* note 182 at 44; Henry GAO and Gregory SHAFFER, "The RCEP: Great Power Competition and Cooperation over Trade", Irvine School of Law, University of California, Research Paper No 2021-09, 1 February 2021 (which discusses China's role in making trade rules). Note, Chapter 12 was one of the last agreed upon by signatories.

[199] See also footnote to *RCEP*, *supra* note 163, art. 12.14(3)(a); Leblond, *supra* note 186.

[200] Soprana, *supra* note 159 at 156.

[201] Abendin and Duan, *supra* note 122 at 18.

[202] *Ibid*., at 13.

[203] WEF, *supra* note 28 at 9.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

consequences, such as weakening cybersecurity, infringing key WTO provisions, and (will likely lead to) trade tensions and discontent in the private sector. Further, the costs will be disproportionately imposed on small businesses with limited resources to understand "divergent national regulatory regimes".[204] Hence, the positive impact of digitalization on developing economies is thwarted by the imposition of restrictions on cross-border data flows.[205] For this reason, the costs of regulatory restrictions on cross-border data flows are considered externalities which, ultimately, "pose a threat to global supply chains".[206] The issues remain, however, as to what can be done on a global level and whether multilateral agreements will achieve anything in practice. The purpose of this part of the article is to address these issues.

Farrell and Newman contend that "power rarely resides in brute coercion, but rather in the political opportunities generated by interaction".[207] In this respect, the WTO as a forum could be part of the solution to aid cooperation and support the free flow of data. The EU, China, Japan, and the United States have each been a part of the WTO JSI negotiations on e-commerce.[208] Abendin and Duan argue that in order to conclude an agreement within the WTO framework, the positions of these four members will need to be reconciled,[209] although the umbrella term "e-commerce" is unlikely to capture the many evolving issues from the digitalization of international trade.[210]

Reconciliation of the many interests that exist in each of these four members presents a significant challenge, particularly in countries susceptible to influence from the private sector. There is some promise: the JSI discussions have touched on difficult topics such as a prohibition of unjustified localization requirements, [211] however, the discussions have not yet led to the necessary reconciliation of strategic positions of key members.[212] Further, other WTO members have refused to accept the legitimacy of these negotiations.[213]

The essentiality of data and data flows for the global economy and human well-being means that DFFT is essential to address digital fragmentation. Agreed rules between nations will be integral in achieving cooperation. Increased national restrictions on cross-border data flows, the difficulties with the WTO, and the e-commerce chapters in the CPTPP and the RCEP identify three main *foci* that need to be considered in a DFFT framework: individual data rights, including privacy protections in relation to personal data; support for cybersecurity and data security in Global South nations; and international cooperation to support intelligence sharing and flexible outcomes. Each may seem simple enough, yet all three present their own unique challenges in a multilateral setting.

The right to privacy is considered a fundamental human right in accordance with the International Covenant on Civil and Political Rights[214] and within the European Charter of

[204] Ahmed, *supra* note 13 at S105.

[205] WEF, *supra* note 28 at 8.

[206] Komaitis, *supra* note 43 at 361.

[207] Henry FARRELL and Abraham NEWMAN, *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security* (Princeton: Princeton University Press, 2019) at 3.

[208] European Parliament, "WTO E-Commerce Negotiations" *European Parliament* (2021), online: At A Glance https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/659263/EPRS_ATA(2020)659263_EN.pdf.

[209] Abendin and Duan, *supra* note 122 at 2.

[210] Ahmed, *supra* note 13 at S102.

[211] *E-Commerce Joint Statement*, *supra* note 121.

[212] Abendin and Duan, *supra* note 122 at 7.

[213] *Legal Status of JSIs, supra* note 156.

[214] *International Covenant on Civil and Political Rights*, 19 December 1966, 999 U.N.T.S. 171, 6 I.L.M. 368 (entered into force 23 March 1976), art. 17.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

