4

WTO Law and Cross-Border Data Flows

An Unfinished Agenda

*Andrew D. Mitchell and Neha Mishra**

A INTRODUCTION

The tension between protecting free data flows and protecting goals such as privacy and cybersecurity is vexing Internet and trade policymakers. Laws and regulations hindering data flows across borders ('data restrictive measures' or 'data restrictions') are often trade restrictive,[1] and some of these measures can violate World Trade Organization (WTO) and Preferential Trade Agreements (PTAs) obligations.[2] However, countries can justify these measures under exceptions in international trade agreements that allow governments to implement measures necessary to achieve their domestic policy objectives,[3] arguably including policies for the stability and security of the domestic Internet.[4] Nonetheless, the inherent contradiction

* Andrew Mitchell is Professor of Law at Monash University. Contact: andrew.mitchell@monash.edu. Neha Mishra is Lecturer at the Australian National University College of Law. Contact: Neha.Mishra@anu.edu.au.

1 W. Reinsch, 'A Data Localization Free-for-All?', *Centre for Strategic and International Studies Blog*, 9 March 2018, available at www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all; N. Cory, 'Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?', *Information Technology and Innovation Foundation*, May 2017, available at www2.itif.org/2017-cross-border-data-flows.pdf.

2 This article refers to both direct data restrictive measures, such as data localisation laws or explicit data storage requirements, and indirect restrictions, such as conditional restrictions on data transfer based on ensuring security or privacy.

3 See, e.g., General Agreement on Trade in Services, 1869 U.N.T.S. 183; 33 I.L.M. 1167 (1994), entered into force 1 January 1995 [hereinafter: GATS], at Preamble, para. 4; Article XIV; Article XIV*bis*.

4 See generally S. Wunsch-Vincent, 'The Internet, Cross-Border Trade in Services, and the GATS: Lessons from US – Gambling', *World Trade Review* 5 (2006), 319–335; H. V. Singh, A. Abdel-Latif, and L. Tuthill, 'Governance of the International Trade and the Internet: Existing and Evolving Regulatory Systems', Global Commission on Internet Governance Paper No 32 (2016); T. Wu, 'The World Trade Law of Censorship and Internet Filtering', *Chicago Journal of International Law* 7 (2006), 263–287.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

between the globality of the Internet and the (often) inward-looking data restrictive measures creates uncertainties for data-driven sectors.[5]

Modern-day digital services, such as cloud computing services, play an important role in facilitating businesses across the global supply chain, particularly by enabling them to expeditiously and efficiently move data across countries.[6] Some experts have even argued that data should be included as a 'fifth item to the traditional list of issues addressed by trade policy: movement of goods, persons, services, capital, and data'.[7] Yet, a contradictory narrative exists, emphasising the importance of legal checks on cross-border data flows, especially the regulatory advantages of data territoriality, to inter alia ensure privacy, security and ethical use of data.[8]

This article adopts a holistic perspective on the relevance of international trade law to data flows by (i) exploring the different regulatory issues pertaining to data flows that directly relate to international trade law; and (ii) recommending a framework in WTO law incorporating legal obligations on cross-border data flows alongside other relevant disciplines that enhance trust in the Internet ecosystem. Many contemporary electronic commerce issues are covered in recent PTAs; however, these PTAs often take different approaches, for example, on issues of cross-border data flows and data protection.[9] In the long run, such varied approaches may lead to fragmented rules on trade in digital services.[10] In contrast, the WTO being the only multilateral trade institution in the world, with a membership of 164 countries, is better suited to develop coherent, balanced and representative rules for a data-driven economy, as discussed further in this article. Moreover, electronic commerce–related issues are now more prominent at the WTO, including under the joint statement initiative, providing a timely opportunity to WTO members to develop new and relevant rules on data flows.[11]

[5] C. Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford: Oxford University Press, 2013), at 159.

[6] J. Manyika et al., *Digital Globalization: The New Era of Digital Flows* (Washington, DC: McKinsey Global Institute, 2016); United Nations, 'Big Data for Sustainable Development', 9 December 2019, available at www.un.org/en/sections/issues-depth/big-data-sustainable-development/index.html.

[7] D. Ciuariak and M. Ptaskhina, *The Digital Transformation and the Transformation of International Trade* (Geneva/NewYork: ICTSD/IDB, 2018), at vi.

[8] A. Clement, 'Canadian Network Sovereignty: A Strategy for Twenty-First-Century National Infrastructure Building', in CIGI (ed), *Special Report: Data Governance in the Digital Age* (Waterloo: CIGI, 2018), at 26–33, at 31. See also R. H. Weber and E. Studer, 'Cybersecurity in the Internet of Things: Legal Aspects', *Computer Law and Security Report* 32 (2016), 715–728.

[9] See A. D. Mitchell and N. Mishra, 'Data at the Docks: Modernizing International Trade Law for the Digital Economy', *Vanderbilt Journal of Entertainment and Technology Law* 20 (2018), 1073–1134, at 1086–1087. See also Chapter 1 in this volume.

[10] See, e.g., M. Burri, 'The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation', *University of California Davis Law Review* 51 (2017), 65–132, at 99–110.

[11] See WTO, Joint Statement on Electronic Commerce, WT/L/1056, 25 January 2019; WTO, Joint Statement on Electronic Commerce, WT/MIN(17)/60, 13 December 2017. See also WTO, Declaration on Global Electronic Commerce, WT/MIN(98)/DEC/2, 20 May 1998.

This article explores various elements required within the WTO framework to address the policy ramifications of data restrictive measures, focusing on General Agreement on Trade in Services (GATS). However, we acknowledge that our research query is cross-cutting and other issues might be relevant including the alignment of GATS with General Agreement on Tariffs and Trade 1994 (GATT 1994),[12] Agreement on Technical Barriers to Trade (TBT)[13] and Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).[14] Further, where relevant, we also refer to applicable electronic commerce rules in different PTAs.

The first section explores the multilayered policy framework governing data flows and cross-border data flows identifying various policy goals typically associated with data restrictions. The following section then explains the trade-related aspects of data flow regulation by focusing on two interconnected topics: (i) the special nature of digital trade and trade in data that makes it harder to apply existing GATS provisions to digital services and (ii) those aspects of data flows that are trade related and, thus, should be addressed in a trade law framework. Finally, the last section proposes a novel WTO framework on data flows by identifying the foundational principles for data regulation and the legal provisions necessary to enable security, predictability and certainty in data flows. This section also discusses the feasibility of implementing this proposal at the WTO.

The article concludes that the WTO framework can and should evolve to accommodate the policy challenges of a data-driven economy, including adoption of binding provisions on free cross-border data flows; prohibition on data localisation; and introducing relevant provisions facilitating business and consumer trust in the digital ecosystem such as online consumer protection, privacy and cybersecurity. This framework should also include provisions centred on the specific needs of developing countries, such as providing them with technical assistance and capacity-building support, as well as facilitating digital inclusion and development. We, however, acknowledge various political constraints in adopting our proposal wholesale at the WTO, given the political sensitivity of the issues involved, and the policy preference of various countries to use PTAs to negotiate rules on data flows. Nonetheless, we believe that the existing WTO framework remains better suited and more relevant in achieving greater balance, coherence and consistency in trade rules on data flows, and that sufficient incentives exist for WTO members to meaningfully engage in reforming WTO rules to make them more relevant to the data-driven economy.

[12] General Agreement on Tariffs and Trade 1994, 1867 U.N.T.S. 187; 33 I.L.M. 1153 (1994), entered into force 1 January 1995 [hereinafter: GATT].

[13] Agreement on Technical Barriers to Trade, 1869 U.N.T.S. 299, 33 I.L.M. 1125 (1994), entred into force 1 January 1995 [hereinafter: TBT].

[14] Agreement on Trade-Related Aspects of Intellectual Property Rights, 1869 U.N.T.S. 299; 33 I.L.M. 1197 (1994), entered into force 1 January 1995 [hereinafter: TRIPS].

B REGULATING DATA FLOWS: A MULTILAYERED POLICY FRAMEWORK

Notwithstanding the economic benefits of free data flows, countries restrict data flows to address various policy concerns. This section first discusses the most common rationales for imposing data restrictive measures, such as privacy and cybersecurity protection.[15] It then covers other aspects of data transfer that concern governments, such as illegal and unauthorised data access by foreign countries, trade secrets theft, and consumer risks in electronic transactions. Finally, the section discusses how data restrictive measures can relate to achieving domestic economic development.

I *Privacy and Cross-Border Data Flows*

With increasing digitalisation of services, privacy concerns have become significant.[16] Fifty-eight percent of all countries have now adopted or are in the process of adopting data protection laws.[17] Many of these laws contain provisions affecting cross-border data flows. Perhaps, the most prominent example is the European Union (EU) General Data Protection Regulation (GDPR).[18] The GDPR sets various conditions for cross-border transfer of data; for example, routine data transfers are only allowed to those countries having an equivalent level of data protection as the EU. Further, the GDPR provides for mechanisms, such as Standard Contractual Clauses and Binding Corporate Rules, prescribing additional mechanisms for individual companies to transfer personal data outside the EU,[19] and a right to be forgotten, allowing individuals to demand Internet platforms to delink their data to make it untraceable online.[20] The intended aim of these restrictions is preventing circumvention of EU's data protection laws and increasing individuals'

[15] S. A. Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?', *World Trade Review* 1 (2018), 1–37, at 11.

