World Trade Review (2020), **19**, 341–364
doi:10.1017/S1474745619000120

ORIGINAL ARTICLE

Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?

Neha Mishra

Melbourne Law School
Email: mishra.neha@gmail.com

(First published online 2 May 2019)

Abstract

Measures restricting data flows outside one's borders, including mandatory data/server localization measures, are not only a barrier to trade, but also largely ineffective in achieving better internet security or trust. Nevertheless, governments deploy such measures, primarily on grounds of cybersecurity and privacy, potentially violating their obligations under the General Agreement on Trade in Services (GATS). In this article, I investigate whether GATS-inconsistent measures may be justified under GATS Art. XIV when aimed at ensuring privacy or cybersecurity, and, if so, whether GATS Art. XIV effectively balances trade and internet policy. As the internet governance framework is complex and somewhat ambiguous, applying GATS Art. XIV to cybersecurity/privacy measures necessitates balancing of trade liberalization principles and domestic internet policy. This exercise can be effective in weeding out data localization measures disguised as privacy/cybersecurity measures, particularly by employing relevant technical and factual evidence. However, given the lack of binding international law/norms on these issues, GATS Art. XIV has a limited role, particularly in cases involving direct conflict between multistakeholder/transnational internet norms and domestic internet policies, or where the measures are founded on contentious standards/benchmarks on privacy/cybersecurity. Ultimately, ensuring free and secure data flows requires a multidimensional policy response, including strengthening linkages between trade law and internet governance.

1. Introduction

Data localization is one of the most contentious and challenging policy issues in digital trade today.[1] Chander and Le define data localization to include any measure 'that specifically encumber(s) the transfer of data across national borders'.[2] In a legislative proposal on cross-border data flows, the European Commission defines data localization as 'any obligation, prohibition, condition, limit or other requirement' contained in the 'laws, regulations or administrative provisions of the Member States, which imposes the location of data storage or other processing requirements in the territory of a specific Member State or hinders storage or other processing of data in any other Member State'.[3] Following these broad definitions, in this article a variety of

I gratefully acknowledge the support of the Australian Government Research Training Program Scholarship and the Competitive Additional Funding received from Melbourne Law School. I thank Tania Voon, Andrew Mitchell, Victor do Prado, Nikitas E Hatzimihail, Yannis Voudouris, and fellow panellists and participants at the 7th PEPA-SIEL Conference 2018, and two anonymous reviewers for the World Trade Review for their very helpful comments and insights on earlier drafts of this article.

[1]See, e.g., A. G. Martinez, 'The End of Data without Borders', *The Wired* (1 February 2018); K. Komaitis, 'The "Wicked Problem" of Data Localization', 3(2) *Journal of Cyber Policy* (2017), 355.

[2]A. Chander and U. P. Le, 'Data Nationalism', 64 *Emory Law Journal* (2015), 677, 680.

[3]See European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Framework for the Free Flow of Non-Personal Data in the European Union', Doc. no. 2017/0228 (COD) (13 September 2017), Art. 3(5).

laws and regulations restricting data flows outside one's borders, whether directly or indirectly, are included within the scope of data localization. For example, explicit data residency laws requiring data to be stored[4] and/or processed[5] in domestic servers,[6] and even routed within the territory during transit,[7] fall within the scope of data localization. Further, implicit restrictions including cross-border data flow restrictions on grounds of privacy or data protection,[8] cybersecurity[9] and law enforcement[10] could indirectly force localization by imposing impracticable regulatory requirements or unreasonable compliance costs.

Data localization is premised on the logic that the degree of governmental control over data processing, access, and transfer significantly increases once data are located within one's borders. As data are a highly valuable resource in the digital economy,[11] several countries increasingly attempt to confine data within their borders to increase economic profits.[12] Further, many countries believe that domestic laws and regulations can be enforced easily when data reside in local servers; for example, compliance with domestic privacy laws or obtaining data access for criminal investigations.[13] Since the Snowden revelations in 2013 (exposing the massive digital surveillance of the US government), several countries have also advocated data localization for protecting national sovereignty, including national security, and preventing breach of their citizens' privacy through foreign surveillance.[14] In practice, however, a country might have multiple policy

[4]See, e.g., Портал персональных данных Уполномоченного органа по защите персональных данных [Federal Law no. 242-FZ of 21 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] (Russia), 'Russian Data Localisation Law', Art. 18(5).

[5]For example, in the European Union data storage includes data processing. See W. K. Hon *et al*., 'Policy, Legal and Regulatory Implications of a Europe-only Cloud', 24 *International Journal of Law and Information Technology* (2016), 251, 259.

[6]Sometimes, a data localization measure may not prohibit cross-border transfer although it may necessitate localization. See, e.g., Russian Data Localization Law. See also L. Tuthill, 'Cross- border Data Flows: What Role for Trade Rules?', in P. Sauvé and M. Roy (eds.), *Research Handbook on Trade in Services* (Cheltenham: Edward Elgar, 2016), pp. 357, 363.

[7]For example, a Schengen routing plan was proposed by Germany requiring all personal data of EU residents to be only routed through the EU. See P. Bank, 'Deutsche Telekom: "Internet Data made in Germany Should Stay in Germany"', *DW: Made for Minds* (18 October 2013), www.dw.com/en/deutsche-telekom-internet-data-made-in-germany-should-stay-in-germany/a-17165891.

[8]See, e.g., *Regulation 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*, Regulation (EU) 2016/679 of the European Parliament and of the Council [2016] OJ L119 (1 May 2018) (GDPR). In this paper, I use privacy and data protection interchangeably, particularly while referring to legislative frameworks.

[9]See, e.g., J. Wagner, 'China's Cybersecurity Law: What You Need to Know', *The Diplomat* (1 June 2017), https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/.

[10]See, generally, Chander and Le, 'Data Nationalism', supra n. 2, at 730–734; M. F. Ferracane, 'Restrictions to Cross-Border Data Flows: A Taxonomy', ECIPE Working Paper no. 1/2017, European Centre for International Political Economy (November 2017), 6.

[11]'The World's Most Valuable Resource is no Longer Oil, but Data', *The Economist* (6 May 2017), www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[12]See, e.g., Communication from the African Group, 'Work Programme on Electronic Commerce', Report of Panel Discussion on 'Digital Industrial Policy and Development', WTO Doc. JOB/GC/133 (21 July 2017).

[13]See, generally, Shin-yi Peng and Han-wei Liu, 'The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?', 51(2) *Journal of World Trade* (2017), 183, 199. See also A. Mcquinn and D. Castro, 'How Law Enforcement Should Access Data Across Borders', Information Technology and Information Foundation (July 2017), 1, 2; W. K. Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction through a Cloud Computing Lens* (Cheltenham: Edward Elgar, 2017), pp. 48–49. For historical discussion on this issue, see D. R. Bender, 'Transborder Data Flow: An Historical Review and Considerations for the Future', 79(3) *Special Libraries*, 230–235.

[14]S. Aaranson, 'Why Trade Agreements are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security', 14(4) *World Trade Review* (2015), 671, 674, 682–685; J. F. Hill, 'The Growth of Data Localization Post-Snowden: Analysis and Recommendations for US Policymakers and Business Leaders', Paper presented at Conference on the Future of Cyber Governance, The Hague Institute for Global Justice (1 May 2014).

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

considerations behind a data localization measure, including conveniently hiding its protectionist intent behind legitimate public policy rationales.[15]

By impeding cross-border data flows, data localization measures disrupt various activities in the global supply chain. A broad variety of services and goods manufacturing processes incorporate digital elements such as cloud computing, big data processing, and artificial intelligence.[16] By creating barriers to data flows, therefore, data localization measures also create barriers to trade. For example, a data localization law forcing local data storage or processing increases compliance costs for foreign service providers and reduces market access, particularly for small and medium-sized enterprises (SMEs).[17] In other cases, even when the data localization requirement is not explicit, certain regulatory requirements (such as compliance with stringent technical standards) make cross-border data transfers impracticable.

Data localization measures are subject to rules under international trade agreements, particularly the *General Agreement on Trade in Services* (GATS)[18] as they affect the 'production, distribution, marketing, sale and delivery' of various internet and internet-enabled services.[19] Applying GATS to data localization measures raises several questions such as the sectors affected by the measure, relevant commitments in that sector, and the nature and extent of violations including obligations on non-discrimination, market access, and domestic regulations, and the justification of such measures under GATS exceptions: the general exception (GATS Art. XIV) and the national security exception (GATS Art. XIV bis).[20] This article focuses on one key aspect of the above assessment: presuming a data localization measure violates a Member's GATS obligations, how does GATS Art. XIV apply if the Member desires to justify the measure on grounds of cybersecurity or privacy? Does GATS Art. XIV adequately safeguard the Member's right to take measures on these grounds? Can GATS Art. XIV achieve a sound balance between trade and internet policy? The focus is primarily on privacy and cybersecurity as they are the most commonly proffered rationales for implementing data localization measures.[21] This article does not directly address other issues, such as online censorship,[22] data access for domestic legal enforcement and investigations,[23] as well as justification of data localization under GATS Art. XIV bis (national security exception).[24]

[15]See N. Mishra, 'Data Localization Laws in a Digital World', *Public Sphere* (2016), 136, 144–151.

[16]J. Manyika *et al*., 'Digital Globalization: The New Era of Global Flows', McKinsey Global Institute (March 2016), www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows, 1. See also UNCTAD, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development', United Nations (2016), http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf, xi.

[17]M. Bauer *et al*., 'The Costs of Data Localisation: Friendly Fire on Economic Recovery', ECIPE Occasional Paper 3/2014 (2014), 10.

[18]Marrakesh Agreement Establishing the World Trade Organization (opened for signature 15 April 1994), 1869 UNTS 183 (entered into force 1 January 1995), annex 1B, General Agreement on Trade in Services (GATS).

[19]GATS Art. I: 1 read with Art. XXVIII(b).

[20]See, generally, D. Crosby, 'Analysis of Data Localization Measures under WTO Services Trade Rules and Commitments', Policy Brief, E15 Initiative (March 2016); generally, A. Mitchell and J. Hepburn, 'Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer', 19 *Yale Journal of Law & Technology* (2017), 182.

[21]S. Aaronson, 'What Are We Talking About When We Discuss Digital Protectionism?', Working Paper, Economic Research Institute of Asia (July 2017), 14.

[22]See, generally, T. Wu, 'The World Trade Law of Censorship and Internet Filtering', 7 *Chicago Journal of International Law* (2006), 263; B. Hindley and H. Lee-Makiyama, 'Protectionism Online: Internet Censorship and International Trade Law', ECIPE Working Paper 12/2009, ecipe.org/publications/protectionism-online-internet-censorship-and-international-trade-law.

[23]See, generally, Komaitis, 'The "Wicked Problem" of Data Localisation', supra n. 1, at 355; Mcquinn and Castro, 'How Law Enforcement Should Access Data Across Borders', supra n. 13; J. Selby, 'Data Localization Laws: Trade Barriers, Legitimate Responses or Cybersecurity Risks, or Both?', 25 *International Journal of Law & Information Technology* (2017), 213.

[24]See, generally, Shin Yi Peng, 'Cybersecurity Threats and the WTO National Security Exceptions', 18 *Journal of International Economic Law* (2015), 449.