Fundamental Rights.[215] Despite this, at present, the right to privacy is not universal, which creates fragmentation. To avoid fragmentation, it is critical that measures to protect privacy (and other data rights) exist globally, but, at the same time, they are not disguised restrictions on international trade. Hence, it will be necessary to consider measures that are reasonable and necessary for the protection of individual privacy. It would be reasonable for nations to agree on minimum regulatory protections, much like those imposed by the TRIPS agreement.[216] Indeed, the development of TRIPS demonstrates that conceptualizing behind-the-border rules for harmonization purposes at a multilateral level can be achieved; however, the inclusion of minimum regulatory requirements within the WTO agreements has traditionally been difficult due to the additional costs and the complexity that these provisions require.[217] Much like the minimum provisions under TRIPS, many nations have already enacted privacy laws. However, "some developing countries suffer from a distinct lack of national laws regulating, for instance, online consumer protection, electronic transactions, data protection, and cybercrime".[218] Although the GATS framework does support privacy through the exception provisions, this is a matter entirely different to a minimum requirement for personal data privacy. An exception provision does little more than allow for privacy, whereas a "beyond-the-border" provision (such as imposed by the GDPR) will do far more to foster trust and consumer confidence. Therefore, the discussion on privacy should encompass standards and a definition of personal data that can be universally accepted. Alternatively, recognition of different members' standards could be a pathway forward for resolving these issues.

A meaningful starting point may be a common definition of "personal information" or "personal data". In the GDPR and the PIPL, these are largely aligned to include only data that is related to "natural persons".[219] Indeed, a decision on the type of data to be protected by regulatory frameworks to support the recognition of the human right privacy is a logical first step and one that *should* be easily negotiated at a multilateral level. It is when ambitions move beyond these seemingly simple outcomes that minimum requirements may become troublesome. The use of encryption as a means to provide data protection provides an example of this. "Data encryption is a process or technique of translating data from text to hashed code that can only be decrypted with a special key."[220] Under the GDPR, encryption is referenced many times and identified as a best practice approach. Far from being a mandate, the GDPR repeatedly mentions encryption as an appropriate measure for data security.[221] The GDPR directive can be contrasted to the Chinese approach where data encryption is now supported, but only with the caveat that Chinese government entities must have access to the encryption key.[222] In this respect, the competing values of these major trading nations will impose potentially

[215] Jörn REINHARDT, "Realizing the Fundamental Right to Data Protection in a Digitized Society" in Marion ALBERS and Ingo Wolfgang SARLET, eds., *Personality and Data Protection Rights on the Internet: Brazilian and German Approaches* (Cham: Springer International Publishing 2022), 55 at 56.

[216] For instance, under Article 33 of the *TRIPS*, *supra* note 129, there is a minimum of twenty years of protection.

[217] Van Den Bossche and Zdouc, *supra* note 20 at 741.

[218] Isabelle Durant, "Developing Countries and Trade Negotiations on E-Commerce" *UNCTAD* (19 February 2021), online: UNCTAD https://unctad.org/news/developing-countries-and-trade-negotiations-e-commerce; UNCTAD, *What Is at Stake for Developing Countries in Trade Negotiations on E-Commerce?: The Case of the Joint Statement Initiative* (2021), online: UNCTAD https://www.un-ilibrary.org/content/books/9789210056366.

[219] *GDPR*, supra note 58, art. 4(11); *PIPL, supra* note 110.

[220] Narendra Sahoo, "Role of Encryption in GDPR Compliance" *Tripwire* (31 March 2021), online: Fortra https://www.tripwire.com/state-of-security/security-data-protection/role-of-encryption-in-gdpr-compliance/.

[221] *Ibid*.

[222] Laskai and Adam, *supra* note 95.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

challenging barriers to any agreement in the short term. As an alternative, mutual recognition poses an alternative to harmonization, which may prove successful.[223] Mutual recognition would mean that no harmonization of definitions or processes is necessary but, at the same time, it would require members to agree to support differences in other domestic jurisdictions. However, mutual recognition of privacy standards may prove equally difficult to agree upon. The benefit would be that the mutual recognition pathway may allow members to maintain a degree of flexibility to ensure that specific regulatory priorities could be pursued.[224]

A second critical element is that governments in developed economies need to provide knowledge and financial support to the Global South. DFFT requires emphasis on supporting data and cybersecurity in Global South nations for two reasons.[225] First, the development of emerging economies is in the global interest as well as a matter of distributive justice. There is no fairness in enforcing the same measures in all nations unless support is provided to nations that need it most. Second, in matters of global privacy, cybersecurity, and consumer protection, any system weakness will result in unintended and negative outcomes, creating a global weakness that would not otherwise exist.[226] The Budapest Convention provides evidence of this, in particular, its provisions that support harmonization of laws addressing cybercrimes.[227] Hence, more minimum standards on cybercrimes may not be necessary – what is needed is a global data framework to provide for capacity building for Global South nations as a priority.[228] Capacity building should focus on data security measures and privacy requirements to ensure that Global South nations are not disadvantaged by any new developing minimum standards. Capacity building within the Global South will be critical to support "varying levels of e-commerce readiness".[229]

