World Trade Review (2019), 18: 4, 579–607
© *Susannah Hodson* doi:10.1017/S1474745618000277 First published online 3 September 2018

Applying WTO and FTA Disciplines to Data Localization Measures

SUSANNAH HODSON

Australian National University, Australia

Abstract: The last decade has seen a proliferation of measures requiring data to be stored within national borders. Such restrictions, known as 'data localization measures', disrupt digital trade and run counter to the borderless reality of the internet. But the effectiveness of existing WTO rules to adequately discipline data localization measures remains inconclusive. In the absence of meaningful progress at the multilateral level, FTA negotiations are developing new models to address such barriers. This article compares how data localization measures would be disciplined under the General Agreement on Trade in Services (GATS) and the *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (CPTPP) framework. It argues that the CPTPP represents a significant advance on the GATS and strikes an appropriate balance between facilitating businesses' growing need to transfer and store data across national borders while preserving governments' right to regulate in the public interest.

1. Introduction

The internet has revolutionized the global trading environment and economic activity, creating new opportunities for businesses and consumers alike.[1] Both the internet and the world of e-commerce have made it possible to rely on the ability to process, transfer, and store data across national borders. Global data transfers (known as 'cross-border data flows') have accordingly become the fastest growing component of world trade and are crucial for almost every industry sector.[2]

Despite their importance to global value chains, the absence of agreed international standards has prompted a proliferation of barriers to cross-border data flows, including 'data localization measures' which require certain data to be

Email: susannah.j.hodson@gmail.com.

1 In its 2017 Information Economy Report, UNCTAD estimated that global e-commerce amounted to $25.3 trillion in 2015, 90% of which comprised business-to-business e-commerce and 10% of which comprised business-to-consumer sales. UNCTAD, 'Information Economy Report 2017' (2017) xiii, http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf (accessed 5 March 2018).

2 Michael Mandel, 'Data, Trade and Growth', Progressive Policy Institute (Policy Brief, 24 April 2013), www.progressivepolicy.org/wp-content/uploads/2014/04/2014.04-Mandel_Data-Trade-and-Growth.pdf (accessed 5 March 2018).

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

stored within national borders.[3] Such measures have disrupted trade flows and increased operating costs for businesses.[4] While there is insufficient empirical evidence to quantify precisely the costs of such restrictions, data localization is commonly regarded as one of the most significant contemporary trade barriers facing digitally enabled businesses.[5]

Data localization measures have been implemented by developed and developing countries alike.[6] Among the countries that have introduced such measures over the last decade are: Australia, Canada, China, the European Union (EU), India, Indonesia, Republic of Korea, Nigeria, Russia, Turkey, and the USA.[7] The nature and scale of these measures varies greatly. Countries such as China and Russia have introduced far-reaching blanket local storage requirements, whereas other countries, including Canada and Australia, have implemented narrower sector-specific restrictions targeting personal data and other specific classes of information.[8] Even the USA, which has traditionally championed the free flow of data to serve the interests of its tech giants, has introduced data localization restrictions which apply to cloud computing service providers that work for the Department of Defence and information systems that store or transmit federal tax information.[9]

The range of approaches to regulating cross-border data flows often reflects different cultural values, especially with regard to sensitive issues such as privacy and security. In recent years, high profile international cyber attacks and espionage activity have increased the public interest in data protection. In particular, public pressure to protect personal information increased following the Snowden leaks of 2013, which revealed the extent of US surveillance activities targeting American and foreign citizens. The Snowden leaks were especially controversial

3 While there is no universally accepted definition of 'data localization', this article interprets the term as measures which require certain data to be physically stored on servers or data centres within a country's territory.

4 Daniel Castro and Alan McQuinn, 'Cross-Border Data Flows Enable Growth in All Industries', Information Technology and Innovation Foundation (February 2009) 9.

5 Asia Cloud Computing Association, *Cloud Readiness Index 2016* (2016) 14.

6 Neha Mishra, 'Data Localisation Laws in a Digital World' (4 December 2015) *Public Sphere*, 137, www.publicspherejournal.com/wp-content/uploads/2016/02/06.data_protection.pdf (accessed 5 March 2018).