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

Section 2 discusses the various technical and economic aspects of data localization, and comments on the general utility of data localization as a tool for cross-border data regulation. I argue that although data localization measures are technologically and economically inefficient, several governments strongly believe in (or at least advocate) their effectiveness in achieving domestic policy goals. Section 3 reflects on the various perspectives on privacy and cybersecurity, both from a domestic public policy perspective and in context of the multistakeholder internet governance community. I argue that the framework for regulation of cross-border data flows is complex and ambiguous because perspectives on internet privacy and cybersecurity at the international/transnational and domestic level are distinct and often conflicting. Given this complex policy environment, Section 4 investigates the application of Art. XIV to data localization measures, and whether it balances trade liberalization with cybersecurity and privacy considerations. I emphasize that the application of GATS Art. XIV essentially entails an assessment of cybersecurity and privacy issues from a domestic policy point of view, rather than multistakeholder norms in internet governance. Thus, the balance sought under GATS Art. XIV is between trade liberalization obligations and a Member's understanding of privacy and cybersecurity.

Section 5 argues that GATS Art. XIV can achieve the desired balance between trade liberalization and domestic public policy; for example, when applied thoughtfully considering relevant technical and factual evidence and thoroughly examining if certain cybersecurity/privacy measures have a hidden protectionist intent. Experts in the internet technical and policy community (including the Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), Internet Governance Forum (IGF), Internet Corporation for Assigned Names and Numbers (ICANN) or even the International Telecommunications Union (ITU) can provide relevant inputs regarding how data flows occur in digital networks, and whether specific measures/standards are effective in achieving security or privacy, at least from a technological standpoint. However, in the absence of international consensus on cybersecurity and internet privacy, the effectiveness of GATS Art. XIV in assessing legitimacy of data localization measures is inevitably limited. For example, where data localization measures are imposed in violation of multistakeholder norms/principles in internet governance, WTO panels have limited scope to consider the relevance of these norms/principles as they are largely not legally binding. Similarly, examining measures based on contentious standards or benchmarks on privacy and/or cybersecurity raises complex technical questions that WTO panels cannot usually address.

Section 6 concludes that although GATS Art. XIV remains an important and effective tool in fighting growing digital protectionism, it cannot and should not operate in a vacuum. Moving forward, when developing solutions to address data localization or other restrictions on data flows, both domestic policymakers and international trade institutions, such as the World Trade Organization (WTO), should remain wary of placing excessive emphasis on disciplines in GATS or other international trade agreements, and instead work towards developing a more balanced, multidimensional framework addressing various facets of internet and data regulation.

2. Data Localization: An Efficient Tool for Data Regulation?

The rapid adoption of data localization has triggered extensive debates on their effectiveness to achieve public policy goals such as protecting privacy of individuals and enhancing security of data and the networks carrying these data. From a technical perspective, geographical prescriptions on data flows and data storage contradict the fundamental end-to-end architecture of the internet that requires unhindered and instantaneous flow of data across the network, irrespective of the origin or content of the data.[25] Further, data routing is autonomous because the underlying technical protocols move data through the most efficient route rather than aligning with

[25]S. Garfinkel, 'The End of End-to-End?', *MIT Technology Review* (1 July 2003); Hon, *Data Localization Laws and Policy,* supra n. 13, at 32, 105.

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

territorial boundaries.[26] Therefore, data localization artificially interferes with the technical and logical infrastructure of the internet and affects its reliability as a platform for transferring data.

From the perspective of economic efficiency, data localization measures also have undesirable consequences for all concerned stakeholders – governments, businesses, and consumers. First, data localization measures can hurt a country's economy by reducing productivity of services, and increasing prices for all.[27] Second, monitoring whether service providers comply with data localization laws requires governments to inefficiently expend resources[28] to achieve rather impracticable outcomes, particularly because: (i) data are instantaneously transferred through multiple locations of the world in nanoseconds, making it almost impossible to track the exact location of specific data points in real-time;[29] (ii) the end goal of achieving greater data security or protection is not contingent on the location of the data, as envisaged under a data localization measure but rather on the underlying technical protocols and designs of digital services.[30] For example, if the encryption mechanism of a digital service is weak, user privacy can be compromised irrespective of the server location; similarly, if a cloud service provider does not provide robust security, its servers remain susceptible to cyberattacks, even if a government forces the provider to locate its server farms within its borders.

Data localization increases compliance and operational costs for foreign providers of digital services as they are forced to build local servers or use local services in all implementing countries, foregoing the network economies of scale.[31] For example, instead of efficiently managing data distribution through continuous back-end transactions across multiple global/regional servers, companies are required to synchronize their data distribution with fewer domestic servers with increased chances of overloading and security breaches.[32] Further, foreign companies bear a significant increase in transaction costs to comply with stringent and restrictive standards of privacy or security that prevent interoperability across the global supply chain.[33] For instance, data protection laws containing extensive requirements to obtain consent from individual users and/or appropriate authorities for use/processing or transfer of data significantly increase compliance costs for companies.[34] Further, domestic companies that depend on or use digital services as well as end consumers have reduced access to competitive foreign services and lose significant business and other opportunities.[35]

Given that data localization measures are economically inefficient and even disruptive, several policy communities are concerned about the sharp rise in such measures, particularly since 2013.[36] This includes the internet technical and policy community, consisting of various

[26]R. Barnes *et al*., *Technical Considerations for Internet Service Blocking and Filtering*, RFC 7754, Internet Engineering Task Force (March 2016), 12.

[27]See Bauer *et al*., 'The Costs of Data Localisation', supra n. 17.

[28]See, e.g., H. Lovells, 'Russia Releases 2017 Data Privacy Inspection Plans: Microsoft Passes 2016 Inspection' (19 January 2017), www.hldataprotection.com/2017/01/articles/international-eu-privacy/russia-releases-data-privacy-inspection-plans-for-2017-microsoft-passes-2016-inspection/; 'Russia's Personal Data Localization Law: Expanding Enforcement', Lexology, TFM Group (27 April 2016).

[29]Hon, *Data Localization Laws and Policy*, supra n. 13, at 100; T. Sargsyan, 'Data Localization, and the Role of Infrastructure for Surveillance, Privacy and Security', 10 *International Journal of Communications* (2016), 2221.

[30]For a discussion on the technological efficiency of data localization measures, see Section 4.2.2.

[31]I. Mihaylova, 'Could the Recently Enacted Data Localization Requirements in Russia Backfire?', 50(2) *Journal of World Trade* (2016), 313, 317–319; Hon, *Data Localization Laws and Policy*, supra n. 13, at 112–114; Leviathan Security Group, 'Quantifying the Costs of Forced Localization' (2015), https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf, 3.

[32]R. Bennett, 'Surge in Data Localization Laws Spells Trouble for Internet Users on *TechPolicyDaily.com* (10 May 2016), www.aei.org/publication/surge-in-data-localization-laws-spells-trouble-for-internet-users/.

[33]Mihaylova, 'Could the Recently Enacted Data Localization Requirements in Russia Backfire?', supra n. 31, at 313, 317–319.

[34]See, e.g., GPPR, Arts. 6–9, 22.

[35]Mihaylova, 'Could the Recently Enacted Data Localization Requirements in Russia Backfire?', supra n. 31, at 313, 317–319; Hon, *Data Localization Laws and Policy*, supra n. 13, at 112–114.

[36]Hill, 'The Growth of Data Localization Post-Snowden', supra n. 14.

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

multistakeholder organizations involved in internet governance;[37] trade institutions such as the WTO;[38] human rights bodies;[39] as well as few governments, particularly digital leaders such as Japan and the US.[40] Amongst the recurring concerns against data localization are fragmentation of the global network of the internet into inefficient, localized internets;[41] rise in digital protectionism leading to reduced economic opportunities and productivity;[42] and an increase in online surveillance and oppressive censorship.[43]

On the other hand, certain governments advance strong policy rationales to justify data localization. Countries such as China and Russia propagate the need for increased sovereign control over domestic cyberspace (or what China has re-branded as cyber sovereignty).[44] Others have advocated the need for data localization to achieve more specific objectives such as protecting data and network security (without necessarily distinguishing it from national security),[45] preventing cybercrimes, assisting in domestic investigations and law enforcement, and compliance with domestic laws such as privacy and intellectual property laws.[46] However, very rarely do countries admit that their data localization measure has a protectionist rationale, although this is often the case in practice, irrespective of how the measure is framed.[47] As will be discussed later in Sections 4 and 5, GATS Art. XIV can facilitate detecting the disguised protectionist rationale behind data localization measures.

[37]The internet technical and policy community consists of organizations such as Internet Governance Forum (IGF), Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), Internet Corporation for Assigned Names and Numbers (ICANN), and Internet Society (ISOC). Further, civil society organizations and technology companies are also often active members of the internet governance community, participating through several of the above bodies. See, e.g., discussion at IGF 2017 on 'Digitalization and International Trade' (19 December 2017), www.youtube.com/watch?v=O7f5h6eTn8w.

[38]See discussion of electronic commerce at the WTO in D. Crosby, 'E-commerce and Digital Trade for Development: Negotiations to Soft Launch at MC11', E15 Initiative (October 2017), http://e15initiative.org/blogs/e-commerce-and-digital-trade-for-development-negotiations-to-soft-launch-at-mc11/. See also Conference Notes, *Conference on the Use of Data in the Digital Economy* (2 and 3 October 2017), Geneva, www.wto.org/english/res_e/reser_e/datadigitalc17notes_e.pdf.

[39]See, e.g., K. M. Yilma, 'The "Right to Privacy in the Digital Age": Boundaries of the "New" UN Discourse', 87(4) *Nordic Journal of International Law* (2018), 485–528 (discussing the UN General Assembly resolutions on digital privacy). See also Access Now, 'The Impact of Forced Localisation on Human Rights' (4 June 2014), www.accessnow.org/the-impact-of-forced-data-localisation-on-fundamental-rights/. See also A. Chander, 'International Trade and Internet Freedom', 102 *American Society of International Law Proceedings* (2009), 37.

[40]WTO, *Work Programme on Electronic Commerce – Non-paper from the United States*, WTO Doc. JOB/GC/94 (4 July 2016) [2.3]; WTO, *Work Programme on Electronic Commerce – Non-Paper for the Discussions on Electronic Commerce/Digital Trade from Japan*, WTO Doc. JOB/GC/100 (25 July 2016) [2.2].

[41]See, generally, W. J. Drake *et al.*, 'Internet Fragmentation: An Overview', Future of the Internet Initiative White Paper, World Economic Forum (January 2016); Global Commission on Internet Governance, 'One Internet', CIGI and Chatham House (2016).

[42]See, e.g., WTO, *Work Programme on Electronic Commerce – Non-paper from the United States*, supra n. 40; WTO, *Work Programme on Electronic Commerce – Non-Paper for the Discussions on Electronic Commerce/Digital Trade from Japan*, supra n. 40.

[43]Sargsyan, 'Data Localization, and the Role of Infrastructure for Surveillance, Privacy and Security', supra n. 29, at 2221.

[44]S. Shackelford and F. Alexander, 'China's Cyber Sovereignty: Paper Tiger or Rising Dragon?', *Asia & the Pacific Policy Society* (18 January 2018), www.policyforum.net/chinas-cyber-sovereignty/. See also L. DeNardis *et al.*, 'The Rising Geopolitics of Internet Governance: Cyber Sovereignty v. Distributed Governance', Paper presented at Columbia SIPS Tech & Policy Initiative, Columbia SIPA (November 2016).

[45]D. Broeders, *The Public Core of the Internet: Towards an International Agenda for Internet Governance*, Amsterdam University Press (2016), p. 13; DeNardis *et al.*, 'The Rising Geopolitics of Internet Governance', supra n. 44, at 16–17.

[46]See, generally, Mitchell and Hepburn, 'Don't Fence Me In', supra n. 20, at 182, 188–195.

[47]Bauer *et al.*, 'The Costs of Data Localisation', supra n. 17, at 5, 6.