[16] See, e.g., Centre for International Governance Innovation, *2018 CIGI-Ipsos Global Survey on Internet Security and Trust* (Waterloo: CIGI, 2018); General Assembly of the United Nations, The Right to Privacy in the Digital Age, 71st Session, A/C.3/71/L.39/Rev.1, adopted 21 November 2016.

[17] UNCTAD, UNCTAD Global Cyberlaw Tracker: Summary of Adoption of E-Commerce Legislation Worldwide, available at https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx.

[18] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), OJ L [2016] 119/1.

[19] See generally A. Mattoo and J. P. Meltzer, 'International Data Flows and Privacy: The Conflict and Its Resolution', *Journal of International Economic Law* 21 (2018), 769–789, at 775–776.

[20] Article 17 GDPR.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

control over personal data processing. Other countries, such as Russia[21] and China,[22] have introduced explicit data localisation laws to protect privacy.

No international consensus exists on the best means to achieve online privacy, owing to the distinct socio-cultural perspectives on privacy across countries.[23] For example, the EU strongly advocates privacy as a fundamental human right,[24] including arguing for a blanket exemption for privacy laws in trade agreements.[25] EU's domestic framework has been emulated by other non-EU countries, including India.[26] However, not all countries share a similar perspective on privacy. For instance, in China (which has adopted GDPR-like provisions), privacy is viewed as a matter of information security.[27] To the contrary, in the United States (US) and broadly, under the Asia-Pacific Economic Cooperation (APEC) Privacy Framework,[28] privacy is protected as a consumer right.[29] Finally, several developing countries are yet to implement a privacy or data protection law; thus, data management is solely the prerogative of digital service suppliers in these countries.

II *Cybersecurity and Cross-Border Data Flows*

The relationship between cybersecurity and data restrictions is a relatively underexplored area,[30] although one-third of new trade-related concerns relate to

[21] Article 18(5) Портал персональных данных Уполномоченного органа по защите персональных данных [Federal Law No. 242-FZ of 21 July 2014 on Amendments to Certain Legislative Acts of the Russian Federation with Regard to Specifying the Procedure for the Processing of Personal Data in Data Telecommunications Networks].

[22] Article 37 Cybersecurity Law of the People's Republic of China [Zhonghua Renmin Gongheguo Wangluo Anquan Fa], adopted 7 November 2016, available at: www.chinalawinfo.com.

[23] Kuner, note 5, at 33–34.

[24] G. Buttarelli, 'Less Is Sometimes More', *European Data Protection Supervisor Blog*, 18 December 2017, available at https://edps.europa.eu/press-publications/press-news/blog/less-sometimes-more_en.

[25] European Commission, Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection in EU Trade and Investment Agreements, February 2018, available at https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf [hereinafter: Horizontal Provisions].

[26] Government of India, Ministry of Electronics and Information Technology, The Personal Data Protection Bill 2018, available at https://meity.gov.in/content/personal-data-protection-bill-2018.

[27] See, e.g., J.-A. Lee, 'Hacking into China's Cybersecurity Law', *Wake Forest Law Review* 53 (2018), 57–104, at 99–103.

[28] APEC, *APEC Privacy Framework* (Singapore: APEC Secretariat, 2005).

[29] C. Bulford, 'Between East and West: The APEC Privacy Framework and the Balance of International Data Flows', *I/S: Journal of Law and Policy* 3 (2007–2008), 705–722, at 707–709; See APEC, note 28, at Foreword; S. Yakovleva, 'Should Fundamental Rights to Privacy and Data Protection Be a Part of the EU's International Trade "Deals"?', *World Trade Review* 1 (2017), 477–508.

[30] See S. Y. Peng, 'Cybersecurity Threats and the WTO National Security Exceptions', *Journal of International Economic Law* 18 (2015), 449–478; M. F. Ferracane, 'Data Flows and National Security: A Conceptual Framework to Assess Restrictions on Data Flows under GATS Security Exception', *Digital Policy, Regulation and Governance* 21 (2019), 44–70.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

cybersecurity.[31] The predominant motive behind cybersecurity measures is shielding a country's citizens and infrastructure against potential risks arising from poor cybersecurity practices. These risks may relate to consumer risks, such as compromising personal data through unauthorised hacking or cyberattacks; risks threatening public order (but not creating a war-like situation) resulting from security failures in ubiquitous technologies such as Internet of Things (IoT) and cloud computing; network attacks on the domain name system; and finally, national security risks arising from attacks on a country's critical infrastructure including a cyberwar-like situation.[32] For example, both the Chinese and Vietnamese cybersecurity law, which inter alia mandate data localisation, equate cybersecurity to different national interests in cyberspace, covering issue-areas varying from data security to ensuring control over domestic data flows.[33]

Several experts argue that ensuring security through data restrictive measures is largely ineffective. First, divergent cybersecurity laws (including technical standard requirements) across countries make it harder for suppliers of digital products to adopt best-in-class standards and practices in security.[34] For example, indigenous cybersecurity standards (particularly those that are not interoperable with globally recognised standards) hamper the ability of companies to 'reduce network latency and maintain redundancy for critical data',[35] and detect potential cyber risks.[36] Similarly, data localisation on grounds of security increases costs for companies in replicating their systems across different countries.[37] Second, data flow restrictions eventually increase concentration of data in specific servers, making targeting in cyberattacks much easier.[38] Finally, as long as countries remain connected to the global network, data (whether stored locally or otherwise) remains vulnerable to cyberattacks (such as distributed denial of service attacks). In restricting data storage/processing to specific jurisdictions, these risks cannot be eliminated.[39]

[31] WTO, 'Members Debate Cyber Security and Chemicals at Technical Barriers to Trade Committee', *WTO News*, 15 June 2017, available at www.wto.org/english/news_e/news17_e/tbt_20jun17_e.htm.

[32] C. Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems', *German Law Journal* 18 (2017), 881–918, at 897.

[33] United States Trade Representative, *2016 National Trade Estimate Report on Foreign Trade Barriers* (Washington, DC: Office of the US Trade Representative, 2016), at 91; WTO, Measures Adopted and under Development by China Relating to Its Cybersecurity Law, Communication from the United States, S/C/W/274, 26 September 2017; *Lu□t an ninh mạng* [Law 24 on Cybersecurity], Law No 24/2018/QH14 (Vietnam). See also Chapter 12 in this volume.

[34] *Digitalization for All: Future-Oriented Policies for a Globally Connected World*, Joint B20 Statement, 2017, at 11.

[35] Business Software Alliance, 'Cross-Border Data Flows', 2017, available at www.bsa.org/~/media/Files/Policy/BSA_2017CrossBorderDataFlows.pdf.

[36] H. J. Brehmer, 'Data Localization: The Unintended Consequences of Privacy Litigation', *American University Business Review* 67 (2018), 924–969, at 967.

[37] Ibid., at 965.

[38] A. Chander and U. P. Lê, 'Data Nationalism', *Emory Law Journal* 64 (2015), 677–739, at 717.

[39] Ibid., at 715.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

III *Protecting Consumer Rights through Data Restrictions*

The discussion of the relationship between cross-border data transfers and protecting consumer rights is often subsumed under privacy-related discussions such as obtaining informed user consent for data use/processing and data interoperability across different digital media. However, protecting consumers also relates to other issues such as reliability of data analytics and prohibiting discriminatory treatment of certain consumer groups.[40] For example, the increased use of artificial intelligence (AI) raises concerns regarding exclusion of minority groups through biased algorithms.[41] Another online consumer-protection related issue is ensuring integrity and authenticity of electronic commerce transactions.[42]

Regulatory frameworks addressing online consumer protection at an international/transnational level are absent because rights and remedies available to consumers are largely addressed through contracts and domestic laws.[43] The growth of digital trade, however, necessitates a coherent international framework rather than isolated domestic laws to address disputes related to cross-border e-commerce transactions.[44] Cross-border aspects of online consumer protection include issues such as failed delivery of services or inadequate quality, misuse of consumer data, and misinformation regarding specific digital products and services.[45] Since these issues can relate to cross-border activities of both service suppliers and consumers, incompatible or weak domestic frameworks often pose a hindrance to protecting consumer rights transnationally.

Governments have so far not explicitly adopted data restrictions based on consumer protection laws (e.g. to ensure a higher standard of data ethics or protection of consumers in one-sided digital service contracts). However, certain domestic laws like the GDPR incorporate elements of consumer protection such as restricting data-based consumer profiling.[46] Further, the e-Privacy Directive in the EU imposes requirements for cookies that can obstruct the free cross-border flow of data.[47] Poor

[40] M. Scrage, 'Big Data's Dangerous New Era of Discrimination', *Harvard Business Review*, 29 January 2014.

[41] L. Enochs, 'Policy Is Crucial in Curbing Discriminatory Artificial Intelligence', *CIGI*, 6 June 2018, available at www.cigionline.org/articles/policy-crucial-curbing-discriminatory-artificial-intelligence.

[42] See OECD, *Consumer Protection in E-Commerce: OECD Recommendations* (Paris: OECD Publishing, 2016).