7 Information Technology Industry Council Press Release, 'Snapshot of Data Localisation Measures' (19 January 2017), www.itic.org/public-policy/SnapshotofDataLocalizationMeasures1-19-2017.pdf (accessed 28 May 2018).

8 Australia has restrictions in place relating to personally identifiable health records and Canada has provincial restrictions relating to personal information. For an analysis of the data localization measures throughout the world, see Information Technology Industry Council Press Release, 'Snapshot of Data Localisation Measures' (29 July 2016), www.itic.org/public-policy/SnapshotofDataLocalizationMeasures7-29-2016.pdf (accessed 5 March 2018).

9 Nigel Cory, 'Cross Border Data Flows: Where are the Barriers and What do They Cost?', Information Technology and Innovation Foundation (1 May 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost (accessed 30 May 2018).

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

in the EU, where deep sensitivities over the protection of personal information reflect acute memories of communist-era state surveillance. Fundamental differences in the EU and US ideologies and approaches to data protection and privacy have been a source of tension in the *Transatlantic Trade and Investment Partnership* (TTIP) negotiations, which are currently stalled.[10] This article does not take a position on the relative merits of any jurisdiction's privacy frameworks, but recognizes that the protection of privacy is a legitimate policy objective which should be accommodated in trade rules governing data transfers.

Some data localization measures appear to be motivated by traditional protectionist impulses to increase local investment and employment opportunities. For example, in 2012 Indonesia introduced wide-reaching data localization measures as part of the Government's strategy to correct its trade deficit and improve infrastructure.[11] While such policies may increase infrastructure spending and employment opportunities in the short term, they can be counterproductive, with initial investments offset by subsequent efficiency losses and reduced inward investment in the long term.[12]

Data localization measures are expected to continue to proliferate in coming years, partly as a consequence of heightened political concerns about privacy, security, and data protection. In addition, jurisdictional uncertainty associated with internet regulation may also prompt governments to introduce data localization measures in an attempt to subject data to local legislation and law enforcement.[13] The propagation of such measures will fragment firms' global operations by forcing suppliers to use separate data centres in each country in which they operate. This in turn will impede businesses' ability to process and analyse large quantities of data; an essential operating function for most multinational firms as well as an increasing number of SMEs.

While policymakers face increased pressure to address data localization restrictions within the multilateral trading system, the effectiveness of existing WTO rules to discipline adequately data localization measures remains inconclusive. The internet was in its infancy when the General Agreement on Trade in Services (GATS) was concluded in 1994, so it is little surprise that the GATS does not expressly address digital trade barriers. Nonetheless, GATS disciplines do provide some safeguards against digital trade barriers – including data localization

10 See James Fontanella-Khan, 'Data Protection Ruled Out of EU-US Trade Talks', *Financial Times* (5 November 2013). For a comparison of EU and US data protection laws, including the EU's new General Data Protection Regulation 2016/679 (May 2018), see DLA Piper 'Data Protection Laws of the World: Full Handbook' (1 June 2018), www.dlapiperdataprotection.com (accessed 3 June 2018).

11 Government Regulation 82/2012 (Indonesia). See also Arianto Patunru and Sjamsu Rahardja, 'Trade Protectionism in Indonesia: Bad Times and Bad Policy', Lowy Institute (May 2015).

12 Castro and McQuinn, 'Cross-Border Data Flows Enable Growth in All Industries', supra n. 4, 9.

13 Shin-Yi Peng and Han-Wei Liu, 'The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?', 2 *Journal of World Trade* (2017) 183, 195.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

measures – that discriminate against foreign suppliers or restrict market access in sectors for which Members have taken commitments. However, the absence of specific rules means that significant uncertainty prevails over how the GATS might be applied to data localization measures in the event of a dispute.

Panels and the Appellate Body have allayed this uncertainty to some extent by adopting an evolutionary and technology-neutral approach to interpreting the GATS, finding that commitments are presumed to encompass all modes of supply, including online delivery, unless a Member explicitly specifies a limitation in its schedule. However, the ongoing WTO negotiating stalemate has prevented these decisions from being transposed into textual provisions. Relying on judicial activism rather than consensus-based WTO negotiations to determine the coverage of internet services under the GATS diminishes legal certainty and leads to outcomes which do not necessarily reflect the views of the WTO membership.