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

3. Privacy and Cybersecurity as Drivers of Data Localization: Conflicting Perspectives

Cybersecurity and data protection/privacy are perhaps the two most challenging issues in internet governance today.[48] The ubiquity of internet data flows in both economic and socio-cultural aspects of human lives also exposes us to new forms of risks, including hacking, malware, and distributed denial of service attacks, massive surveillance programmes, phishing attacks, fake news, etc. Therefore, unsurprisingly, all major stakeholders, including governments, private companies, and the internet technical community, are extremely focused on these issues. However, the perspectives of these stakeholders are often distinct and conflicting, resulting in a fragmented, complex, and uncertain regulatory environment for data flows.

The internet technical community tends to view cybersecurity and privacy as being fundamental for a free and open internet.[49] In other words, free flow of data is not considered prejudicial to online privacy or security, provided the underlying technical protocols and designs are robust and secure, and promote interoperability across the different layers of the internet, across networks, and various digital services. Further, free flow of data is only possible in networks that are secure and where the digital services providers comply with best practices in privacy and cybersecurity.[50] The internet technical community, therefore, emphasizes the importance of implementing open and transparent standards through discussions in multistakeholder fora such as the IETF and W3C rather than closed standards implemented by governments. Government-mandated digital standards not only affect openness and interoperability of the internet and data flows but are also less secure as the secrecy of the applicable standard(s) increases chances of security flaws going undetected by the internet technical community.[51]

Today, the technology industry faces immense pressure from both governments and civil society to provide secure and reliable digital services, and curb exploitation/misuse of personal data collected from internet users.[52] Typically, private companies prefer a self-regulatory approach so that they can adopt best-in-class and the most innovative security and privacy practices and technical standards, instead of being subject to excessive government regulations or prescriptive standards that restrict market access and increase compliance costs.[53] With increasing pressure from governments and civil society, however, the private sector is now showing greater openness

[48]See, generally, Global Commission on Internet Governance, 'One Internet', supra n. 41; ISOC, 'Understanding Security and Resilience of the Internet' (2013), www.internetsociety.org/sites/default/files/bp-securityandresilience-20130711.pdf; OECD, *Digital Security Risk Management for Economic and Social Prosperity*, OECD Recommendation and Companion Document (17 September 2015); J. Kulesza, *International Internet Law* (Abingdon: Routledge, 2012), 67; OECD, The *OECD Privacy Framework* (2013), www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[49]ISOC, 'Understanding Security and Resilience of the Internet', supra n. 48, at 3; OECD, *OECD Digital Economy Outlook* (OECD Publishing, 2015), p. 19; J. West, 'A Framework for Understanding Internet Openness', Centre for International Governance Innovation and Chatham House, Paper Series no. 35 (May 3016), 5; N. Mishra, 'International Trade, Internet Governance and the Shaping of the Digital Economy', ArtNet Working Paper No. AWP 618, UNESCAP (29 June 2017), 11–15.

[50]ISOC, 'Understanding Security and Resilience of the Internet', supra n. 48, at 3. See also Global Commission on Internet Governance, supra n. 41, at 2.

[51]L. De Nardis, 'Five Destabilizing Trends in Internet Governance', 12(1) *I/S: A Journal of Law and Policy* (2015), 113, 130.

[52]See, e.g., 'If Facebook Will Not Fix Itself, Will Congress?', *The Economist* (11 April 2018), www.economist.com/united-states/2018/04/11/if-facebook-will-not-fix-itself-will-congress; S. Frier, 'Facebook Plunges as Pressure Mounts on Zuckerberg Over Data', *The Bloomberg* (19 March 2018), www.bloomberg.com/news/articles/2018-03-19/facebook-s-zuckerberg-under-pressure-to-answer-for-data-breach; J. Lee, 'The Rise of China's Tech Sector: The Making of an Internet Empire' (4 May 2017), www.lowyinstitute.org/the-interpreter/rise-china-s-tech-sector-making-internet-empire; L. James, 'Tech Ethics in Practice' (20 March 2018), https://medium.com/doteveryone/tech-ethics-in-practice-44b710fbc44c.

[53]See, generally, D. D. Hirsch, 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?', 34 *Seattle University Law Review* (2011), 439; 'The Framework for Global Electronic Commerce', Principles, 1–4, https://clinton-whitehouse4.archives.gov/WH/New/Commerce/read.html; L. J. Gibbons, 'No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace', 6(3) *Cornell Journal of Law & Policy* (1997), 475; A. P. Hwa, 'Self-Regulation after WGIG', in W. J. Drake (ed.), *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance*, United Nations (2008), pp. 130–132.

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

towards a co-regulatory approach; for example, engaging in dialogues or partnering with governments to frame regulatory solutions for cross-border data flows that are reasonable, well-balanced, and promote digital innovation and growth.[54]

However, at the domestic level, several governments believe that free flow of data across national borders undermines cybersecurity and data protection, and, therefore, governments should intervene to restrict data flows across borders to safeguard their citizens against various cyber risks. For example, the EU has adopted an extensive data protection regime under the General Data Protection Regulation (GDPR); China has enforced a cybersecurity law which inter alia requires data localization;[55] Russia has an extensive data protection law which inter alia mandates data localization;[56] Australia,[57] India,[58] Turkey,[59] and Canada[60] impose data localization requirements in specific sectors. As governments remain highly suspicious of foreign companies' use of personal data and their security practices, data localization remains a feasible policy tool. However, certain countries have a much broader vision of exercising greater control over all activities in domestic cyberspace through data localization, including the information available to its citizens. This idea of control over domestic cyberspace is rhetorical as the internet is not circumscribed by territorial boundaries, and, hence, not designed to be subject to sovereign controls.[61]

The prescriptive regulatory approach envisaged by governments does not align with the multistakeholder approach envisaged by experts in the internet technical community as well as the private sector.[62] Further, even among governments, a huge divide exists on the appropriate framework for cybersecurity and privacy laws and regulations. For example, the US and EU backlash against the Chinese cybersecurity law at the WTO,[63] and the tension between data transfer mechanisms of the Asia Pacific Economic Cooperation (APEC) and the EU reflects the deep divide among countries on privacy and cybersecurity issues.[64] As the conflicts between these perspectives remain unresolved, no international consensus exists on how to synergize different standards of data protection and conflicting perspectives on cybersecurity. Consequently, governments find it tactically convenient to restrict data flows through data localization rather than attempting a middle path on these issues. This conflict has also incentivized certain governments

[54]For academic initiatives in this direction, see M. Carr, 'Public–Private Partnerships in National Cyber-security Strategies', 1(1) *International Affairs* (2016), 43; World Economic Forum and Boston Consulting Group, 'Cyber Resilience Playbook for Public Private Collaboration' (January 2018), www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf, 42–44.

[55]中华人民共和国网络安全法 [Cybersecurity Law], People's Republic of China, National People's Congress (7 November 2016), Art. 37.

[56]Russian Data Localisation Law, Art. 18(5).

[57]*Personally Controlled Electronic Health Records Act 2012* (Cth), s 77 (in connection with e-health records).

[58]S. Sinha, 'Store data locally, RBI directs payment facilitators', *The Economic Times* (6 April 2018), https://economictimes.indiatimes.com/articleshow/63636133.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

[59]*Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions*, Law no. 6493 (20 June 2013) (Turkey), Art. 23 (in connection with e-payments).

[60]*Freedom of Information and Protection of Privacy Act*, RSBC (1996), s 30.1 (British Columbia); *Personal Information International Disclosure Protection Act*, NS2006, s 5 (Nova Scotia).

[61]Shackelford and Alexander, 'China's Cyber Sovereignty', supra n. 44.

[62]Several engineers of top technology companies are also members of technical standard setting institutions such as the IETF and W3C, thus showing the close links between the internet technical community and the private sector.

[63]See, e.g., H. Monicken, 'US, China Trade Criticisms at the WTO Over Cybersecurity Measures', 36(4) *Inside US Trade* (14 December 2018), https://insidetrade.com/daily-news/us-china-trade-criticisms-wto-over-cybersecurity-measures; Communication from the United States, *Measures Adopted and Under Development by China Relating to Its Cybersecurity Law – Questions to China*, WTO Doc. S/C/W/378 (3 October 2018); Communication from the United States, *Measures Adopted and Under Development by China Relating to Its Cybersecurity Law*, WTO Doc. S/C/W/376 (23 February 2018); Communication from the United States, *Measures Adopted and Under Development by China Relating to Its Cybersecurity Law*, WTO Doc. S/C/W/274 (26 September 2017); Communication from the European Union, *Statement by the European Union to the Committee on Technical Barriers to Trade 20 and 21 June 2018*, WTO Doc. G/TBT/N/CHN/1172 (9 July 2018). See also United States Trade Representative, *National Trade Estimate Report* (2016), 91.

[64]Lexology, 'APEC and EU Discuss Interoperability between Data Transfer Mechanisms', www.lexology.com/library/detail.aspx?g=22884b49-4d9b-45d9-a14a-708235bbca26.

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

to attempt exporting their regulatory models on data protection or cybersecurity to other countries, particularly through regional trade agreements,[65] causing further fragmentation in the global regulatory framework on data flows.[66]

Unlike issues of public morals or public order which are largely influenced by domestic values/ideals,[67] cybersecurity and data protection are unique issues because both governments and multistakeholder internet communities consider them as fundamental policy issues. The private sector also has a special role because of their responsibility for installing security and privacy controls in the technical protocols of the internet and design of digital services.[68] However, even if the private sector designs and adopts interoperable, robust, and secure protocols and standards, governments have the ability to block these protocols and standards by either exercising control over the physical infrastructure (such as server farms or Internet Exchange Points) or imposing mandatory domestic technical standards that do not align with best practices in the digital industry. Such measures are particularly facilitated by the lack of international consensus on legal principles governing cybersecurity and online privacy in international organizations, including the UN,[69] ITU,[70] and other platforms such as the World Summit on the Information Society.[71] In the absence of relevant international law or norms, the divide between the multistakeholder norms, private sector views, and domestic public policy appears to be irreconcilable.

4. Assessing Data Localization Measures under GATS General Exception

If a data localization measure fails to comply with a Member's GATS obligations, GATS Art. XIV can be used by a Member to justify derogation from its legal obligations. However, these exceptions cover a limited, exhaustive list of policy objectives. Therefore, this section investigates whether data localization measures, based on grounds of cybersecurity or privacy, can fit into one of the sub-sections of GATS Art. XIV and, thereafter, satisfy the conditions of the necessity test as well as the chapeau of GATS Art. XIV. I argue that data localization measures implemented to achieve data protection/privacy and cybersecurity fall under the exceptions available under

[65]See, e.g., *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (CPTPP) (signed 8 March 2018, not in force), www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text/#CPTPP, Art. 14.8.2 (setting out a broad definition of regulatory framework for protection of personal information including self-regulatory privacy models, prevalent in the US and other APEC countries); *United States–Canada–Mexico Trade Agreement* (USMCA), https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/united-states-mexico, Art. 19.15.2 (emphasizing on risk-based approaches to cybersecurity). See also C. Kuner, 'The Internet and the Global Reach of EU Law', LSE Law, Society and Economy Working Papers 4/2017, London School of Economics and Political Science (2017), 23–25.

[66]See, generally, on electronic commerce provisions in regional trade agreements, M. Wu, 'Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System', Overview Paper, RTA Exchange, Inter-American Development Bank and International Centre for Trade and Sustainable Development (November 2017); J. Huang, 'Comparison of E-commerce Regulations in Chinese and American FTAs: Converging Approaches, Diverging Contents and Polycentric Directions?', 64(2) *Netherlands International Law Review* (2017), 309.

[67]See, e.g., Appellate Body (AB) Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services* (*US–Gambling*), WT/DS285/AB/R (20 April 2005) [95], [294], [296], [301] [313]; AB 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 (19 January 2010) [141].