[43] See generally K. McGillivray, 'A Right Too Far? Requiring Cloud Service Providers to Deliver Adequate Data Security to Consumers', *International Journal of Law and Information Technology* 25 (2017), 1–25, at 5–12.

[44] See generally B. Wylie and S. Macdonald, 'What Is a Data Trust?', *CIGI*, 9 October 2018, available at www.cigionline.org/articles/what-data-trust.

[45] See OECD, note 42.

[46] See Articles 21 and 22 GDPR.

[47] Article 5(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

cybersecurity practices of digital service providers can also pose a challenge to online consumer protection. For example, certain countries prescribe technical standards for cloud service providers in order to ensure adequate quality of cloud services for Internet users within the country.[48] Such measures, however, inhibit global business models/practices of cloud service providers, thereby restricting the free flow of data and significantly increasing compliance costs for foreign companies, in turn raising prices and reducing choice for consumers.[49]

IV *Access to Data for Law Enforcement*

Governments consider ready access to data a priority as the Internet is critical for carrying out different human activities, including criminal ones. However, the legal position on access to extraterritorial digital data is unsettled.[50] Consequently, different governments have adopted measures to increase regulatory control over data including data localisation laws. For example, the Indian government announced that payment service providers offering services in India must localise their data operations so as to ensure regulatory oversight over all financial transactions.[51] Additionally, certain governments have tried to exercise greater control over encryption in order to obtain access to data.[52] Selby has argued that data restrictive measures are primarily driven by the competition between governments to achieve more intelligence by controlling data flows, especially given the monopoly of American technology companies.[53]

The dispute involving Microsoft and the US government is an example of the difficulties associated with accessing data located outside one's borders.[54] In this dispute, the US government issued a warrant for data located on Irish servers for domestic law enforcement activities, which Microsoft refused to comply with

Electronic Communications Sector, OJ L [2002] 201/37; see also L. Coll and R. Simpson, *The Internet of Things and Challenges for Consumer Protection* (London: Consumers International, 2016), at 41.

[48] See, e.g., China is developing domestic standards for cloud computing under the Information Security Technology – Security Capability Requirements of Cloud Computing Services.

[49] Z. Fan and A. Gupta, 'The Dangers of Digital Protectionism', *Harvard Business Review*, 30 August 2018.

[50] K. Eichensehr, 'Data Extraterritoriality', *Texas Law Review* 95 (2017), 145–160, at 152.

[51] Reserve Bank of India, Storage of Payment System Data Notification, RBI/2017-18/153, 6 April 2018, available at www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0.

[52] See, e.g., A. Reikis, 'Australian Bill to Create Back Door into Encrypted Apps in "Advanced Stages"', *The Guardian*, 12 April 2018; see also US Library of Congress, 'Government Access to Encrypted Communications: France', 10 January 2016, available at www.loc.gov/law/help/encrypted-communications/france.php.

[53] J. Selby, 'Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?', *International Journal of Law and Information Technology* 25 (2017), 213–232, at 231–232.

[54] *Microsoft Corporation* v. *United States*, 584 U. S.__(2018).

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

because the warrant related to data located outside the United States.[55] One of the key issues highlighted through this dispute was the ineffectiveness of Mutual Legal Assistance Treaties (MLATs) or letters rogatory to obtain legal access to extraterritorial data. While MLATs are time consuming and only exist between specific countries, letters rogatory are discretionary and thus unreliable.[56] This case was finally resolved by the adoption of the Clarifying Lawful Overseas Use of Data (CLOUD) Act containing a procedure for obtaining extraterritorial data based on principles of comity through executive action.[57]

V *Digital Industrial Policy in Developing Countries*

The use of data restrictive measures as digital industrial policy is becoming popular in certain countries in Africa and India.[58] The main argument is that most developing countries are unable to benefit from global digital value chains as the intellectual property (IP) and critical data resources are largely owned by companies in developed countries.[59] In other words, public ownership of data is considered vital to achieve domestic economic interests.[60] Thus, developing countries have argued that they should be able to adopt digital industrial policies, including data localisation and content filtering measures.[61] UNCTAD has further supported this approach, including advocating that developing countries should not be compelled to support the moratorium on customs duties on electronic transmissions (which is a fundamental requirement for free flow of data), as it would cause significant tariff losses.[62]

[55] J. Daskal, 'Microsoft Ireland Argument Analysis: Data, Territoriality, and the Best Way Forward', *Harvard Law Review Blog*, 28 February 2018.

[56] S. P. Mulligan, *Cross-Border Data Sharing under the CLOUD Act* (Washington, DC: Congressional Research Service, 2018), at 12–14.

[57] Ibid., at 9–10.

[58] See, e.g., WTO, Work Programme on Electronic Commerce: Moratorium on Customs Duties on Electronic Transmissions, Communication from India and South Africa, WT/GC/W/747, 12 July 2018 [hereinafter: Communication from India and South Africa]; WTO, Work Programme on Electronic Commerce: Report of Panel Discussion on 'Digital Industrial Policy and Development', Communication from the African Group, JOB/GC/133, 21 July 2017 [hereinafter: Communication from the African Group].

[59] UNCTAD, Adapting Industrial Policies to a Digital World for Economic Diversification and Structural Transformation, 2nd Session, 19 and 20 March 2018, Geneva, TD/B/C.I/MEM.8/5, 12 February 2018, at paras. 29–30; UNCTAD, *Trade and Development Report 2018: Power, Platforms and the Free Trade Delusion* (Geneva/New York: United Nations Publications, 2018) [hereinafter: UNCTAD Development Report], at 70–72, 77–78.

[60] B. Fang, *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace* (Singapore: Springer, 2018), at 358–359.

[61] Communication from the African Group, note 58; UNCTAD Development Report, note 59, at 69, 84, 89, 109.

[62] UNCTAD, *Rising Product Digitalisation and Losing Trade Competitiveness* (Geneva/New York: United Nations Publications, 2017), at 16–17; UNCTAD, *Digital Economy Report: Value Creation and Capture: Implications for Developing Countries* (Geneva/New York: United Nations Publications, 2019), at xix.

India and Africa have expressed public support for UNCTAD's position on digital industrial policy at the WTO on numerous occasions,[63] although certain studies indicate that these policies are unlikely to be effective.[64] Unsurprisingly, certain developing countries, including Nigeria and Indonesia, have adopted data restrictive measures to create opportunities for domestic players.[65]

C TRADE-RELATED ASPECTS OF DATA GOVERNANCE

The discussion in the previous section indicates the complex, multilayered nature of data governance, and the need for a holistic and multidimensional trade framework on cross-border data flows. While not all governance issues related to data transfers are trade related, certain issues including online consumer protection, cybersecurity and privacy, as discussed later, are necessary to ensure a stable regulatory framework for digital trade. Being atypical of trade agreements, these issues are not explicitly covered in WTO agreements, such as the GATS.

I *Applying WTO Disciplines to Data Restrictive Measures*

Several scholars have examined how GATS applies to data restrictive measures and this section does not replicate such efforts.[66] For example, if a dispute were to arise on a data restrictive measure, legal obligations on national treatment and domestic regulation would be relevant if the measure favoured domestic services and service suppliers or imposed unreasonable compliance requirements on foreign services and service suppliers.[67] Similarly, restricting or banning cross-border data flows in sectors where members have made explicit GATS commitments could violate market access obligation.[68] GATS also encourages transparency of regulations.[69] Lastly, the general exceptions in Article XIV GATS can be relevant in distinguishing

[63] Communication from India and South Africa, note 58; WTO, Work Programme on Electronic Commerce: The E-Commerce Moratorium and Implications for Developing Countries, Communication from India and South Africa, WT/GC/W/774, 4 June 2019.

[64] M. Farid Badran, 'Economic Impact of Data Localization in Five Selected African Countries', *Digital Policy, Regulation and Governance* 20 (2018), 337–357; E. van der Marel, H. Lee-Makiyama, and M. Bauer, 'The Costs of Data Localisation: A Friendly Fire on Economic Recovery', ECIPE Occasional Paper No 3 (2014). See Chapter 3 in this volume.

[65] Chander and Lê, note 38, at 701–703.

[66] See, e.g., A. Mitchell and J. Hepburn, 'Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer', *Yale Journal of Law and Technology* 19 (2017), 182–237; M. Burri, 'The Regulation of Data Flows through Trade Agreements', *Georgetown Journal of International Law* 48 (2017), 407–448; S.-Y. Peng and H.-W. Liu, 'The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?', *Journal of World Trade* 51 (2017), 183–204, at 199.

[67] Mitchell and Hepburn, note 66, at 195–206.

[68] Ibid.

[69] Article III GATS.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

blatantly protectionist data restrictive measures (which are impermissible) from legitimate policy measures (falling within the scope of these exceptions). Thus, theoretically, the principles underlying GATS support an open environment for data flows without restraining WTO members from regulating the Internet for legitimate reasons.[70]

However, applying the pre-Internet era GATS disciplines to data-related disputes is challenging. Wu terms this as the 'problem of interpretative technological translation',[71] i.e. applying GATS to technologies not envisioned at the time these rules were framed.[72] First, cross-border data flows relate to not only trade in services but also trade in goods.[73] Segregating the goods-related and services-related aspect of measures can be challenging when services form an integral part of a good (e.g. IoT). Second, interpreting whether a member's commitments in its GATS Schedule on national treatment and market access cover data flows in a certain sector is tough due to the cross-cutting nature of digital services.[74] Third, the proximity of service suppliers and consumers in the digital supply chain leads to highly intrusive (and sometimes, inefficient) data restrictive measures that are also trade inhibiting.[75]

II *Trade-Related Aspects of Data Flows*

Given that GATS is not sufficiently adaptable to a data-driven economy, we delve deeper into aspects of data regulation that are trade related but remain inadequately addressed in GATS.