In the absence of meaningful progress at the multilateral level, bilateral and plurilateral free trade agreements (FTAs) have developed new models to address contemporary digital trade barriers.[14] In particular, the *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (CPTPP) contains the most ambitious provisions on data transfers and storage of any FTA to date.[15] Though regional solutions are inherently inferior to multilateralism insofar as they involve only a subset of WTO Members and can distort global trade flows, the CPTPP nonetheless represents an innovative precedent for addressing data issues in future trade agreements.

The CPTPP data framework improves on GATS disciplines by proscribing a broader range of data localization measures, including some measures which do not otherwise breach national treatment or market access obligations and would therefore not be disciplined under the GATS. The CPTPP rules also move away from archaic distinctions between modes of supply and service sectors which underlie the GATS approach to scheduling. Importantly, the CPTPP framework strikes a balance between facilitating businesses' growing need to transfer and store data across national borders while preserving governments' right to regulate in the public interest. The latter is achieved through the introduction of a new

14 *Free Trade Agreement between the United States of America and the Republic of Korea*, signed 30 June 2007 [2012] (entered into force 15 March 2012); *Comprehensive and Progressive Agreement for Trans-Pacific Partnership*, signed 8 March 2018 (not yet entered into force); *Third Review of the Australia – Singapore Free Trade Agreement*, signed 13 October 2016 [2017] (entered into force 1 December 2017).

15 *Comprehensive and Progressive Agreement for Trans-Pacific Partnership*, signed 8 March 2018 (not yet entered into force). The revised CPTPP incorporates the provisions of the original TPP (including the E-Commerce Chapter) *mutatis mutandis* except for a very limited number of provisions which have been suspended following the late withdrawal by the United States. The TPP data provisions remain unchanged in the CPTPP text.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

exception to preserve the autonomy of governments to restrict data flows in pursuit of a legitimate public policy objective. While there is some ambiguity about the scope of this exception, its inclusion is important given that digital technologies are rapidly evolving and the full range of potential intersections between data trade liberalization and policy interests remains unknown.

Scholars have analysed data localization trends globally as well as the applicability of the GATS and free trade agreements to data localization measures.[16] This article contributes to existing scholarship by providing a comparative analysis of the effectiveness of the GATS and CPTPP frameworks for disciplining such measures.

Sections 2 and 3 of this paper consider the adequacy of both the GATS and emerging FTA rules at addressing data localization measures, while section 4 compares the effectiveness of the two frameworks.

2. The applicability of WTO rules to data localization measures

In this section, I examine the effectiveness of GATS rules in disciplining data localization measures. My analysis suggests that, despite the absence of specific WTO disciplines on data transfers, the GATS does provide a baseline of protection against measures which restrict the cross-border transfer and storage of data, especially where restrictions are far-reaching and discriminate against foreign suppliers. Nonetheless, I contend that GATS rules are ultimately deficient insofar as they apply archaic distinctions between modes of supply and service sectors and fail to discipline trade-distorting data localization measures which do not contravene national treatment or market access obligations.

The lack of specific provisions addressing data transfers means significant ambiguity prevails with regard to how the existing rules might be applied to data localization measures in the event of a dispute. Although two WTO disputes to date have considered the applicability of the GATS to internet services, no panel has yet considered the applicability of GATS rules to data localization measures.[17]

16 See, e.g., Anupam Chander and Uyen Le, 'Data Nationalism', 64 *Emory Law Review* (2015) 677; Peng and Liu, 'The Legality of Data Residency Requirements', supra n. 13; Lee Tuthill, 'Cross-Border Data Flows: What Role for Trade Rules?', in Pierre Sauvé and Martin Roy (eds.), *Research Handbook on Trade in Services* (Elgar Online, 2016) 357; Mishra, 'Data Localisation Laws in a Digital World', supra n. 6; John Selby, 'Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?', 25(3) *International Journal of Law and Information Technology* (2017) 213; Mira Burri. 'The Regulation of Data Flows through Trade Agreements', 48 *Georgetown Journal of International Law* (2017) 407.