The role of the WTO needs to be recognized. There is no global institution that has a "mandate to evaluate and track policy intervention in the digital domain".[230] Some scholars suggest that this may be a time when an institutionalized approach is unwarranted. "Regulatory sandboxes" rather than "binding agreements" could be a pathway forward in the data driven economy.[231] However, accepting that argument means that the pursuit of DFFT through cooperation should effectively be abandoned. It is critical that this does not happen. It is unfortunate that the pathway forward through the multilateral trade regime is far from clear for participating nations. Indeed, despite progress through the JSI, member resistance means that the outcomes of negotiations are uncertain and are at risk of

[223] Ahmed, *supra* note 13 at S114.

[224] Gregory SHAFFER, "Trade Law in a Data-Driven Economy: The Need for Modesty and Resilience" (2021) 20 World Trade Review 259 at 275.

[225] David COLLINS, Joo-Hyoung LEE, and Tae JUNG PARK, "A Soft Landing for Developing Countries and Non-Discrimination in Digital Trade: Possible Lessons from Asian Countries" (2021) 55(4) Journal of World Trade 649.

[226] Joanna ŚWIĄTKOWSKA, "Tackling Cybercrime to Unleash Developing Countries' Digital Potential", The European Cybersecurity Forum - CYBERSEC and AGH University of Science and Technology, Background Paper 33, January 2020 at 49.

[227] Jonathan CLOUGH, "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization" (2014) 40(3) Monash University Law Review 698 at 736.

[228] *China's Proposal on WTO Reform,* Communication from China, Communication No. 19-3287, WTO Doc. WT/GC/W/773 (13 May 2019), at para. 3.11.

[229] UNCTAD, *supra* note 218 at 45.

[230] Evenett and Fritz, *supra* note 6 at 145.

[231] Dan CIURIAK, "The Economics of Data: Implications for the Data-Driven Economy" (4 February 2018) Social Science Research Network, online: SSRN https://papers.ssrn.com/abstract=3118022 at 7.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

being nothing more than a talkfest. Nevertheless, these challenges do not present insurmountable barriers to the ongoing ability for the WTO[232] to work against fragmentation through the rules-based order and the negotiation platform it supports.[233]

Although new and existing PTAs have foreshadowed a promising trend,[234] the differences between the agreements could potentially exacerbate fragmentation rather than address it. In this respect, each PTA will be signed by a handful of nations compared to the 164 members of the WTO. This means that fragmentation will not be overcome with each PTA. As such, the objective of DFFT must remain on the negotiating agenda of the WTO in order to avoid "a silo-oriented data-driven economy".[235] The precise nature of the terms of negotiation may be difficult to predict. However, the objective of trade for the benefit of all should remain central and global cooperation should continue to be pursued. Where sovereignty is prioritized over the global good, nations engage in economic statecraft, which will only exacerbate digital fragmentation and the North/South digital divide.[236]

The final and critical point is that there needs to be acceptance by the private sector to avoid fragmentation.[237] Presently, localization trends have been set by governments through legal requirements and corporate demands. Hence, the connection between government policy and industry needs should be strengthened, but with a view to consider global markets (over time), not just local and present concerns. In this regard, trust will be critical for private entities to have confidence in data security and protection beyond their own borders. The analysis in this paper does not provide a pathway to trust between entities, nations, or regions; rather, minimum requirements for cooperation have been identified. Trust is a higher standard that will require seismic shifts and perseverance. However, in a world where national interests have always trumped global ones, trust may be nothing more than an unattainable aspiration.

V. Conclusion

Data localization rules and barriers to cross-border data flows are inefficient, leading to slow movement of capital and lost profits for private entities.[238] Alternatively, a secure digital environment improves efficiency through consumer confidence and by supporting a safe online environment. In the age of digital trade, there is a need for nations to cooperate so the global community can benefit. At the same time, individual nation priorities in terms of data security remain essential for an effective digital society. This presents its own issues. As Farrell and Newman posit, one of the most significant concerns with a globalized society is the problem of rule overlap.[239] That is, "different regulatory systems come to interfere with and influence each other".[240] The extension of rules beyond borders (such as is done by the GDPR and China's PIPL) means that this is even more problematic. However, given the nature of digital transfers, extraterritorial rules in these matters are necessary. An agreement between WTO members, providing for a global data framework, may help minimize costs and allow trading partners from different jurisdictions to participate in open cross-border transactions. However, the differences