[68]M. L. Mueller, *Networks and States: The Global Politics on Internet Governance* (Cambridge, MA: MIT Press, 2010), pp. 163.

[69]E. Korzak, 'UN GGE on Cybersecurity: The End of an Era?', *The Diplomatic* (31 July 2017), https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/; on the issue of privacy, the UN has only adopted resolutions with no binding effect. See, e.g., *The Right to Privacy in the Digital Age*, 69th session, Third Committee, Agenda Item 68 (b), UN Doc. A/C.3/69/L.26/Rev.1 (19 November 2014). See also *Guiding Principles on Business and Human Rights*, endorsed by the Human Rights Council in 2011

[70]See R. Hill, 'Dealing with Cyber Security Threats: International Cooperation, ITU, and WCIT', Paper presented at 7th International Conference on Cyber Conflict: Architectures in Cyberspace (2015), 124, 25.

[71]See M. Mueller, 'Goodbye and Good Riddance to "Enhanced Cooperation"', *The Internet Governance Project* (10 February 2018), www.internetgovernance.org/2018/02/10/goodbye-good-riddance-enhanced-cooperation/.

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

GATS Art. XIV(c) and GATS Art. XIV(a). However, assessing the necessity of such measures under these sub-provisions entails a tough balancing of trade and the domestic understanding of internet policy goals. The tools available to Panels and the Appellate Body (AB)[72] under the weighing and balancing test developed under GATS Art. XIV can often be helpful to weed out protectionist data localization measures. However, in cases where such measures have multiple objectives (for example, a privacy measure incidentally favouring indigenous digital sector(s)) or are based on contested regulatory standard(s) (for example, determining adequacy of privacy laws of data recipient countries based on specific criteria),[73] the effectiveness of GATS Art. XIV in balancing various trade and non-trade policy considerations is less certain. To some extent, the design and implementation of such measures can be investigated by thoughtfully using relevant technical and factual evidence to detect any disguised protectionist intent. However, in the absence of specific international law, norms, or standards on cybersecurity and privacy, and divided views among technical experts regarding the most effective standards for data protection and cybersecurity, WTO tribunals will inevitably face limitations in deciding on the legitimacy of such measures in many disputes.

4.1 Contextualizing Privacy and Cybersecurity under GATS Art. XIV

Being a pre-internet era treaty, the provisions contained in GATS were not designed keeping in mind the public policy challenges of a digital era, particularly those related to cross-border data transfers via the internet. For example, GATS does not contain any rules requiring its Members to adopt basic domestic frameworks on privacy and cybersecurity (unlike rules in recent PTAs such as the CPTPP and USMCA which provide for explicit commitments).[74] Certain experts therefore argue that GATS obligations are outdated, including those related to telecommunications services, posing severe challenges in addressing data-related disputes.[75] Others argue that GATS disciplines are relevant but need to be updated or reformed to reflect the unique challenges of a data-driven economy.[76]

Although the exceptions contained in GATS Art. XIV can be creatively interpreted to cover contemporary policy challenges arising in domestic internet and data regulation, these policy objectives were clearly not envisaged at the time of the formulation of the treaty. Therefore, this section explores if and how GATS Art. XIV(c) and (a) covers data localization measures implemented on grounds of privacy and cybersecurity by reference to the principle of evolutionary interpretation of treaties.

4.1.1 GATS Art. XIV(c) Can Cover Both Privacy and Cybersecurity-Related Measures

Under GATS Art. XIV(c), a data localization measure can be provisionally justified provided: (a) it is implemented to secure compliance with domestic 'laws and regulations'[77] including those relating to:[78]

[72]Panel and AB refer to the dispute settlement bodies of the WTO and is sometimes collectively referred as 'WTO tribunals' in this article.

[73]See, e.g., GDPR Art. 45 (containing the adequacy mechanism to assess if a foreign data protection framework is essentially equivalent to that of the EU).

[74]For detailed discussion of the relevant provisions in these agreements, see Wu, 'Digital Trade-Related Provisions in Regional Trade Agreements', supra n. 66; J.-A. Monteiro and R. Teh, 'Provisions on Electronic Commerce in Regional Trade Agreements', WTO Working Paper ERSD-2017-11, WTO (July 2017); A. Chander, 'The Coming North American Digital Trade Zone', *Net Politics* (9 October 2018), www.cfr.org/blog/coming-north-american-digital-trade-zone.

[75]H. Lee-Makiyama, 'Cross-border Data Flows in the Post-Bali Agenda', in S. J. Evenett and A. Jara (eds.), *Building on Bali – Work Programme for the WTO* (Centre for Economic Policy Research, 2013), pp. 163, 164; But see Tuthill, 'Cross-border Data Flows', supra n. 6, at 357, 371; Crosby, 'Analysis of Data Localization Measures under WTO Services Trade Rules and Commitments', supra n. 20.

[76]See, e.g., M. Burri, 'Designing Future-Oriented Multilateral Rules for Digital Trade', in P. Sauvé and M. Roy (eds.), *Research Handbook on Trade in Services* (Cheltenham: Elgar, 2016), pp. 331, 349. See also Mitchell and Hepburn, 'Don't Fence Me In', supra n. 20, at 182, 230–236.

[77]See AB Report, *Mexico – Tax Measures on Soft Drinks and Other Beverages* (*Mexico–Taxes on Soft Drinks*), WT/DS308/AB/R (24 March 2006) [79]. The AB held that 'laws and regulations' refer to domestic laws and regulation, and not international law, unless it is incorporated into domestic law.

[78]GATS Art. XIV(c)(i) (ii) (iii).

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

(i) the prevention of *deceptive and fraudulent practices* or to deal with *the effects of a default on services contracts*;
(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*;
(iii) *safety*;[79]

(b) the above 'laws and regulations' are otherwise consistent with WTO law; and (c) the data localization measure is necessary to secure compliance with these laws and regulations.[80]

In my view, an evolutionary interpretation[81] of the terms contained in the above exceptions cover different aspects of cybersecurity and internet privacy.[82] For instance, laws preventing 'deceptive and fraudulent practices' in GATS Art. XIV(c)(i) and 'safety' in GATS Art. XIV(c)(iii) could refer to domestic laws designed to protect consumers from cybercrimes resulting from unauthorized hacking by third parties, malware attacks, etc. The most commonly used tools to achieve this include imposing security standards, banning malicious software, or necessitating service providers to employ cybersecurity best practices. For example, UNCTAD has estimated that 72% of the countries in the world have adopted at least some cybercrime laws.[83] Further, several governments are now implementing data localization measures to enhance their cybersecurity environment and protect the interests of domestic internet users.[84]

Further, to obtain stronger enforcement of domestic consumer protection or data protection laws, digital service providers are often required to provide tailored privacy and security undertakings in their terms of use or contractual arrangements between digital service providers and users. Some examples include obtaining informed consent for third-party use of personal data, protecting personal data from unauthorized use by third parties, protecting personal data against data breaches, and providing appropriate quality of digital services.[85] Similarly, certain domestic laws require mandatory notification of all data breaches to governments so as to hold the companies accountable for losses as well as safeguard consumer rights.[86] Such laws might increase compliance

[79]Emphasis added.

[80]Panel Report, *Colombia – Indicative Prices and Restrictions on Ports of Entry* (*Colombia–Ports of Entry*), WT/DS/366/R (27 April 2009) [7.514]; AB Report, *United States – Measures Relating to Shrimp from Thailand* (*US–Shrimp (Thailand)*), WT/DS343/AB/R; WT/DS345/AB/R (1 August 2008) [7.174]. See also AB Report, *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef* (*Korea – Various Measures on Beef*), WT/DS161/AB/R, WT/DS169/AB/R (10 January 2001) [157]; AB Report, *Thailand – Customs and Fiscal Measures on Cigarettes from the Philippines* (*Thailand–Cigarettes (Philippines)*), WT/DS371/AB/R (15 July 2011) [177]; AB Report, *US–Gambling* [6.536]–[6.537]. See also Ming Du, 'The Necessity Test in World Trade Law: What Now?', 15 *Chinese Journal of International Law* (2016), 817, 835.

[81]For a useful discussion on the principle of evolutionary interpretation, see G. Marceau, 'Evolutive Interpretation by the WTO Adjudicator', 21 *Journal of International Economic Law* (2018), 791–813.

[82]In context of evolutionary interpretation, see AB Report, *United States – Import Prohibition of Certain Shrimp and Shrimp Products* (*US–Shrimp*), WT/DS58/AB/R (6 November 1998) [129]; AB Report, *China–Publications and Audiovisual Services* [396]; Panel Report, *Mexico – Measures Affecting Telecommunications Services* (*Mexico–Telecoms*), WT/DS204/R (1 June 2004) [7.2]. While Members tend to accept GATS exception in an online context, they also favour a narrow reading of exceptions, see Work Programme on Electronic Commerce, *Progress Report to the General Council*, WTO Doc. S/L/74 (27 July 1999) [14].

[83]UNCTAD, 'UNCTAD Global Cyberlaw Tracker', https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx.

[84]The most widely discussed example is the Chinese cybersecurity law. See 中华人民共和国网络安全法 [Cybersecurity Law] (People's Republic of China) National People's Congress (7 November 2016). For a comprehensive discussion of data localization laws, see M. F. Ferracane *et al*., 'Digital Trade Restrictiveness Index', European Centre for International Political Economy (2018), http://globalgovernanceprogramme.eui.eu/wp-content/uploads/2018/09/DTRI-final.pdf.

[85]For example, the GDPR imposes most of these requirements on all service providers in the EU, irrespective of the location where the data are stored and processed.

[86]For example, several US states impose a requirement for notification of data breaches. See National Conference of State Legislatures, 'Security Breach Notification Laws' (29 September 2018), www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. Several countries in the Asia-Pacific region, including Australia and Korea, also impose data breach notification laws. See Nicholas Blackmore, 'Mandatory Data Breach Notification Laws

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

costs for companies, particularly where extensive cross-border data transactions are involved, and can be particularly burdensome for foreign companies.[87] However, they could be justified as measures necessary to achieve compliance with domestic laws dealing with 'default on service contracts' (with reference to contracts in the online environment) under GATS Art. XIV(c)(i).

Finally, 'protection of privacy of individuals' in GATS Art. XIV(c)(ii) can be interpreted in the context of the internet and online services, thus covering restrictions on data transfer contained in data protection laws, or other compliance requirements on service providers such as obtaining informed consent from internet users and preventing unauthorized use of personal data. The right to privacy has been widely recognized in the online context as a fundamental human right in other international treaties,[88] with 58% countries across the world having adopted data protection laws.[89] Therefore, considering the significance of these contemporary policy concerns, GATS Art. XIV(c)(ii) should also be interpreted to include domestic laws addressing privacy concerns in the online context.

In assessing whether the domestic laws and regulations are consistent with WTO law, Panels usually presume legitimacy unless shown otherwise.[90] Certain aspects of data protection or cybersecurity laws could be inconsistent with WTO law. If a data protection measure imposes certain conditions for cross-border data transfer (for example, that the recipient country has an equivalent level of data protection, also known as the adequacy mechanism), it can be challenged if these conditions are discriminatory or ambiguous. For example, in Russia, any country that is party to the Strasbourg Convention[91] is deemed to have an adequate level of data protection irrespective of how the law might be implemented in that country.[92] Kuner also argues that the grounds for evaluation of adequacy under the GDPR are largely political rather than objective requirements.[93] Similarly, if a specific technical standard or regulatory requirement for cybersecurity is implemented without guidelines or in a discriminatory fashion, it could be inconsistent with WTO law. For example, the Chinese cybersecurity law requires all foreign service suppliers to adopt 'secure and controllable' standards without clearly specifying how they can meet this requirement.[94] Additionally, this law also forces foreign companies to disclose the source code of their digital services to the government.[95]

Spread Across Asia-Pacific' (2 March 2018), www.kennedyslaw.com/thought-leadership/article/mandatory-data-breach-notification-laws-spread-across-asia-pacific.