1 Privacy Protection and GATS

As discussed earlier, privacy protection is the most common rationale for imposing data restrictions. Arguably, GATS acknowledges the importance of privacy protection under the exceptions contained in Article XIV(c)(ii) GATS:

> (N)othing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures:
>
> (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to:

[70] J. López González and J. Ferencz, *Digital Trade and Market Openness* (Paris: OECD Publishing, 2018), at 6.

[71] Wu, note 4, at 264.

[72] Ibid.

[73] Aaronson, note 15, at 6–7.

[74] L. Tuthill and M. Roy, 'GATS Classification Issues for Information and Communication Technology Services', in M. Burri and T. Cottier (eds), *Trade Governance in the Digital Age* (Cambridge: Cambridge University Press, 2012) at 157–178, at 167; R. H. Weber and M. Burri, *Classification of Services in the Digital Economy* (Berlin: Springer, 2012), at 49.

[75] Aaronson, note 15, at 6–7.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

> (ii) the protection of the *privacy of individuals in relation to the processing and dissemination of personal data* and *the protection of confidentiality of individual records and accounts*.[76]

Further, paragraph 5(d) of GATS Telecommunications Annex states:

> [A] Member may take such measures as are necessary to ensure the *security and confidentiality of messages*, subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade in services.[77]

The exceptions for 'protection of privacy of individuals' in Article XIV(c)(ii) GATS and 'ensuring security and confidentiality of messages' in the Telecommunications Annex indicate that WTO members were aware of and recognised the fundamental importance of privacy as a policy objective and, therefore, considered them permissible even if they violated trade obligations of a WTO member. Further, Article XIV (c)(ii) GATS does not prevent members from choosing a specific standard of privacy/data protection, but rather requires examination of whether the adopted measure/standard on data protection is indeed necessary to achieve compliance with domestic privacy/data protection laws.

However, Article XIV(c)(ii) GATS cannot ensure that all WTO members adopt a sound and robust framework on data protection/privacy, but only protects their right to impose restrictions/measures to safeguard privacy of individuals and/or protect confidentiality and security of electronic transmissions. Online privacy is a fundamental precondition for open, transparent and secure flows of data across borders.[78] For example, consumers are likely to engage in digital trade only when they trust that the digital service suppliers adequately prevent unauthorised access or misuse of their data. Similarly, GATS does not address trade barriers resulting from variations in privacy frameworks across countries, as it does not specifically mandate WTO members to develop mutually compatible frameworks on privacy. For example, the mechanism available under Article VII GATS for mutual recognition of 'standards or criteria for the authorization, licensing or certification of services suppliers' has never been utilised for ensuring compatibility of privacy/data protection frameworks of WTO members.[79]

[76] Emphasis added. Additionally, 'public morals' under Article XIV(a) GATS can be interpreted to cover privacy.

[77] Emphasis added.

[78] See generally N. Mishra, 'Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows', *Vanderbilt Journal of Transnational Law* 52 (2019), 463–509, at 492–494.

[79] Article VII:1 GATS.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

2 Cybersecurity and GATS

Another common rationale for imposing data restrictions is protecting security of data or the cyber networks within a country. This rationale is also related to broader national security requirements.[80] Like privacy protection, cybersecurity may be covered under Article XIV GATS, although cybersecurity is obviously not explicitly mentioned.[81] However, the exception could apply if a cybersecurity measure is necessary to maintain public order (Article XIV(a) GATS).[82] For example, certain studies suggest that the entire public utility network of a country (e.g. electricity supply) can be brought down by malware attacks by targeting smart devices used at home.[83] Another issue (particularly in trade in goods) is restrictions on encryption or forced adoption of specific encryption standards and its adverse impact on foreign suppliers.[84] Such measures are detrimental to enhancing trust of Internet users and are likely to render digital products more vulnerable to cyber intrusions.[85]

Further, Article XIV(c)(ii) GATS could be interpreted to cover certain data/Internet security measures:

> (N)othing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures:
>
> (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to:
>
> (i) the prevention of *deceptive and fraudulent practices* or to deal with the effects of a *default on services contracts*;
>
> (iii) *safety*.[86]

Domestic laws related to 'deceptive and fraudulent practices', 'default on services contracts' and 'safety' in Article XIV(c) GATS can be creatively and flexibly interpreted to cover both cybersecurity and consumer protection–related measures. For example, a government can ban insecure and unencrypted services or impose data

[80] See, e.g., Law 24 on Cybersecurity of Vietnam, note 33.

[81] For the purposes of this article, we leave aside the issue of cyber wars and their relevance under Article XIV*bis* GATS because little evidence exists whether cyberattacks constitute armed attack or an emergency in international relations.

[82] Article XIV(a), footnote 5 GATS.

[83] General Electric, 'The Impact of Cyber Attacks on Critical Infrastructure', *GE Digital*, 2017, available at www.ge.com/digital/sites/default/files/download_assets/the-impact-of-cyber-attacks-on-critical-infrastructure-infographic.pdf; CISCO and the Chertoff Group, 'Addressing Critical Infrastructure Cyber Threats for State and Local Governments: Application of a Treat-Centric Approach through the NIST Cybersecurity Framework', 2015, available at www.cisco.com/c/dam/global/en_sg/assets/pdfs/govt_n_critical_infra_2169_cistcg_cisco_white_paper_v4-1.pdf.

[84] See generally R. Buddish, H. Burkert, and U. Gasser, 'Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects', Aegis Paper No 1804 (2018).

[85] D. Castro and A. Mcquinn, 'Unlocking Encryption: Information Security and the Rule of Law', *Information Technology and Innovation Foundation*, March 2016, at 2, 6.

[86] Emphasis added.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

flow restrictions on foreign companies (particularly in sensitive sectors) to ensure that consumer data is not wrongfully used abroad. Further, since Article XIV(c) GATS is not exhaustive, a member may argue that its data restrictive measure is necessary to ensure compliance with domestic cybersecurity laws.

Like online privacy, cybersecurity is an essential component of ensuring free and open environment for global digital trade. However, the earlier mentioned exceptions do not require WTO members to adopt regulatory frameworks or enhance international cooperation on cybersecurity. While certain discussions at the WTO have centred on ensuring that technical compliance requirements for digital products are in conformity with international technical standards (such as under the TBT agreement),[87] similar requirements have not been explicitly included in GATS.

3 Online Consumer Protection and Digital Trade

In addition to privacy protection and cybersecurity, online consumer protection is also important to ensure an open, transparent and secure environment for digital trade and data flows.[88] For example, when buying online, consumers directly interact with service suppliers, and thus may be more vulnerable to one-sided contracts. Further, protecting Internet users from fraudulent transactions, breaches, spam and malware attacks, and data misuse by service providers and third-party advertising services is important for digital trade.[89] In case of divergent consumer protection laws across countries (e.g. rules related to enforcement and authentication of electronic contracts), businesses and consumers both face legal uncertainty when transacting online.[90] While multinational companies such as Amazon can tailor consumer contracts on a country-by-country basis and even build local servers (where such laws exist), smaller companies cannot do so.

GATS does not set any requirements for countries to adopt consumer protection laws in order to ensure adequate quality or security of services and arguably only provides for an exception under Article XIV(c)(ii) GATS to restrict data flows in consumer interests. For achieving liberalisation of digital trade, adopting internationally recognised models of consumer protection and active international cooperation on online consumer protection among WTO members is more beneficial and effective than unilateral domestic restrictions. However, to date, these questions have not been addressed at the WTO.

[87] See WTO, 'WTO Members Start Review of Technical Barriers to Trade Agreement', *WTO News*, 8 and 9 November 2017, available at www.wto.org/english/news_e/news17_e/tbt_15nov17_e.htm; WTO, Committee on Technical Barriers to Trade, Minutes of the Meeting of 8–9 November 2017, G/TBT/M/73, 6 March 2018.

[88] See, e.g., WTO, Joint Statement on Electronic Commerce: Establishing an Enabling Environment for Electronic Commerce, Communication from the European Union, JOB/GC/188, 16 May 2018, at para. 1.3.

[89] Ibid., at para. 2.3.