[232] Mavroidis and Sapir, *supra* note 153.
[233] Mavroidis and Sapir, *supra* note 153 at 175.
[234] Brad KLOEWER, "The Spaghetti Bowl of Preferential Trade Agreements and the Declining Relevance of the WTO" (2016) 44(3) Denver Journal of International Law and Policy 429 at 435.
[235] Evenett and Fritz, *supra* note 6 at 17.
[236] Aggarwal and Reddie, *supra* note 41 at 137; Lacerda Prazeres, *supra* note 101.
[237] WEF, *supra* note 28.
[238] Cory and Dascoli, *supra* note 54.
[239] Farrell and Newman, *supra* note 207 at 27.
[240] *Ibid*.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

in national approaches, both to privacy and data security, underscore the need for flexible co-operation and agreement.[241] Unfortunately, it is possible that an agreement at a multilateral level may result in "watered down" standards (such as those contained in the RCEP) as a result of individual national interests overriding any desire to maintain the integrity of the multilateral trading regime.

If negotiations are pursued fairly and the provisions are subsequently successful, PTAs could be a metaphorical sandpit for the data flow provisions that may later be agreed at a multilateral level. PTAs present a simpler negotiation environment by avoiding the complexity of the 164 different party interests and the diversity that results from the inclusion of the interests of Global South nations (although in the opinions of the authors, this is a necessary complication). However, a PTA can still take many years of dedicated negotiations, with the RCEP being only recently signed after eight years, twenty-one ministerial meetings, and thirty-one negotiation rounds.[242] Thus, PTAs are not able to provide a quick resolution for difficult global issues and may not lead to the widespread benefits that larger multilateral agreements can potentially achieve. Further, the RCEP "carve out" of the e-commerce chapter from dispute settlement indicates that these agreements are not without their weaknesses.

Finally, the importance of DFFT should be underscored. For individuals, privacy is (often) a fundamental human right and a universal concern in the digital age.[243] The objective to protect individual privacy has led many nations, including the EU and China, to establish strict approaches to data protection. At the same time, these strict approaches could create a large divide between nations at different levels of economic development and technical capacities. Further, there is a fear that the introduction of privacy protections may provide a disguised form of trade restrictions or, alternatively, increase the power of central governments to access data of citizens and those that they have commerce with. The intensification of digital trade and the increasing dependence of humans flourishing on digital technologies presents these issues as fundamental challenges for people, businesses, and governments in the twenty-first century. Presently, the path to a global data framework might not be obvious or easy, but it is increasingly essential for a fair digital economic future.

Acknowledgements. The authors would like to thank the reviewers for their comments.

Funding statement. None.

Competing interests. The authors declare none.

Felicity DEANE is an Associate Professor at the School of Law at Queensland University of Technology, Brisbane, Australia.

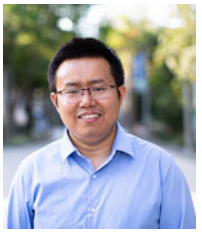
[241] Neeraj, *supra* note 121 at S123; Shaffer, *supra* note 224 at 271, argues that maintaining policy space is essential for governments to ensure the regulations can be introduced that are needed to regulate the oligopolistic behaviour of tech giants.

[242] New Zealand Foreign Affairs & Trade (NZFAT), "Timeline and History of the RCEP Negotiations" NZFAT, online: NZFAT https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/regional-comprehensive-economic-partnership-rcep/next-steps-and-timeline/.

[243] Diggelmann and Cleis, *supra* note 38; OAIC, *supra* note 38.

https://doi.org/10.1017/S204425132300036X Published online by Cambridge University Press

Emily WOOLMER is a graduate of the School of Law at Queensland University of Technology, Brisbane, Australia.



Shoufeng CAO is an ARC Research Fellow at the School of Agriculture and Food Sustainability at the University of Queensland, Brisbane, Australia.

Kieran TRANTER is a Professor (Chair of Law, Technology and Future) at the School of Law at Queensland University of Technology, Brisbane, Australia.

Cite this article: DEANE F, WOOLMER E, CAO S, TRANTER K (2024). Trade in the Digital Age: Agreements to Mitigate Fragmentation. *Asian Journal of International Law* **14**, 154–179. https://doi.org/10.1017/S204425132300036X