[87]See discussion in Section 2 above.

[88]See, e.g., *Universal Declaration of Human Rights*, Art 12; *International Covenant on Civil and Political Rights* Art. 17; *The Right to Privacy in the Digital Age*, 69th session, Third Committee, Agenda Item 68 (b), UN Doc. A/C.3/69/L.26/Rev.1 (19 November 2014).

[89]UNCTAD, 'UNCTAD Global Cyberlaw Tracker', https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx.

[90]AB Report, *United States – Countervailing Duties on Certain Corrosion-Resistant Carbon Steel Flat Products from Germany* (*US–Carbon Steel*), WT/DS213/AB/R (19 December 2002) [157]. See also AB Report, *Dominican Republic – Measures Affecting the Importation and Internal Sale of Cigarettes*, WT/DS302/AB/R (19 May 2005) (*Dominican Republic–Import and Sale of Cigarettes*) [111]; AB Report, *US–Gambling* [138].

[91]*Strasbourg Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Strasbourg Convention) (2005).

[92]Regarding cross-border transfer of personal data (an issue relevant to international trade law), Art. 12.1 of the *Federal Law on Data Protection*, Federal Law no 152-FZ (14 July 2006) allows automatic transfer of personal data (subject to other legal requirements) to countries which are party to the Strasbourg Convention. The Roskomnadzor can also include countries with similar levels of data security as prescribed in the Convention as having adequate standards for cross-border data transfer (Russian Data Protection Law, Art. 12.2).

[93]Kuner, 'The Internet and the Global Reach of EU Law', supra n. 65, at 28.

[94]S. Sacks and M. K. Li, 'How Chinese Cybersecurity Standards Impact Doing Business in China', CSIS Policy Brief, Centre for Strategic and International Studies (August 2018), https://csis-prod.s3.amazonaws.com/s3fspublic/publication/180802_Chinese_Cybersecurity.pdf?EqyEvuhZiedaLDFDQ.7pG4W1IGb8bUGF; Y. Yang, 'China's Cyber Security Law Rattles Multinationals', *The Financial Times*, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/ (31 May 2017).

[95]Ibid.

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

A data localization measure 'secures compliance' with domestic laws and regulations when the measure is intended to enforce the said laws and regulations.[96] The AB has interpreted that securing compliance does not imply that the results of the measure can be guaranteed with 'absolute certainty'.[97] For example, a Member can claim that a data localization measure achieves stronger enforcement against foreign companies breaching domestic data protection laws. A Panel may accept this assertion without sufficient quantitative evidence based on other considerations such as the regulatory capacity of the country and the importance of privacy within the specific cultural context of the society. For the purposes of this article, I assume that these conditions are satisfied to further my analysis, although these factors could be scrutinized further based on the context and design of the data localization measure.

4.1.2 GATS Art. XIV(a) Is Relevant in Cases Involving Cyber Risks to Maintaining Public Order

Certain cybersecurity laws and regulations may be designed to achieve the objective of maintaining public order (GATS Art. XIV(a)). This assessment needs to focus on whether there is a 'genuine and sufficiently serious threat … to one of the fundamental interests of the society'.[98] The AB acknowledges that the notion of 'public order' can 'vary in time and space, depending upon a range of factors, including prevailing social, cultural, ethical and religious values'.[99] Therefore, 'public order' in GATS Art. XIV(a) could be interpreted to cover measures designed to address cyberthreats affecting WTO Members.[100] For instance, GATS Art. XIV(a) could cover measures designed to address security threats to Internet of Things (IoT) that pose a 'serious threat' to security of all homes connected via smart gadgets.[101] Finally, given that in certain societies, protecting individual privacy has significant cultural and social connotations,[102] certain Members may argue that safeguarding individual privacy through data localization is fundamental to protection of public morals under GATS Art. XIV(a). However, because GATS Art. XIV(c) already contains an explicit provision for protection of privacy, this argument is less likely to be made in a dispute.

4.2 Necessity of Data Localization Measures to Achieve Privacy and Cybersecurity

In over two decades of its jurisprudence, WTO tribunals have developed a holistic necessity test to assess the necessity of a measure under GATS Art. XIV, consisting of: (i) assessing the relative importance of the interests and values underlying the measure; and (ii) a 'weighing and balancing' test in light of those policy objectives considering the contribution of the measure to the objective, the restrictive impact of the measure on international commerce, and availability of reasonable and less trade restrictive alternatives.[103]

[96]N. Munin, *Legal Guide to GATS* (Kluwer Law International, 2010), p. 366.

[97]AB Report, *Mexico–Taxes on Soft Drinks* [72]–[74]; See also Panel Report, *China – Measures Affecting Imports of Automobile Parts* (*China–Auto Parts*), WT/DS339/R, WT/DS340/R, WT/DS342/R (18 July 2008) [7.337].

[98]See GATS Art. XIV (a), footnote 5.

[99]Panel Report, *US–Gambling* [6.461].

[100]In a related context, the Tallinn 2.0 Manual explicitly states the principle of sovereignty extends to 'the physical, logical and social layers' of cyberspace. One aspect of the exercise of sovereignty is the freedom to implement domestic cyber-policies including privacy and cybersecurity laws and regulations. See M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), pp. 13–16.

[101]See, e.g., S. J Shackleford *et al.*, 'When Toasters Attack: Enhancing the "Security of Things" through Polycentric Governance', 2 *University of Illinois Law Review* (2017), 415.

[102]See, e.g., AB Reports, *European Communities – Measures Prohibiting the Importation and Marketing of Seal Products* (*EC–Seal Products)*, WT/DS400/AB/R / WT/DS401/AB/R (18 June 2014) [5.199].

[103]AB Report, *Brazil – Measures Affecting Imports of Retreaded Tyres* (*Brazil–Retreaded Tyres*), WT/DS332/AB/R (17 December 2007) [146], [178]; AB Report, *US–Gambling* [307]; *Korea–Various Measures on Beef* [164]; AB Report, *Colombia – Measures Relating to the Importation of Textiles, Apparel and Footwear* (*Colombia–Textiles*), WT/DS461/AB/R

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

4.2.1 Relative Importance of Privacy and Cybersecurity

Protecting privacy of internet users, and achieving cybersecurity are fundamental requirements for maintaining the stability of the internet and enabling a trusted environment for cross-border data flows.[104] Key players in the international community, including the UN and its agencies, and internet governance organizations pay close attention to issues of cybersecurity and privacy in the context of international relations.[105] As the internet is integrated into the day-to-day lives of people, and cybercrimes are on the rise, governments are also resorting to new measures to ensure that digital services are secure, and internet users are not exploited by internet platforms; these include implementing national cybersecurity strategies[106] and full-fledged data protection frameworks.[107] The protection of individual privacy is also explicitly covered under GATS Art. XIV(c), given that service providers undermining privacy was a serious concern, even in the pre-internet era.[108] Given the strategic importance of protecting privacy and cybersecurity, including the enormous risks associated with failing to provide for these frameworks in a digitalized economy, Panels are likely to accord very high priority to these objectives in a data localization-related trade dispute.

4.2.2 How Data Localization Achieves Privacy and Cybersecurity

In justifying a measure under GATS Art. XIV, the defendant must provide objective evidence of the necessity of a measure, rather than asserting or stating its policy objectives.[109] Therefore, a 'genuine relationship of means and ends' between the measure and policy objective is essential to prove that a data localization measure contributes to the stated policy objective(s).[110] As discussed in Section 2, data localization measures aimed at cybersecurity and privacy usually interfere with the standard end-to-end architecture of the internet, and potentially affect the technical design of digital products. Thus, in assessing the contribution of a data localization measure in achieving compliance with cybersecurity and privacy laws, the Panel is likely to examine evidence on how the specific measure impacts the underlying technical features of a digital service, whether it enhances (or has the potential to improve) security of the networks and/or security and privacy of data, and how it impacts data flows. However, this examination is restricted to examining the sufficiency of evidence regarding the effectiveness of the measure (i.e. whether it contributes to cybersecurity and privacy); but in appreciating such evidence,[111] the Panel cannot become an 'arbiter' of various technical opinions on cybersecurity or privacy measures.[112]

Technical evidence often weighs against the ability of data localization measures to contribute to policy objectives of cybersecurity and privacy.[113] Data localization does not reduce network

(22 June 2016) [5.75], [5.77]. See also Ming Du, 'The Necessity Test in World Trade Law: What Now?', 15 *Chinese Journal of International Law* (2016), 817.

[104]See discussion above in Section 3 above.

[105]Ibid.

[106]As per the Global Cybersecurity Index 2017, about 38% of countries have a national cybersecurity strategy and 12% are in the process of implementing such a strategy. See UN News, 'Half of all countries aware but lacking national plan on cybersecurity, UN agency reports' (5 July 2017), https://news.un.org/en/story/2017/07/560922-half-all-countries-aware-lacking-national-plan-cybersecurity-un-agency-reports.

[107]UNCTAD, 'Data Protection and Privacy Legislation Worldwide', http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

[108]AB Report, *US–Gambling* [304].

[109]Ibid.

[110]AB Report, *Brazil–Retreaded Tyres* [210]. See also AB Report, *EC–Seal Products* [5.210].

[111]Thus, the Panel could accord higher priority to certain types of evidence presented in a dispute. See AB Report, *European Communities – Measures Affecting Asbestos and Products Containing Asbestos* (*EC–Asbestos*), WT/DS135/AB/12 (5 April 2001) [161].

[112]See Panel Report, *EC–Asbestos* [8.182], also [8.181].

[113]T. Maurer *et al.*, 'Technological Sovereignty: Missing the Point?', in M. Maybaum *et al.* (eds.), *Architectures in Cyberspace* (NATO CCD COE Publications, 2015), pp. 53, 61–62; N. Cory, 'Cross-Border Data Flows: Where Are the Barriers and What Do They Cost?', Information Technology and Innovation Foundation (May 2017), 3–4; Komaitis, 'The

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

vulnerabilities such as cyberattacks, vulnerability to natural disasters, or data fraud.[114] On the contrary, localizing makes data less secure as it becomes concentrated in specific servers, and, hence, an easier target for cyberattacks and surveillance.[115] Further, data localization does not increase government access to the data if the data are encrypted[116] or enhance governmental control if multiple jurisdictions can simultaneously claim right to that data.[117] Technical evidence also indicates that data localization causes engineering inefficiencies; for instance, interfering with underlying transfer protocols of the network to route data in a specific manner and, thereby, disrupting trade in digital services.[118]

However, data localization could enable easier monitoring of local servers or taking actions against operators breaching data protection or cybersecurity laws, particularly considering the low levels of international cooperation on these issues. For example, tracking down violations or pursuing civil/criminal action against violators in one's territory might be easier than taking actions against those companies operating and providing their services from abroad. Further, data localization may be justified if a country prevents transfer of data to countries with a very poor track record of cybersecurity or data protection; for example, where governments are known to force companies to hand over data coercively. In such cases, investigating the technical efficacy of a data localization measure in addition to other factual evidence may provide meaningful input in assessing the contribution of the measure to the stated policy objective.