[90] Consumers International, note 47, at 40–41.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

4 GATS Compatibility of Digital Industrial Policy

Certain countries, as discussed earlier, impose data restrictions as a tool of industrial policy. GATS prohibits members from imposing data restrictive measures in those sectors where they have made explicit commitments on national treatment and market access,[91] and also prohibits arbitrary and discriminatory measures that are unconnected to domestic regulatory objectives.[92] However, given the importance of protecting developing countries' interests at the WTO, especially their meaningful integration into the global economy,[93] WTO members can consider if certain data restrictive measures are beneficial to developing countries and least-developed countries (LDCs). For example, some developing countries/LDCs may argue that they need more time to open specific sectors to global competition. However, a necessary part of bridging the digital divide between developed and developing countries involves improving domestic access to high-quality and competitively priced digital services and platforms.[94] Data restrictive measures reduce consumer access to competitive digital services and could backfire in the long run and inhibit the growth of developing countries. Thus, investigating the necessity of data restrictive measures to enable digital development of developing countries is important.[95]

5 Data-Related Issues Outside the Scope of WTO Law

Certain aspects of data regulation cannot be addressed by WTO law even if they have a trade-restrictive impact. For example, in examining whether a measure is necessary to protect public morals under Article XIV(a) GATS, WTO panels and the Appellate Body have taken a deferential stance towards online censorship, as in *China – Publications and Audiovisual Products*.[96] Thus, WTO members are largely free to adopt measures censoring content online provided they comply with Article XIV(a) GATS. Given that the evaluation of the data content is based on the specific socio-cultural circumstances of each country, leaving out such issues from the ambit of trade agreements is judicious. However, further dialogues in the Internet policy and international human rights community on the necessity and the most appropriate tools for online censorship might better inform the application of Article XIV(a) GATS. WTO law also cannot address the international cooperation framework for

[91] See Article XVI and Article XVII GATS.
[92] Article XIV GATS. See also Article VI:1 and 5 GATS.
[93] Article IV and Preamble GATS.
[94] See generally The World Bank, *World Development Report 2016: Digital Dividends* (Washington, DC: The World Bank, 2016).
[95] See, e.g., WTO, 'Data Localization: Balancing Trade Disciplines and National Policy Objectives', Discussions at the WTO Public Forum 2018, session on audio file, 4 October 2018, available at www.wto.org/audio/pf18session76.mp3.
[96] Appellate Body Report, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products (China – Publications and Audiovisual Products)*, WT/DS363/AB/R, adopted 21 December 2009, at paras. 240–243.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

accessing extraterritorial data as it is better addressed by international treaties such as MLATs or other initiatives, such as the CLOUD Act, as mentioned earlier.

D DEVISING A WTO FRAMEWORK ON DATA FLOWS

An ideal digital trade framework should facilitate free data flows, digital innovation, and healthy competition in the global digital market without interfering with a country's right to legitimately regulate the Internet.[97] In this section, we propose a WTO framework on data regulation addressing various trade-related aspects of data flows that fits better into such an ideal digital trade framework. The suggested framework is similar to certain recent PTAs but with specific modifications that adapt to the diversity of the WTO membership. The following first section discusses the foundational principles of data regulation in international trade law, while the subsequent section advances our proposals for reform in WTO law.

I *Foundational Principles of Data Regulation in International Trade Law*

1 Fostering Digital Trust at a Domestic and Transnational Level

WTO disciplines should enable 'digital trust', which in turn requires preserving user privacy, protecting consumers against spam, fraudulent transactions and cybersecurity attacks, and facilitating business trust, for example, providing adequate IP protection and a competitive environment for digital innovation.[98] To contribute to digital trust, the WTO framework should (i) facilitate increased transnational dialogues and international regulatory coordination and cooperation on relevant issues, such as data flows, cybersecurity and privacy; and (ii) safeguard policy space necessary for countries to enable and maintain Internet trust in domestic cyberspace, provided they meet the requirements of reasonableness (e.g. under Article VI GATS) and are not disguised protectionist measures (e.g. evaluation under Article XIV GATS). In our view, this two-fold approach to enable digital trust will promote 'trustworthy information relationships' in the global ecosystem for cross-border data transfers.[99] However, we do not argue that WTO rules are alone sufficient to ensure digital trust but rather that they could contribute to the global framework for data regulation.[100]

[97] See generally López González and Ferencz, note 70, at 37.

[98] B. Chakrovorthi, 'Trust in Digital Technology Will Be the Internet's Next Frontier, for 2018 and Beyond', *The Conversation*, 4 January 2018; J. Hoffmann, 'Constellations of Trust and Distrust in Internet Governance', in European Commission, *Trust at Risk: Implications for EU Policies and Institutions* (Brussels: European Commission, 2017), 85–98, at 9–13.

[99] Idea borrowed from N. Richards and W. Hartzog, 'Privacy's Trust Gap: A Review', *Yale Law Journal* 126 (2017), 1180–1224, at 1186–1187.

[100] S. A. Aaronson, 'Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security', *World Trade Review* 14 (2015), 671–700, at 679.

2 Ensuring Interoperability and Transparency to Facilitate Free Flow of Data

WTO disciplines should ensure interoperability and transparency of Internet regulations/regulatory frameworks to facilitate data flows and greater accountability in digital networks. These twin objectives are particularly important for highly beneficial but risky technologies such as AI and IoT.[101]

Article VII GATS provides for mutual recognition of 'standards or criteria for the authorization, licensing or certification of services suppliers'. Although non-binding, Article VII:5 GATS recognises the need for more international coordination between WTO members on domestic regulations pertaining to licensing, certification or authorisation of service suppliers:

Wherever appropriate, recognition should be based on multilaterally agreed criteria. In appropriate cases, members shall work in cooperation with relevant intergovernmental and non-governmental organisations towards the establishment and adoption of common international standards and criteria for recognition and common international standards for the practice of relevant services trades and professions.

Varying standards of privacy and security across countries create impediments to cross-border data flows. While harmonising privacy and cybersecurity laws can be difficult and perhaps impossible due to the divergence of views/practices across different systems, cooperation and interoperability between different regulatory systems is achievable.[102] The WTO can learn from the experience of other international institutions such as United Nations Commission on International Trade Law (UNCITRAL) and the International Institute for the Unification of Private Law (UNIDROIT) that have used similar techniques in various areas of public and private international law respectively to obtain interface between different regulatory frameworks.[103] Further, developing new rules under Article VI:5 GATS relating to 'qualification requirements and procedures, technical standards and licensing requirements' on data flows can incentivise greater recognition of regulatory frameworks among WTO members.[104]

Another fundamental requirement that must be addressed in WTO law is transparency of data regulations. Despite a binding legal mechanism under Article III GATS, several WTO members adopt ambiguously worded data restrictive measures, causing considerable uncertainty for businesses and consumers alike. More mechanisms should be devised to increase governmental accountability at the WTO for their data

[101] S. A. Aaronson, 'Data Minefield? How AI Is Prodding Governments to Rethink in Data', *CIGI*, 3 April 2018, available at www.cigionline.org/articles/data-minefield-how-ai-prodding-governments-rethink-trade-data.

[102] See generally A. O. Sykes, 'Regulatory Competition or Regulatory Harmonization? A Silly Question?', *Journal of International Economic Law* 3 (2000), 257–264.

[103] Ibid.

[104] J. P. Trachtman, 'Lessons for GATS Article VI from the SPS, TBT and GATT Treatment of Domestic Regulation', SSRN Publication (2002), at 34, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=298760.

regulations, including effective use of the Trade Policy Review mechanisms and discussions in various WTO committee meetings. Through such informal and open dialogues, members may be able to build international cooperation on relevant issues, thereby automatically reducing the tendency to adopt opaque data regulations.

3 Exploring New Regulatory Approaches in WTO Law

The third fundamental component necessary to adapt WTO law to the data-driven economy is to explore innovative and inclusive approaches in digital trade and data regulation that consider the multi-stakeholder nature of the Internet governance regime, particularly the central role of private sector in ensuring openness and security of data flows.[105] Different experts have argued that the regulatory framework for data flows requires a more sophisticated approach than traditional multilateral processes. For instance, Shackelford and others argue that majority of privacy and security issues related to digital technologies require poly-centric governance, including a self-regulatory approach in highly technical areas.[106] Kuner emphasises the significance of private sector instruments (including codes of practice and contractual clauses) in regulating cross-border data flows,[107] and argues that regulation of data flows is 'a form of legal pluralism', with no single authoritative framework.[108] Segura-Serrano argues that data regulation requires a hybrid approach involving a mixture of prescriptive and self-regulatory approaches.[109]

Adopting a co-regulatory or hybrid regulatory approach (involving the private sector and multi-stakeholder organisations) at the WTO can be challenging. For example, the WTO has not traditionally liaised with multi-stakeholder institutions, such as those prevalent in Internet policy community. Similarly, WTO rules do not refer to private standards or industry best practices although they may be commonplace in the digital world.[110] However, the WTO can liaise with multilateral institutions in relevant areas. For instance, under GATT, various mechanisms are established for consultation with the International Monetary Fund (IMF) for areas related to currency valuation and exchange.[111] Similarly, regarding applying WTO

[105] L. DeNardis, 'Five Destabilizing Trends in Internet Governance', *I/S: A Journal of Law and Policy* 12 (2015), 113–133, at 115.

[106] S. J. Shackelford et al., 'When Toasters Attack: A Polycentric Approach to Enhancing the Security of Things', *University of Illinois Law Review* 2 (2017), 415–475, at 439.

[107] Kuner, note 5, at 159.

[108] Ibid., at 160.

[109] A. Segura-Serrano, 'Internet Regulation and the Role of International Law', in A. Von Bogdandy, R. Wolfrum, and Ch. E. Philipp (eds), *Max Planck Yearbook of United Nations Law*, Vol. 10 (Leiden: Brill, 2006), 191–272, at 199–200.