The territorial logic behind data localization measures however does not align well with the nature of digital data flows, particularly in the age of ubiquitous cloud computing.[119] Experts argue that cloud computing enables instantaneous and automatic routing of data packets to several locations in the world simultaneously, usually broken down into several smaller packets through a process known as sharding.[120] Thus, the location of internet users is irrelevant to where/how their data are stored.[121] Consequently, the location of the data, i.e. whether they are located in domestic or foreign servers, a single server, or across multiple servers in different parts of the world, cannot be determinative of the security, quality, or privacy of data.[122] Rather, the robustness of the technical designs and protocols underlying the internet network and digital services determine data security and privacy.

"Wicked Problem" of Data Localization', supra n. 1, at 361–362; United States International Trade Commission, 'Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions', Publication no. 4716, Investigation no. 332–561 (August 2017), 285; U. Ahmed and A. Chander, 'Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows', Think Piece, E15 Expert Group on the Digital Economy, International Centre for Trade and Sustainable Development and World Economic Forum (November 2015), 6–7.

[114]Hon *et al.*, 'Policy, Legal and Regulatory Implications of a Europe-only Cloud', supra n. 5, at 251, 262.

[115]P. S. Ryan *et al.*, 'When the Cloud Goes Local: The Global Problem with Data Localization' (December 2013), *Computer*, https://storage.googleapis.com/pub-tools-public-publication-data/pdf/42544.pdf, 54, 56.

[116]Hon, *Data Localization Laws and Policy*, supra n. 13, at 70.

[117]Ibid. 62, 89.

[118]See, generally, L. DeNardis, 'Introduction: One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation', in *A Universal Internet in a Bordered World: Research on Fragmentation, Openness and Interoperability Volume I* (Centre for International Governance Innovation and the Royal Institute of International Affairs, 2016), pp. 4, 6–10.

[119]Hon, *Data Localization Laws and Policy*, supra n. 13, at 32, 105.

[120]J. Kim, 'How Sharding Works', *Medium* (6 December 2014), https://medium.com/@jeeyoungk/how-sharding-works-b4dec46b3f6.

[121]See J. Daskal, 'The Un-Territoriality of Data', 125 *Yale Law Journal* (2015), 326, 329.

[122]D. Hoffman *et al.*, 'Trust in the Balance: Data Protection Laws as Tools for Privacy and Security in the Cloud', 10 *Algorithms* (2017), 47, 55–6; T. Sargsyan, 'The Turn to Infrastructure in Privacy Governance', in F. Musiani *et al.* (eds.), *The Turn to Infrastructure in Internet Governance* (Springer, 2015), pp. 189, 198; Chander and Le, 'Data Nationalism', supra n. 2, at 677, 730.

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

4.2.3 Trade Restrictive Impact of Data Localization

Several studies have focused extensively on the disruptive economic impact of data localization, and its threat to trade in a digital economy.[123] Compliance with data localization measures inevitably disrupts the technological and commercial arrangements inherent to the digital sector, particularly as a majority of players rely on economies of scale in the digital sector.[124] Further, a foreign service supplier might be unwilling to relocate servers to the territories of WTO Members a with poor regulatory or physical infrastructure.[125] Smaller companies might lack sufficient resources to build local servers and thus might be prohibited from entering markets with data localization laws. These factors indicate that data localization measures have an over-all trade-inhibiting effect, by significantly reducing exports by foreign service providers.

However, the direct economic impact of cross-border data flows is not easily measurable,[126] and thus presenting robust quantitative evidence of the restrictive impact of data localization is not always possible.[127] Even in such scenarios, the Panel could be presented with other evidence by the complainant; for example, surveys showing less open or less competitive markets for foreign digital services in a specific market, low trust levels in indigenous digital services or local cloud computing facilities, and lack of sufficient digitally driven services in the domestic market. All these factors could indicate reduced opportunities for export of digital services into the market of a particular Member. Sometimes, understanding the way a data localization measure blocks cross-border data flows can be instructive in assessing the degree of trade restrictiveness. For example, if a data localization measure affects underlying transfer protocols or the integrity of the domain name system, its trade-restrictive impact is far deeper than when it forces a few digital service providers to make cosmetic modifications to their technical design or terms of use.

4.2.4 Availability of Reasonable and Less Trade Restrictive Measures

In conducting a holistic necessity analysis through a 'weighing and balancing' test,[128] alternative measures proposed by the complainant, which are less trade-restrictive, reasonably available to the defendant, and achieve an equivalent level of protection, have been considered very carefully in WTO disputes.[129] For example, can a government compel foreign companies to comply with domestic data protection or cybersecurity laws without necessarily using data localization measures? One commonly discussed alternative is holding service providers accountable for circumventing domestic laws related to data protection and security for breaching domestic laws, irrespective of the location of the data or service provider (also known as the accountability approach). Theoretically, this approach is flexible because instead of imposing fixed standards or highly prescriptive compliance requirements such as data localization, the digital service providers have the freedom to adopt any practices and standards that meet the basic principles of a Member's privacy and cybersecurity laws.[130] However, as argued below, significant debate exists

[123]See, e.g., Bauer *et al.*, 'The Costs of Data Localisation', supra n. 17; J. P. Meltzer, 'The Internet, Cross-Border Data Flows and International Trade', 2 *Asia & the Pacific Policy Studies* (2014), 90, 92; United States International Trade Commission, 'Digital Trade in the US and Global Economies, Part 2', Publication no. 4485 (August 2014) 65; Manyika *et al.*, 'Digital Globalization', supra n. 16, at 1.

[124]Hon *et al.*, 'Policy, Legal and Regulatory Implications of a Europe-only Cloud', supra n. 5, at 251, 253–254.

[125]J. M. Kaplan and K. Rowshankish, 'Addressing the Impact of Data Location Regulation in Financial Services', Global Commission on Internet Governance, Paper Series no 14, CIGI and Chatham House (May 2015), 1.

[126]Economics and Statistics Administration and the National Telecommunications and Information Administration, 'Measuring the Value of Cross-Border Data Flows', US Department of Commerce (September 2016), 1.

[127]Both quantitative or qualitative evidence can be put forth to assess the restrictive impact of a measure. See AB Report, *Brazil–Retreaded Tyres* [146].

[128]For the weighing and balancing test, see AB Report, *EC–Seal Products* [5.214]; AB Report, *China–Publications and Audiovisual Products* [242].

[129]AB Report, *US–Gambling* [308]; AB Report, *Brazil–Retreaded Tyres* [156].

[130]C. Kuner, 'Developing an Adequate Legal Framework for International Data Transfers', in S. Gurtwith *et al.* (eds.), *Reinventing Data Protection* (Springer, 2009), pp. 263, 269.

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

regarding its effectiveness in ensuring data privacy and security compared to prescriptive restrictions on cross-border data transfer.[131] An example is the GDPR, which holds companies liable for applying all the rules in relation to data processing of EU residents, irrespective of where the digital services originate.[132] Some experts like Kuner argue that the above provision negates the need for restrictions on cross-border data transfers in GDPR.[133]

A defending Member is likely to argue that the above alternative is either not 'reasonably available' because of its inadequate regulatory capacity or that it does not achieve an equivalent level of cybersecurity and privacy as a data localization measure. Several experts argue that an accountability approach in data protection is more viable than a prescriptive approach resulting in de facto localization.[134] However, in certain cases, a provision requiring accountability of digital service providers can be ineffective by itself – for example, monitoring, or auditing, the data processing facilities of all digital service suppliers (particularly from outside the country) is practically impossible, even for the most developed Members. Further, when the chances of being caught are negligible, foreign digital providers are likely to avoid the excessive requirements in domestic laws (despite their binding nature), making data processing potentially more unsafe and susceptible to security and privacy breaches.[135] Thus, a Member may argue that data localization measures may be more effective in addressing such security and privacy risks. At best, an accountability approach appears to be a useful complement to strict data privacy and security requirements, including those restricting cross-border data transfers.

Additionally, a complainant might propose that privacy trustmarks or a self-certification mechanism (including for security of digital services and applications) are less trade restrictive than data localization measures.[136] An example of a voluntary certification system is the APEC Cross-border Privacy System (CBPR),[137] where an independent body (either a public entity or private company) certifies that policies and practices of all participating businesses are compliant with the APEC Privacy Framework.[138] However, certain experts have questioned its effectiveness, including its ability to promote a high standard of data protection in participating countries.[139] For instance, TrustArc (formerly, Truste) (an accountability agent for APEC CBPR) has been penalized for fraudulent certifications.[140]

[131]See generally C. J. Bennett, 'The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats', in D. Guagnin *et al.* (eds.), *Managing Privacy through Accountability* (Palgrave Macmillan, 2012), p. 33.

[132]GDPR Art. 3(2).

[133]C. Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law', 5(4) *International Data Privacy Law* (2015), 235, 244. See also S. Yakovleva, 'Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade "Deals"?', *World Trade Review* (2017), 1, 22.

[134]Hon, *Data Localization Laws and Policy*, supra n. 13, at 221. See generally C. L. Bennett, 'The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats', in D. Guagnin *et al.* (eds.), *Managing Privacy through Accountability* (Springer online, 2012), p. 33.

[135]See generally D. Jerker and B, Svantesson, 'The Regulation of Cross-Border Data Flows', 1(3) *International Data Privacy Law* (2011), 180, 194.

[136]These trustmarks are often driven by private parties under the oversight of a governmental agency, e.g., Truste, the accountability agent under APEC CBPR is a business organisation based in the US recognised by the FTC, and Japan Institute for Promotion of Digital Economy and Community JIPDEC, the second accountability agent under APEC CBPR is recognized by the Ministry of Economy, Trade and Industry, Government of Japan. See further information, www.cbprs.org/Agents/AgentDetails.aspx.

[137]APEC, *APEC Cross-Border Privacy Rules System*, /www.cbprs.org/.

[138]APEC, *APEC Privacy Framework* (November 2004), www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

[139]See, e.g., G. Greenleaf, 'APEC Privacy Framework: A New Low Standard', Privacy Law and Policy Reporter (2005), 1; G. Greenleaf, 'Five Years of the APEC Privacy Framework: Failure or Promise?', 25 *Computer Law & Security Report* (2009), 28. Regarding the differences between APEC CBPR and GDPR, see A. Wall 'GDPR Matchup: The APEC Privacy Framework and Cross-Border Privacy Rules', https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/.

[140]See, e.g., Federal Trade Commission, 'TRUSTe Settles FTC Charges it Deceived Consumers through Its Privacy Seal Program', Press Release (17 November 2014), www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its.

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

A complainant may also argue that a mandatory requirement for privacy and security-by-design in all digital products and services are sufficient to ensure data privacy and security of data flows and are a less trade restrictive alternative to data transfer restrictions. In other words, if all digital service providers adopt highly secure and privacy-enabling technologies, data localization measures to achieve privacy and cybersecurity become redundant. The 32nd International Conference of Data Protection and Privacy Commissioners unanimously passed a resolution in 2010 recognizing 'Privacy by Design as an essential component of fundamental privacy protection' and encouraging 'the adoption of Privacy by Design's Foundational Principles … as guidance to establishing privacy as an organization's default mode of operation'.[141] The EU has included a mandatory privacy requirement and security by design in the GDPR.[142] However, a defending Member is likely to argue that mandatory privacy and security-by-design are at best complementary measures due to the lack of global norms on data privacy and security as well as the dearth of international benchmarks.