[110] See generally J. Pauwelyn, 'Rule-Based Trade 2.0? The Rise of Informal Rules and International Standards and How They May Outcompete WTO Treaties', *Journal of International Economic Law* 17 (2014), 739–751, at 739.

[111] See, e.g., Article XV GATT.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

disciplines to environmental issues, WTO members have undertaken various commitments to engage with multilateral environmental institutions.[112] There is no reason why a similar approach cannot be followed in the area of Internet and data regulation where multi-stakeholder institutions and private sector play a key role, for example, in technical standard-setting.

More specifically, some form of regulatory innovation is essential at the WTO to respond to the needs of data-driven sectors. For example, in certain cases, multi-stakeholder discussions involving Internet experts can enable a more balanced evaluation of cyber risks in digital services and the necessity of certain trade restrictive measures to address these cyber risks. This approach might be more effective than imposing unilateral data restrictions, which are not only highly trade restrictive but also have limited impact on ensuring digital trust and innovation.[113]

II *Reforms in the WTO Framework for Data Regulation*

The next section discusses various rules that we think should be included in a new WTO framework governing data flows. Many of the proposed rules in our framework somewhat resemble the rules in certain recent PTAs, such as the United States–Mexico–Canada Agreement (USMCA) and Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). However, we incorporate additional suggestions and modifications to make these rules more balanced and representative of interests of developing countries, as well as address fundamental public policy challenges in data regulation, including protecting regulatory autonomy of WTO members, as and when necessary.

1 Horizontal Obligation on Cross-Border Data Flows and Data Localisation

WTO law should incorporate horizontal obligations on ensuring free flow of data for the purposes of conducting regular business transactions and to prohibit forced data localisation. Data flows are fundamental for the growth of the digital economy and are required for both services and manufacturing sectors. In the age of cloud computing, when companies manage data resources in real time based on server capacities and real-time demands on server space, prohibitions on cross-border data flows and geographical restrictions on data storage can be a significant trade barrier.

[112] See, e.g., 'Relevant WTO Provisions: Text of 1994 Decision', available at: www.wto.org/english/tratop_e/envir_e/issu5_e.htm; see also 'Relevant WTO Provisions: Text of Services Decision', available at www.wto.org/english/tratop_e/envir_e/issu6_e.htm.

[113] Experts have also proposed technological or principles-based solutions to privacy and security issues. See J.-S. Bergé, S. Grumbach, and V. Zeno-Zencovich '"The Datasphere", Data Flows beyond Control, and the Challenges for Law and Governance', *European Journal of Comparative Law and Governance* 5 (2018), 144–178, at 156; Kuner, note 5, at 168.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

Thus, we recommend a horizontal obligation for enabling cross-border data flows for purposes of conducting businesses and prohibition on data localisation measures.

Provisions on data flows can be found in recent PTAs, such as Peru–Australia Free Trade Agreement (PAFTA),[114] USMCA, CPTPP, etc.[115] We discuss the CPTPP later as successive PTAs contain similar provisions. Article 14.11(2) CPTPP states: 'Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.' Further, CPPTPP Article 14.13(2) provides,: 'No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.'

Both these provisions are, however, rightly subject to an exception in Article 14.11(3) and Article 14.13(3) CPTPP, respectively to 'adop[t] or maintai[n] measures' inconsistent with Article 14.11(2) and Article 14.13(2) in order to achieve a 'legitimate public policy objective', provided that such measure is 'not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or disguised restriction on trade' and 'does not impose restrictions on transfers of information/the use or location of computing facilities, greater than required to achieve the objective'. We recommend a similar provision within the WTO framework.

Although Article 14.11(3) and 14.13(3) CPTPP are similar to Article XIV GATS and Article XX GATT, clarifying the scope of 'legitimate public policy objective' with an illustrative list will be helpful. For example, the list should specify that cybersecurity, privacy, online consumer protection and protecting public order qualify as 'legitimate public policy objectives'. Further, the exceptions available under Article XIV and Article XIV*bis* GATS should clearly remain applicable for examination of data restrictive measures. For example, a WTO member should remain free to restrict data flows or require data localisation if it is necessary for achieving compliance with domestic laws, for protecting public morals or maintaining public order, or to protect essential security interests.

Given the delicate issues involved in data regulation, clarity in obligations and exceptions on data flows ensures that policy space of WTO members remains untouched. For example, in the Financial Services Chapter of the USMCA, a provision clearly acknowledges the data access to regulators should not be prohibited by data localisation measures. Article 17.20(1) states in this regard:

> No Party shall require a covered person to use or locate computing facilities in the Party's territory as a condition for conducting business in that territory, so long as the Party's financial regulatory authorities, for regulatory and supervisory purposes, have immediate, direct, complete, and ongoing access to information processed or stored on computing facilities that the covered person uses or locates outside the Party's territory.

[114] Peru–Australia Free Trade Agreement (PAFTA), signed 12 February 2018.
[115] Horizontal Provisions, note 25.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

This provision is extremely helpful in clarifying both that (i) regulatory and supervisory authorities should have access to data for authorised and legal purposes; and that (ii) data localisation is not essential to ensure access to data.

2 Enabling International Cooperation on Cybersecurity Issues

Provisions related to relevant trade-related aspects of cybersecurity should be included in WTO law to facilitate an open and secure environment for cross-border data flows. However, we do not recommend that such rules prescribe any specific standards for cybersecurity.

First, WTO members should consider a mandatory requirement for international cooperation on cybersecurity issues.[116] This is not entirely new to the WTO; for instance, WTO members have taken concrete action to ensure greater international cooperation on trade-related environmental issues.[117] Further, given the unique role of private sector in devising and implementing cybersecurity standards, WTO rules should also provide for international cooperation between its members and non-state organisations that play a key role in international governance (including multi-stakeholder bodies).[118] For example, relevant institutions should be consulted at the stage of developing these rules and, later, if trade dispute related to a cybersecurity measure were to arise.[119] Although a little unconventional, recent years have seen WTO being more open to liaise with non-state entities, especially on digital issues. For example, in 2017, a new initiative was launched by WTO and two private sector–led multi-stakeholder institutions, World Economic Forum and Electronic World Trade Platform (e-WTP) entitled 'Enabling Electronic Commerce' to facilitate public–private dialogues on electronic commerce issues.[120]

Second, rather than enforcing domestic cybersecurity standards, WTO members should be encouraged to give preference to internationally recognised standards and best practices in cybersecurity over indigenous cybersecurity standards. Such

[116] In this context, see Articles 24, 25, 27, and 31 Convention on Cybercrime. See also Article 14.16 CPTPP.

[117] WTO, Relevant WTO Provisions: Text of 1994 Decision, available at www.wto.org/english/tratop_e/envir_e/issu5_e.htm; Y. Wang, 'UNEP and WTO Announce Initiative to Align Trade with Sustainable Development', *SDG Knowledge Hub*, 30 January 2018.

[118] See generally K. Karachalios and K. McCabe, *Standards, Innovation, and Their Role in the Context of the World Trade Organization* (Geneva: ICTSD/WEF, 2014).

[119] The latter is possible under the WTO Framework. See Marrakesh Agreement Establishing the World Trade Organization, 1867 U.N.T.S. 3, entered into force 1 January 1995, Annex 2 (Understanding on Rules and Procedures Governing the Settlement of Disputes, DSU), at Article 13.

[120] WTO, 'World Economic Forum and eWTP Launch Joint Public-Private Dialogue to Open Up E-Commerce for Small Business', *WTO News*, 11 December 2017, available at www.wto.org/english/news_e/news17_e/ecom_11dec17_e.htm.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

provisions are atypical of trade agreements, especially for trade in services.[121] Recent PTAs, such as the USMCA, recognise the importance of adopting internationally recognised cybersecurity standard. Article 19.15(2) states that:

> Given the evolving nature of cybersecurity threats, the Parties recognize that *risk-based approaches may be more effective than prescriptive regulation* in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its jurisdiction to use, *risk-based approaches that rely on consensus-based standards and risk management best practices* to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.[122]

However, adopting a similar provision in the WTO framework will be much tougher and is not recommended because of lack of consensus on whether a risk-based approach is most appropriate to address cyber risks.

Finally, all WTO members should be required to adopt a basic level of cybersecurity regulation to prevent countries from becoming havens for criminal or illegal use of digital services and data. This requirement should not prevent members from adopting stricter regulations on cybersecurity as long it is not arbitrary, discriminatory or unreasonable.

3 Requiring Privacy Frameworks and Promoting Mutual Recognition Mechanisms

Requiring all WTO members to adopt a basic regulatory framework for protection of personal information or privacy protection is fundamental for ensuring free flow of data. Meltzer and Mattoo argue that the privacy exception available under Article XIV(c)(ii) GATS is insufficient as it pressurises WTO panels to adjudicate on sensitive privacy issues, which is particularly difficult given that 'data-source countries' are unlikely to 'accept one-sided limits on their right to protect privacy'.[123] To deal with this uncertainty and distrust in other members' privacy frameworks, many countries introduce stringent privacy measures that decrease competitiveness and efficiency of both foreign and domestic digital businesses. Mattoo and Meltzer argue that increasingly more countries are likely to seek bilateral arrangements, such as the data transfer agreement between the EU and the United States (EU–US Privacy Shield) to enable cross-border data flows while ensuring privacy remains protected abroad.[124] They also argue that international recognised standards and guidelines,

[121] G. Gari, 'What Can International Standards on Services Do for GATS?', *E15 Initiative*, September 2015, available at http://e15initiative.org/blogs/what-can-international-standards-on-services-do-for-gats/.

[122] Emphasis added.

[123] Mattoo and Meltzer, note 19, at 789.

[124] Ibid., at 786–788. The EU–US Privacy Shield was invalidated in 2020 by the European Court of Justice, raising significant concerns regarding a future data transfer arrangement between the EU and the United States.

such as the OECD Privacy Framework, provide a basis for aligning privacy laws across countries.[125] However, we see more widespread benefits if, under the ongoing plurilateral negotiations, WTO members considered a provision requiring adoption of a basic domestic privacy framework in line with internationally recognised standards and guidelines.

Recent PTAs contain rules on privacy/data protection, although two different approaches can be seen in EU-led PTAs and US-led PTAs.[126] For example, the USMCA contains the following provision (building on a similar provision in CPTPP):

> To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. In the development of its legal framework for the protection of personal information, each Party should take into account *principles and guidelines of relevant international bodies*, such as the *APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)*.[127]

The specification of OECD and APEC privacy principles as benchmarks could be controversial in a multilateral context, given that they are considered lenient in comparison to the GDPR and similar frameworks. To the contrary, EU FTAs are generally cautious in specifying appropriate rules on data protection, although they require full compatibility with international standards, in the sense that 'the Parties agree that the development of electronic commerce must be fully compatible with the international standards of data protection, in order to ensure the confidence of users of electronic commerce'.[128]

The EU has advocated an even stronger provision on privacy protection in a recent proposal on data flows: 'Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards.'[129]

This provision provides a carte blanche for countries to adopt a privacy framework, irrespective of their trade commitments. We recommend a more balanced provision in WTO law, somewhere in between the lenient provision in USMCA and the provision proposed by EU, which could also increase disguised protectionist

[125] Ibid.

[126] As per Wu, about one-third of PTAs contain a provision requiring data protection for electronic commerce. See M. Wu, *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System* (Geneva/Washington, DC: IDB/ICTSD, 2017), at 20. See also Chapter 1 in this volume.

[127] Article 19.8(2) USMCA (footnote omitted; emphasis added).

[128] Article 7.48(2) EU-Korea FTA.

[129] But see Horizontal Provisions, note 25.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

measures. The PAFTA offers an example of a more balanced framework on privacy that accommodates varying perspectives. It provides in Article 13.8(2): 'To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies.'

Such a provision will provide ample opportunity for WTO members to discuss appropriate principles and guidelines in relevant institutions as well as accommodate evolving norms in this field.[130] Further, such a provision does not inhibit members from undertaking institutional innovations to protect privacy beyond the basic requirements, provided they are not arbitrary or discriminatory in nature.[131]

Additionally, WTO members should be encouraged to use the mechanism available under Article VII GATS to develop mutual recognition schemes for privacy certifications of different members to ensure greater interoperability within the multilateral system. However, in the short run, they are likely to be bilateral or regional initiatives between like-minded members till greater consensus evolves on privacy issues. Finally, WTO could liaise with institutions dealing with international cooperation for development of privacy rules/standards and cross-jurisdictional privacy enforcement, such as International Conference of Data Protection and Privacy Commissioners.

4 Incorporating Consumer Trust Enhancing Measures

Consumer trust is a fundamental requirement for digital trade. This requires not only strong domestic laws but also persistent international cooperation and engagement across relevant stakeholders, such as private companies, consumer advocacy organisations and consumer protection agencies. Further, the types of risks faced by consumers is also changing in a digital world and includes dangerous cybercrimes, such as distributed denial of service attacks, phishing attacks, hacking, identity theft and cyberstalking.[132] Dealing with these issues requires WTO's engagement with other relevant institutions, such as the International Consumer Protection Enforcement Network, UNCITRAL and other regional bodies with expertise on consumer protection issues, such as the OECD.

[130] Some have argued for an international treaty on data protection under the auspices of the WTO – this would exceed the competence of the WTO. See generally J. R. Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace', *Stanford Law Review* 52 (2000), 1359–1362, at 1315.

[131] See generally D. A. Hyman and W. E. Kovacic, 'Implementing Privacy Policy: Who Should Do What?', *Fordham Intellectual Property, Media and Entertainment Law Journal* 29 (2019), 1117–1149.

[132] OECD, *Consumer Protection in E-Commerce: OECD Recommendations* (Paris: OECD Publishing, 2016), at paras. 48–49. See also Interpol, Cybercrime, available at www.interpol.int/Crimes/Cybercrime.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press

WTO rules do not address online consumer protection issues directly and, hence, we recommend new rules to integrate this dimension in WTO framework. First, all WTO members should be required to adopt a basic regulatory framework on online consumer protection, including providing sufficient remedies to e-commerce users and ensuring that businesses provide adequate quality of digital products. The UNCITRAL Model Law on Electronic Commerce could be incorporated by reference in WTO law. Second, WTO members should adopt a mandatory cooperation mechanism for addressing the transnational aspects of online consumer protection, including information sharing and providing assistance for cross-border enforcement of consumer protection laws.[133] Implementing such provisions might require systematic changes to domestic laws of several developing countries and, therefore, they might need technical assistance, as earlier noted.

Several PTAs already contain provisions on online consumer protection, although many of them are non-binding.[134] Further, these provisions are loosely worded and do not incentivise countries to develop meaningful cooperation on online consumer protection issues. Being a multilateral institution, the WTO is better placed to facilitate increased dialogue between consumer protection (and other relevant) regulators to ensure effective international cooperation in the field.

5 Enabling Digital Innovation and Promoting Business Trust

WTO rules should also incorporate mechanisms to improve business trust to support a data-driven economy. For example, interoperable and transparent standards in data regulation can facilitate business trust. To achieve this, WTO members could consider adoption of TBT-like disciplines in context of trade in services. For instance, all members should be required to adopt only such technical standards in their digital services that are consistent with internationally recognised standards.[135] Further, unreasonable standards constituting unnecessary barriers to trade and more burdensome than necessary to achieve a policy objective such as ensuring privacy or security should be prohibited.[136] Such provisions could reduce the use of indigenous domestic standards that disrupt data flows.

WTO members could also be required to consider/use only internationally recognised standards in framing domestic regulations, including imposing standards for data security and privacy.[137] This obligation could be difficult to implement in

[133] See OECD, *Consumer Protection Enforcement in a Global Digital Marketplace* (Paris: OECD Publishing, 2018), at 10.

[134] Article 19.7(3) USMCA.

[135] In the context of definition of 'international standardizing body' in the TBT, see Appellate Body Report, *United States – Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products*, WT/DS381/AB/R, adopted 16 May 2012, at paras. 353, 357, 359.

[136] See, e.g., Article 2.2 TBT.

[137] See Annex 8-B, Section A CPTPP.

practice because multi-stakeholder and private sector–driven standards are prominently used in data operations but have little recognition in WTO law. For example, the data routing architecture of the Internet is largely based on protocols established by the Internet Engineering Task Force (IETF), a multi-stakeholder organisation developing voluntary Internet standards. Similarly, cybersecurity standards are largely developed by private sector. In fact, experts argue that Internet-related standards function better when they are open and driven by market competition rather than unilateral measures.[138] To address this gap, an arrangement similar to the TBT Code of Good Practice could be adopted in context of GATS.[139] This would provide an opportunity for private or multi-stakeholder standards to gain greater recognition at the WTO while ensuring that these standards are being formulated with transparency, participation and accountability.[140] For example, the International Organization for Standardization (ISO), a private standard-setting organisation, has a strong partnership with WTO and plays an instrumental role in harmonising standards in goods through contributions to the WTO committee meetings and providing reports to WTO members.[141]

Additionally, certain PTAs, such as the CPTPP and USMCA, include provisions to enhance business trust in the context of digital services by protecting the source code and vital digital assets of foreign companies from unauthorised disclosure.[142] In the USMCA, this provision is extremely broad and prohibits governments from requiring access to both source code and algorithms as a condition of market access.[143] However, similarly worded provisions can pose problems in the multilateral context because (i) many developing countries consider technology transfer as an important prerequisite for bridging the existing digital divide between developing and developed countries (an issue requiring further debate and negotiations);[144] and (ii) certain countries fear that algorithms and technical codes underlying digital services may be discriminatory, insecure or allow unauthorised data access to certain countries or groups, and therefore, should be scrutinised further.[145]

To address the above concerns, we recommend a provision in WTO law that would prohibit forced disclosure of source code and algorithm, but subject to an

[138] OECD, OECD Guidelines for Cryptography Policy, adopted on 27 March 1997, available at www.oecd.org/sti/ieconomy/guidelinesforcryptographypolicy.htm#preface.

[139] Annexes 3 and 4 TBT.

[140] See Annex 3 TBT. See also WTO ISO Standards Information Gateway: List of Standardizing Bodies, available at https://tbtcode.iso.org/sites/wto-tbt/list-of-standardizing-bodies.html.

[141] See generally S. Charnovitz, 'International Standards and the WTO', GW Law Faculty Publications and Other Works Paper No 394 (2005).

[142] Article 19.16 USMCA; Article 14.17 CPTPP.