In each of the above cases, the Panels consider whether these evidently less trade restrictive alternatives are reasonably available to the defendant, practicable, and whether they achieve an equivalent (or better) regulatory outcome as data localization. Under GATS, Members have autonomy to choose their desired level of protection and the means to safeguard their domestic policy objective.[143] Thus, the Panel is only able to evaluate the efficacy of the data localization measure, or any other tools used to achieve cybersecurity/privacy, along with the proposed less trade restrictive alternatives by looking at the evidence presented in a dispute. This evidence can sometimes be instructive in detecting disguised security/privacy measures. For example, if a Member claims that its data localization measure will prevent all security or privacy breaches, no evidence is likely to support such an assertion. However, to date, no international consensus exists on the viability of many of the above-discussed alternatives, despite several efforts of the industry and certain governments (for instance, making the APEC CBPR compatible with the GDPR). Therefore, even if sufficient evidence were presented by technical experts supporting the efficiency of the above discussed alternative measures, which are potentially less trade-restrictive, the Panel will most likely refrain from considering them due to the absence of international standards on data privacy and cybersecurity.[144] Such a restrained approach is perhaps more judicious, given that WTO tribunals are not appropriately equipped to prescribe or favour specific technical or domestic policy standards, and lack the mandate and expertise to prescribe internet policies.

4.2.5 Outcomes of Weighing and Balancing Test

The outcome of the weighing and balancing test would depend on several factors in each dispute, such as the design and implementation of the measure, the stated motive behind the measure, the evidence presented by the disputing and third parties, the availability of other technical experts, and finally, the alternatives advanced by the complainant to the data localization measure. The assessment in the above section indicates that a clear motive of disguised protectionism would usually be caught by GATS Art. XIV. For example, if a Member claims that a certain measure has a security or privacy objective but evidence suggests no such causal link, then the measure would be illegal under GATS. A case in point is the Russian Data Localization Law[145] – the rationale of protecting the privacy of Russian citizens by forcing all foreign companies to store

[141]A close reading of this resolution however indicates that privacy by design was seen as a complement to legal and regulatory measures, and not as an alternative.

[142]GDPR Art. 25.

[143]GATS Preamble, fourth recital.

[144]See, e.g., M. Finnemore and D. B. Hollis, 'Constructing Norms for Global Cybersecurity', 110(3) *American Journal of International Law* (2016), 425;

[145]For a detailed study of the measure, see A. Savelyev, 'Russia's New Personal Data Localization Regulations: A Step Forward or a Self-imposed Sanction?', 32 *Computer Law & Security Review* (2016), 128.

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

a master copy of all personal data locally is unclear given that data localization: (i) significantly increases the costs borne by foreign companies;[146] and (ii) reduces the quality of services available (and, hence, security and privacy of data).[147]

Even if a data localization measure has a strong privacy or cybersecurity rationale, it might be based on a contested regulatory standard or benchmark, which might represent a specific country's vision of desirable internet policy but does not necessarily reflect the values of the internet governance community. For example, several experts (particularly in the private sector) argue that the security standards in the Chinese cybersecurity law are disproportionate, deliberately ambiguous, and geared towards achieving cybersovereignty, rather than ensuring high levels of security or privacy.[148] Similarly, the application of the test is less clear when a data localization measure has multiple objectives. For example, a data protection law resulting in localization also creates economic advantage for the domestic digital industry, such as the increase in data centers in the EU to facilitate compliance with GDPR.[149]

4.3 Assessing Data Localization Measures under GATS Art. XIV Chapeau

Assuming a data localization measure satisfies the exception provided under one or more of the sub-clauses of GATS Art. XIV, it should also be examined for consistency with the chapeau of GATS Art. XIV which reads:

> Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures.

The chapeau of GATS Art. XIV prevents abuse of the exceptions available under the sub-sections of this provision.[150] In conducting this assessment, a Panel examines the implementation and operationalization of the measure[151] in order to ensure that the measure is implemented in 'good faith'.[152]

First, a Panel should assess whether 'like conditions' prevail either (a) between the Member imposing the data localization measure and other exporting Members; or (b) in case a data localization measure, favours or disfavours specific exporting Members, then between those Members and other exporting Members. An example of (b) would be a data protection law with an adequacy mechanism which allows data transfers to specific Members but otherwise generally disallows cross-border transfer of data in order to achieve compliance with its domestic data protection laws. In assessing 'like conditions', the Panel could compare the internet regulatory conditions in different countries. For example, if a country has a very poor track record of cybersecurity, then it is unlike another country which has a strong framework for cybersecurity.

[146]A study in 2015 had found that all major foreign internet companies would need to invest a total of 39 billion USD to comply with the data localization law. See L. Ragozin and M. Riley, 'Putin Is Building Great Russian Firewall', *Electronic Commerce & Law Report*, www.bloomberg.com/news/articles/2016-08-26/putin-is-building-a-great-russian-firewall (26 August 2016).

[147]See generally B. Cohen *et al.*, 'Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy', 32(1) *Antitrust* (2017), 107, 108–109. See also Section 4.2.2.

[148]See, e.g., AmCham China, 'Navigating the Chinese Cybersecurity Law' (18 May 2018), www.amchamchina.org/uploads/media/default/0001/09/7246f5970b90359c33d47f16e0f5c0518e7981a9.pdf.

[149]See J. I. Wong, 'Europe's Fight over Data Privacy Has a Silver Lining – a Cloud-Computing Boom', *Quartz* (4 October 2016), qz.com/799750/microsoft-msft-azure-europes-in-the-middle-of-a-cloud-boom-thanks-to-data-privacy-rules/.

[150]N. Munin, *Legal Guide to GATS* (Kluwer Law International, 2010), 372.

[151]AB Report, *United States – Standards for Reformulated and Conventional Gasoline* (*US–Gasoline*), WT/DS2/AB/R (20 May 1996), p. 22.

[152]AB Report, *US–Shrimp* [158].

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

Certain indices such as the Global Cybersecurity Index developed by the ITU could be helpful here.[153] Similarly, the Panel could also compare the regulatory culture of privacy in different Members; for example, Members with strong data protection laws, including those that recognize and enforce a fundamental right to privacy, might be unlike those Members that either have a weak regime or have been known to violate the privacy rights of their citizens.

Further, in examining whether the measure constitutes 'arbitrary or unjustifiable discrimination' or is a 'disguised restriction on trade in services', different aspects of the design, structure, and implementation of data localization measure could be informative.[154] For example, if a specific domestic law prevents commercial surveillance by foreign companies, including assembling and manipulating data for estimating market trends, but imposes no similar requirement on domestic companies, then it could qualify as 'arbitrary or unjustifiable discrimination' if regulatory conditions in those countries are otherwise similar.

A measure may constitute a 'disguised restriction on trade in services' if it favours domestic providers to conduct extensive data analysis across their entire customer network while depriving foreign providers of similar benefits, particularly if they cannot have comparable data processing expertise in that country. Another scenario could be when a domestic law prohibits commercial surveillance, while providing extensive powers to the domestic government to breach the privacy of its citizens in an unreasonable manner, or when domestic laws on privacy or security are not seriously enforced against domestic offenders while forcing foreign companies to relocate. For example, despite implementing a blanket data localization law for personal data to safeguard the privacy of its citizens, the Russian government also has a large number of domestic laws that authorize the government to intrude on the privacy of its residents in an unreasonable manner.[155] Finally, certain regulatory requirements might be so excessive or unreasonable that foreign companies might not be able to enter the market altogether (for example, obtaining necessary licenses or permissions to transfer data while providing digital services in that country), thus also qualifying as a disguised restriction on trade in services.

5. Eliminating Protectionist Data Localization Measures, Promoting Free Flow of Data and Preserving Privacy and Cybersecurity: Balancing Trade and Internet Regulation

In applying GATS Art. XIV to data localization measures, two distinct perspectives on internet policy come to the forefront: the views of the internet technical and policy community and those of governments. Clearly, the multistakeholder and transnational norms of internet governance often conflict with domestic cyber policies. However, the principles in international trade agreements, such as GATS, can be read harmoniously with multistakeholder or transnational views on internet governance. Although GATS lacks explicit rules on digital trade and internet data flows, its underlying principle of progressive trade liberalization[156] can align with several norms in internet governance. For example, ensuring free flow of data, one of the fundamental

[153]ITU, 'Global Cybersecurity Index', www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

[154]AB Report, *US–Shrimp* [156]; AB Report, *EC–Seal Products* [5.302].

[155]For example, domestic companies such as domestic online communication providers and internet platforms can track user details and activity (*Federal Law no. 149 on Information, Information Technologies and Protection of Information*, 2006 (Russia), Art. 10.1.3, 10.2.9. Further, the System of Operational Investigatory Measures authorises various government agencies to collect communications data and metadata, including from social media platforms, even prior to receiving a warrant. See N. Marachel, 'Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy' 5 (1) *Media & Communication* (2017), 29, 33. Further, it has also been reported that the Ministry of Communications requires that all digital products to install equipment to facilitate a dragnet Deep Packet Inspection surveillance system. See A. Soloatov and I. Borogoan, 'The Kremlin's New Internet Surveillance Plan Goes Live Today', *The Wired* (11 January 2012), www.wired.com/2012/11/russia-surveillance/;. Finally, the Federal Security Service can set standards for encryption of personal data, enabling state surveillance. See A. K. Zharova and V. M. Elin, 'The Use of Big Data: A Russian Perspective of Personal Data Security', 33 *Computer Law & Security Review* (2017), 482, 486.

[156]GATS Preamble, third recital.

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

principles in internet governance, is also important to ensure that the internet can be utilized as a platform for trade.[157] Similarly, ensuring internet security and facilitating trust in the internet, including protecting privacy of internet users, are not only compelling goals in internet governance, but also increasingly recognized as a precondition for facilitating digital trade.[158] In contrast, domestic policy is often focused on the internet from narrower economic and socio-cultural standpoints. For example, a country might view internet security only from the perspective of national security rather than cybersecurity, or recognize only a very prescriptive model of data protection.

The most judicious approach to remove protectionist data localization measures without intruding into domestic internet policy is to conduct a closer examination of the technical and factual evidence available on a case-by-case basis. GATS Art. XIV provides WTO tribunals the chance to delve into the efficacy of a data localization measure without interfering with the desired level of privacy or cybersecurity of a country. For example, technical or factual evidence is unlikely to support a claim by any government that data localization will eliminate cybercrimes or prevent all data breaches but may suggest that certain forms of localization can be conducive to better security or effective domestic legal enforcement. Conversely, certain forms of localization are unnecessary when they involve transfer of less sensitive data such as day-to-day business data constituting disaggregated and anonymized datasets primarily consisting of non-personal data,[159] or when the underlying technology of a digital service is highly secure and robust. These assessments can be made without assessing whether a Member can pursue cybersecurity or privacy policies within its jurisdiction, and to what degree, thus maintaining the inherent balance enshrined in GATS Art. XIV. In undertaking this assessment, the expertise of the internet technical community can be fruitful as they have precise knowledge of security and privacy technologies, and can provide an objective assessment of the effectiveness of the measure, irrespective of whether the stated objective is rational or excessive.

The reliance on technical or factual evidence will not however reduce the discretion of Panels to assess legitimacy of data localization measures. As security and privacy tools continue to evolve rapidly, the internet technical community is constantly redefining best practices in these areas. Further, due to the diversity of stakeholders in the internet technical and policy community, no single body controls all aspects of digital data transfers.[160] While it is within the powers of the Panel to use external expert evidence,[161] the question is whether certain multistakeholder

[157]Under Para 5(c) of GATS Telecommunications Annex, all Members are under an obligation to allow service suppliers from all WTO Members to use 'public telecommunications transport networks' for the 'movement of information within and across borders, including for intra-corporate communications of such service suppliers' and for 'access to information contained in databases or otherwise machine-readable form in the territory of any Member'. This provision is subject to the exception that Members may take measures 'necessary to ensure the security and confidentiality of messages' provided that they 'are not applied in manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade in services'.