[143] Article 19.16(1) USMCA.

[144] See generally R. S. Neeraj, 'Trade Rules on Source Code – Deepening the Digital Inequities by Locking Up the Software Fortress', Centre for WTO Studies Working Paper CWS/WP/200/37 (2017), 1–37, at 25–36.

[145] See generally B. Goodman and S. Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"', *AI Magazine* 38 (2017), 50–57.

exception allowing governments to access this information for regulatory purposes, such as checking for discriminatory algorithms, auditing security of digital services and for judicial proceedings or governmental investigations.[146] Article 19.16(2) USMCA is a good example as it has been carefully constructed to ensure that governments can access source code and algorithms for regulatory purposes, such as checking for discriminatory algorithms, for patent applications/disputes,[147] for criminal investigations, and auditing security standards of digital services as part of domestic investigations or inspections. However, it does not specify that parties could be required to modify the source code, for example, when an investigation reveals that a company has violated domestic laws or if the security standards are below par, or where the algorithms are discriminatory.

6 Relevance of Special and Differential Treatment for Developing Countries and LDCs

Certain developing countries have claimed that data restrictive measures are necessary to develop their domestic digital sector and protect their economic and social interests, for instance preventing tariff losses resulting from the moratorium on customs duties on electronic transmissions. The WTO is an excellent forum for developing countries to present evidence on the benefits of data restrictive measures in the short run vis-à-vis the losses to their domestic consumers and businesses as well as other measures necessary to promote greater digital inclusion. However, where exceptions are made for developing countries and LDCs to impose data restrictive measures, such as through special and differential treatment, they should be evidence-based and time-bound.

Certain developing countries and LDCs may have inadequate capacity to enforce a framework for data regulation due to insufficient expertise on privacy and cybersecurity. Such members should be provided additional time to make a binding commitment on data flows. For instance, the Trade Facilitation Agreement allows for staggered implementation of obligations, so as to provide more time to developing countries and LDCs to initiate reforms in their domestic system before being fully bound.[148] Further, WTO members should also agree on mandatory technical assistance programmes and capacity-building support for developing countries and LDCs with inadequate regulatory capacity on relevant issues. None of the PTAs deal with development-related concerns in digital trade, particularly enforcing stronger obligations on developed partners to assist developing countries and LDCs. This deficiency can, however, be addressed better through the ongoing WTO plurilateral

[146] See, e.g., Article 19.16(2) USMCA.
[147] Article 14.17(4) CPTPP.
[148] See WTO, UNCTAD E-Commerce Week: Summary of the Session 'Digital Trade as If Development Mattered', Communication from Cambodia and Japan, JOB/GC/185, 27 April 2018.

initiative, which also brings together several developing countries and LDCs (e.g. under the Friends of E-commerce for Development.)

III *The Path Ahead for Rules on Data Flows at the WTO*

WTO members are currently considering two separate mechanisms to reform WTO rules on electronic commerce. First, GATS itself could be reformed using existing mechanisms. For example, under Article XVIII GATS, members could adopt additional commitments on data flows, akin to the Telecommunications Reference Paper.[149] WTO members could also consider adopting dedicated domestic regulations on electronic commerce under Article VI GATS. Certain members have argued for expanding existing GATS commitments on digital services, particularly for computer and related services, where commitments should be made at a two-digit level to increase the scope of commitments.[150] Second, under the joint statement initiative initiated in the last WTO Ministerial Conference and the follow-up negotiations launched at the Davos conference, members are considering a plurilateral agreement on electronic commerce covering different digital trade issues, including data flows and data localisation. The more likely outcome is the adoption of a plurilateral agreement containing electronic commerce–specific rules, like the electronic commerce/digital trade chapters in certain recent PTAs, such as the USMCA and CPTPP.

Despite WTO members making various proposals for reform under the joint statement initiative (including some reforms that we propose in this article), constraints exist in achieving these reforms in practice. First, as regards regulating data, WTO members have varied views; as discussed earlier, while some members support the incorporation of provisions on the free flow of data, others have refrained from this approach to safeguard policy objectives, such as privacy protection, Internet sovereignty and cybersecurity. Aaronson and Leblond argue that the varying approaches to data regulation has resulted in three different 'data realms', reflecting the policy orientation of the United States, China and EU.[151] Implementing a horizontal provision on cross-border data flows and prohibition on data localisation may therefore be difficult to achieve in practice, at least in the short run. The divided approach in data regulation could be one of the key reasons why countries prefer to address data-related rules in PTAs rather than at the WTO, as PTAs provide them greater flexibility in devising rules consistent with their domestic regulatory objectives.

[149] Mitchell and Mishra, note 9, at 1127.

[150] See, e.g., WTO, GATS 2000: Computer and Related Services (CPC 84), Communication from the European Union, S/CSS/W/34/Add.1, 15 July 2002, at para. 10.

[151] S. A. Aaronson and P. Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO', *Journal of International Economic Law* 21 (2018), 245–272, at 245.

Second, the deficiency of binding international frameworks on cybersecurity, online consumer and data/privacy protection poses a major challenge in facilitating cross-border data flows, and may further breed mistrust among countries. Therefore, even if reformed WTO rules required all members to adopt basic frameworks on privacy protection, online consumer protection, and cybersecurity consistent with international standards, legal uncertainty will arise with regard to the appropriate international standard(s) in these areas of regulation. As it is outside the scope of the WTO to set standards or norms in these areas, the success of the proposed rules on privacy, cybersecurity and other related areas is contingent on the development of robust approaches in non-trade fora, including relevant regional, transnational and multistakeholder bodies.

Third, the emerging voice of developing countries and LDCs, especially with regard to special and differential treatment in implementing trade commitments on electronic commerce, might face some opposition at the WTO. Given the political backlash against certain countries misusing their 'developing country' status, some members might object to introducing a development dimension in provisions on data flows. However, as indicated in our proposal, further studies are necessary to understand the development implications of data-driven growth, including the regulatory capacity of developing countries/LDCs to respond to these challenges and introduce relevant provisions accordingly.

Finally, the extent to which the existing architecture of GATS can accommodate new rules on data flows is unclear. For example, if a new plurilateral agreement were to be designed, WTO members would have to determine the legal relationship between this agreement and GATS, including whether the existing GATS commitments would apply.[152] Similarly, given the uncertainty in applying the general exceptions in the context of data restrictive measures,[153] further dialogue is necessary among the WTO members to clarify on the scope/applicability of the exceptions applicable to data restrictive measures.

Despite these constraints, we propose that the WTO can and should play a central role in devising trade rules for the digital age. Although the electronic commerce chapters in PTAs can fill gaps in WTO rules on digital trade in the short run, they are likely to divide the global framework for data regulation, as is already evident in the divergent approaches taken by countries on data flows and data protection in their PTAs. Further, certain areas of reform proposed in this article require a high level of international regulatory cooperation. The WTO, with its widespread worldwide membership, is much better suited to act as a site for facilitating such international regulatory cooperation as compared to regional bodies.[154] Further, as

[152] Mitchell and Mishra, note 9, at 1128–1129.

[153] N. Mishra, 'Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?', *World Trade Review* 19 (2019), 1–24, at 1.

[154] J. P. Meltzer, 'A WTO Reform Agenda: Data Flows and International Regulatory Cooperation', Global Economy and Development Working Paper 130 (2019), at 17–18.

suggested by the increased vigour of negotiations under the joint statement initiative, WTO members have shared interests in promoting digital trade. Given the central role of data flows in the digital economy, sufficient incentives therefore exist for WTO members to engage in negotiating rules on cross-border data flows and related issues. Therefore, we believe that despite certain pragmatic and political constraints, our proposed WTO framework on data flows remains both relevant and timely.

E CONCLUSION

The future of trade in digital services and data entails complex and uncertain policy challenges.[155] Thus, balancing different regulatory concerns is fundamental to ensure a coherent and sustainable regulatory framework for data flows. Being the leading multilateral trade institution, the WTO is well placed to undertake several of the required reforms to bring about better balance between promoting free flow of data while protecting a secure and stable regulatory environment for data and addressing commercial interests of consumers and businesses. However, the WTO cannot deal with all pertinent issues related to data transfer, or act on its own. Instead, the WTO needs to reframe its policy approach to engage with more relevant international and multi-stakeholder institutions and develop disciplines that address relevant dimensions of data regulation.

In this article, we recommend a comprehensive framework on data flows that covers a large range of areas that is atypical of most existing international trade agreements. Our recommendations are more comprehensive than the disciplines incorporated in the USMCA and CPTPP. However, as digital trade continues to grow, WTO law will need to respond to new policy challenges arising with increased data flows. In order to do so, WTO members must consider a comprehensive and balanced regulatory framework, where provisions for free cross-border data flows and prohibition on data localisation are complemented with relevant disciplines on online consumer protection, privacy and cybersecurity. Such an approach would facilitate openness as well as business and consumer trust in digital trade. This framework should also include rules addressing the specific needs of developing countries and LDCs to enable their inclusion into the digital economy. Although such a comprehensive framework will require increased participation, goodwill and commitment of countries, particularly under the ongoing joint statement initiative at the WTO, we believe it can eventually be more meaningful and sustainable.

[155] Shackelford et al., note 106, at 429.

https://doi.org/10.1017/9781108919234.006 Published online by Cambridge University Press