[158]Although no explicit disciplines on electronic commerce have been adopted GATS Art. VI, certain recent free trade agreements refer to building greater internet trust through consumer protection laws, data protection laws, spam, and cybersecurity, indicating a possible future trend that a similar set of domestic regulations might also become necessary under the WTO framework, for example under GATS Art. VI or a Reference Paper. Some examples include *ASEAN–Australia–New Zealand Free Trade Agreement* (AANZFTA) (signed 27 February 2009, entered into force 1 January 2010), Art. 7; *China–South Korea Free Trade Agreement* (China–Korea FTA) (signed 1 June 2015, entered into force 20 December 2015), Art. 13.5; *European Union–South Korea Free Trade Agreement*, Art. 7.49(1)(d); *Australia–United States Free Trade Agreement* (AUSFTA) (signed 18 May 2004) [2005], ATS 1, Art. 16.6; *Japan–Mongolia Economic Partnership Agreement*, Art. 9.6.

[159]For example, in the EU, non-personal data are subject to less stringent standards than personal data (subject to the GDPR). The EU has also adopted a regulation to enable free flow of non-personal data in the EU. See 'Proposal for a Regulation of the European Parliament and Council on a Framework for the Free Flow of Non-Personal Data in the European Union', COM (2017) 495 final (13 September 2017).

[160]See discussion in Section 3 above.

[161]Marrakesh Agreement Establishing the World Trade Organization (opened for signature 15 April 1994), 1867 UNTS 3 (entered into force 1 January 1995), annex 2, Understand on Rules and Procedures Governing the Settlement of Disputes (DSU), Art. 13.

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

bodies such as the IETF, W3C, or the IGF can provide relevant inputs in trade disputes. Are technical codes, private standards, and multistakeholder norms relevant in assessing the necessity of a data localization measure? In practice, these questions are not straightforward and will require WTO tribunals to have at least a functional knowledge of internet governance. Further, the status of such transnational, multistakeholder, and extra-legal instruments (such as technical codes) is unclear in WTO law.[162] However, despite this unclear relationship, it is possible for Panels to consider some of these instruments as factual evidence in disputes even when they cannot be clearly used as legal tools for interpretation.[163]

In exercising its discretion under GATS Art. XIV and whilst weighing and balancing various trade and internet policy goals, WTO tribunals should remain cognizant that robust and effective technical standards on cybersecurity and privacy facilitate the free flow of data, rather than constrain it, as discussed in Section 3. On the other hand, non-transparent and unreasonable technical standards are usually ineffective in making data more secure and impede internet openness.[164] As argued previously, available evidence to date suggests that if a data localization measure adversely affects the open architecture of the internet,[165] it becomes undesirable both from a commercial point of view and from a security/privacy point of view.[166] For example, data localization measures requiring local routing of data interfere with the autonomy of the technical protocols and the reliability of the internet, including accessibility to websites.[167] Measures enforcing specific technical standards can damage interoperability and security, and make data transfer unsafe, particularly if the standards do not reflect industry best practices.[168] If technical standards prescribed by a specific country were indeed effective in ensuring better security or privacy in the network, they would have automatically emerged as global best practices in the technology industry, enhancing internet openness rather than inhibiting free flow of digital services.[169]

On a cautionary note, the role of GATS should not be misplaced or overestimated in the regulation of digital data flows. First, GATS does not recognize cybersecurity and privacy as preconditions for digital trade but rather limits their relevance to GATS Art. XIV (and also, GATS Art. XIV bis, when national security issues are involved).[170] WTO Members are still divided on the role of cybersecurity and privacy in international trade law.[171] This situation is further

[162]See generally M. E. Footer, 'The (Re)Turn to "Soft Law" in Reconciling the Antinomies in WTO Law', 11 *Melbourne Journal of International Law* (2011), 241. For a view on incorporating more multistakeholder/private standards in international trade law, see J. Pauwelyn, 'Rule-Based Trade 2.0? The Rise of Informal Rules and International Standards and How They May Outcompete WTO Treaties', 17(4) *Journal of International Economic Law* (2014), 739.

[163]See, e.g., L. Gruszczynski, 'Trade Law and Tobacco: Plain Sailing' on *Tradelinks* (15 November 2018), www.linklaters.com/en/insights/blogs/tradelinks/trade-law-and-tobacco-plain-sailing (discussing the use of Framework Convention on Tobacco Control (FCTC) guidelines as factual evidence in the recent *Australia – Plain* Packaging dispute. However, the FCTC guidelines constitutes part of an international treaty but had not been signed by all the disputing parties and hence, not binding).

[164]See text accompanying, nn. 49–51.

[165]D. Broeders, 'Aligning the International Protection of "the Public Core of the Internet" with State Sovereignty and National Security', 2(3) *Journal of Cyber Policy* (2017), 366, 367–369.

[166]DeNardis *et al.*, 'The Rising Geopolitics of Internet Governance', supra n. 44, at 14–15.

[167]Noction, 'How Does BGP Select the Best Routing Path' (18 January 2013), www.noction.com/blog/bgp_bestpath_selection_algorithm.

[168]See, e.g., in relation the Chinese WAPI standard for Wi-Fi, http://actonline.org/2016/03/17/mobile-mythbusting-wifi-wapi-and-the-encryption-debate/. See also, DeNardis *et al.*, 'The Rising Geopolitics of Internet Governance', supra n. 44, at 17.

[169]See, e.g., S. Baird, 'The Government at the Standards Bazaar', in L. DeNardis (ed.), *Opening Standards: The Global Politics of Interoperability* (Cambridge, MA: MIT Press, 2011), pp. 13, 18, 19; R. Ghosh, 'An Economic Basis for Open Standards', in L. DeNardis (ed.), *Opening Standards: The Global Politics of Interoperability* (Cambridge, MA: MIT Press, 2011), pp. 75, 76.

[170]See discussion in Section 4.1.

[171]In recent WTO proposals on Electronic Commerce, China and the US took a hands-off approach to data protection and consumer protection issues, while others such as Canada, Chile, Korea, Singapore, Brazil, Hong Kong, Australia, Taiwan, and

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

complicated by the absence of binding international legal principles on internet governance.[172] Thus, the capacity of WTO tribunals to resolve the divide between multistakeholder norms and domestic public policy goals, such as privacy and cybersecurity, is limited. One example here is assessing whether self-regulatory standards in security and privacy can be viable alternatives to data localization. Here, certain types of evidence may assist, such as how similar standards have functioned in countries with similar levels of development or regulatory infrastructure, and the potential costs of monitoring. But, in the end, a Panel may refrain from this exercise to avoid causing dissatisfaction in the broader international community.[173]

Second, given the limited list of policy objectives under GATS Art. XIV, certain evidence from the internet community might be irrelevant, despite reflecting fundamental engineering principles. For example, evidence that a data localization measure affects the integrity of the domain name system may not be as relevant in international trade law,[174] unless it also results in discriminatory treatment of foreign services and service providers, or violates GATS obligations on transparency or domestic regulations.

Addressing data localization measures ultimately necessitates a sophisticated and multidimensional response bringing together several areas of international governance, including international trade law and internet governance. Some policy initiatives that could influence building of better linkages between international trade law and internet governance and policy in the near future include: (i) developing global/transnational consensus in non-trade disciplines, such as data protection, cybersecurity, and international human rights, as well as development of new binding international standards or norms; (ii) developing new rules within the multilateral framework, seeking a better balance between internet openness, security, and privacy, including considering new disciplines on electronic commerce (for example, under GATS Art. VI:4),[175] and provisions on cross-border data flows; and (iii) exploring routes to develop more dialogue and partnerships between trade policymakers and internet experts, particularly while negotiating new rules on electronic commerce.[176]

---

the EU have taken a much stronger stance. See, e.g., WTO, Work Programme on Electronic Commerce, *Communication from Canada, Chile, Colombia, Côte d'Ivoire, the European Union, the Republic of Korea, Mexico, Montenegro, Paraguay, Singapore and Turkey – Trade Policy, the WTO and the Digital Economy*, WTO Doc. JOB/GC/116, JOB/CTG/4 JOB/SERV/248, JOB/IP/21 JOB/DEV/42 (13 January 2017); WTO, *Work Programme on Electronic Commerce – Non-Paper from Brazil*, supra n. 40; WTO, *Non-paper from the United States – Work Programme on Electronic Commerce*, supra n. 40.

[172]See discussion in Section 3 above.

[173]See, e.g., Panel Report, *China–Publications and Audiovisual Products* [7.894], [7.900], where the Panel effectively endorsed state censorship as a reasonably available and less trade restrictive alternative to censorship by selected entities.

[174]See, e.g., discussion on Article 37 of *Draft Measures on Internet Domain Names* introduced by China in D. Sepulveda and L. E. Strickling, 'China's Internet Domain Name Measures and the Digital Economy', on National Telecommunications and Information Administration blog (16 May 2016), www.ntia.doc.gov/blog/2016/china-s-internet-domain-name-measures-and-digital-economy. This measure was, however, ultimately removed from the final regulations.

[175]GATS Art. VI(4) reads as follows:

> With a view to ensuring that measures relating to qualification requirements and procedures, technical standards and licensing requirements do not constitute unnecessary barriers to trade in services, the Council for Trade in Services shall, through appropriate bodies it may establish, develop any necessary disciplines. Such disciplines shall aim to ensure that such requirements are, inter alia:
>
> (a) based on objective and transparent criteria, such as competence and the ability to supply the service;
> (b) not more burdensome than necessary to ensure the quality of the service;
> (c) in the case of licensing procedures, not in themselves a restriction on the supply of the service.

[176]See generally A. D. Mitchell and N. Mishra, 'Data at the Docks: Modernizing International Trade Law for the Digital Economy', 20(4) *Vanderbilt Journal of Entertainment & Technology Law* (2018), 1073, 1109–1129.

https://doi.org/10.1017/S1474745619000120 Published online by Cambridge University Press

6. Conclusion

The absence of international consensus on internet governance issues coupled with the dated nature of GATS will pose complex problems if disputes on data localization measures are brought before the WTO. To a certain extent, GATS Art. XIV can be creatively and thoughtfully applied to reduce protectionist data localization barriers while preserving a country's right to regulate on grounds of cybersecurity and privacy. However, the application of GATS Art. XIV entails extensive assessment of complex technical issues to balance free flow of data with legitimate public policy concerns. In assessing such issues, WTO tribunals can consider a range of technical and factual evidence to assess the technical efficacy of data localization measures in achieving privacy and cybersecurity. However, as the broader internet regulatory framework is deeply divided between multistakeholder/transnational internet governance norms and domestic public policy, this assessment is not always straightforward. Ultimately, the role of international trade law in data flow regulation is circumscribed by the lack of binding norms in internet governance.

This article also points out the importance of understanding the broader relationship between international trade law and internet governance in the context of cross-border data flows. To play a meaningful role, international trade law should not interfere with both the fundamental infrastructure of the internet and the exercise of regulatory autonomy in the domestic space for legitimate public policy objectives. While the latter can often be read into GATS Art. XIV (and XIV bis), the former is typically based on transnational norms and extra-legal codes outside the scope of GATS. Thus, applying international trade law to data localization effectively not only requires contextualizing existing rules to the digital economy but also contingent on the development of norms and standards in internet policy and governance. Ultimately, synergy between different fields of international governance, including trade law and internet governance, is essential for building a global network for communication and data flows. Moving forward, in developing solutions to address data localization or other restrictions on data flows, one should remain wary of placing excessive emphasis on disciplines in GATS or other trade agreements, and instead work towards developing a more balanced, multidimensional framework addressing various facets of internet and data regulation.

Author ORCIDs. Neha Mishra, 0000-0003-3028-2734

Cite this article: Mishra N (2020). Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation? *World Trade Review* **19**, 341–364. https://doi.org/10.1017/S1474745619000120