17 The two WTO disputes which have considered the applicability of the GATS to internet services are: Panel Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/R, adopted 10 November 2004, para. 6.287 (*US–Gambling*); Panel Report, *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, WT/DS363/R, adopted 12 August 2009, para. 412 (*China–Publications and Audiovisual Products)*.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

This absence of jurisprudence generates legal uncertainty about the extent to which data localization measures are permissible under the GATS.

2.1 *The coverage of e-commerce under the WTO framework*

The General Agreement on Tariffs and Trade (GATT) was established in 1947 to replace the pre-World War II system of competitive imperial trading blocs with a single global framework for world trade. Subsequent negotiation rounds added new Members and reduced barriers to international trade in goods. The GATT remained the principal treaty governing international trade until the WTO was established in January 1995, following the conclusion of the Uruguay Round of multilateral trade negotiations. A number of new agreements were added at this time, including the GATS. But as digital trade was still in its infancy in the mid-1990s these agreements did not include specific provisions in respect of e-commerce.

In the years since, the WTO has come under increasing pressure from Members and industry to take a more active role in addressing barriers to digital trade. However, multilateral negotiations on digital trade issues have been challenging. The Doha Round, which was launched in 2001, has not substantially considered e-commerce. Such issues were sequenced behind more politically sensitive issues such as agriculture trade liberalization, which remains unresolved. In addition, some Members insisted on linking any concessions on e-commerce to the extension of concessions to developing countries in other areas; a demand which has proven similarly difficult to reconcile.[18]

The 1998 WTO Ministerial Council established a WTO Work Programme to 'examine all trade-related issues relating to global electronic commerce'.[19] Shortly after the Work Programme was established however, it became clear that Members held widely divergent views on what e-commerce outcomes the WTO membership should pursue. In particular, progress was constrained by differences in views over whether digital products (such as software, movie files and music files) should be classified as goods or services and which WTO Agreement (i.e. the GATT or GATS) would accordingly govern these products.[20] Such threshold questions still remain unresolved and continue to complicate e-commerce negotiations in the WTO.

The only concrete outcome that the WTO has delivered on e-commerce to date has been an agreement by Members not to impose customs duties on electronic transmissions.[21] This is known as the 'moratorium' on customs duties and was first agreed by Members in 1998 with successive extensions agreed at every subsequent biennial WTO Ministerial Conference. While the moratorium is symbolically

18 Sacha Wunsch-Vincent, 'WTO E-Commerce and Information Technologies: From the Uruguay Round through the Doha Development Agenda: A Report for the UN IDT Task Force', Markle Foundation (2005) 47–51, www.iie.com/publications/papers/wunsch1104.pdf (accessed 5 March 2018).

19 WTO, 'Declaration on Electronic Commerce', WT/MIN(98)/DEC/2, adopted 20 May 1998.

20 Wunsch-Vincent, 'WTO E-Commerce and Information Technologies', supra n. 18, 10.

21 WTO, 'Declaration on Electronic Commerce', WT/MIN(98)/DEC/2, adopted 20 May 1998.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

important in signalling Members' commitment to facilitating digital trade, its commercial impact is negligible given the prohibitive administrative difficulty for any Member to impose discriminatory customs duties on electronic content.[22]

In preparation for the Eleventh WTO Ministerial Conference (MC11), held in Buenos Aires in December 2017, three non-papers on e-commerce were circulated by the USA, the EU and others, and Brazil.[23] These non-papers were intended to guide discussions about what the WTO could achieve on e-commerce. Both the non-papers tabled by the EU and others and the USA cited disciplines on cross-border data restrictions as an area where the WTO could potentially facilitate digital trade. The third non-paper tabled by Brazil did not include any reference to data localization, reflecting lingering sensitivities in Brazil following the political fallout over an unsuccessful attempt to introduce broad data localization requirements as part of Brazil's Civil Rights Framework for the Internet in 2014.[24]

While these non-papers were intended to be mapping exercises rather than formal proposals, they suggest there is a ground-swell of interest among some Members, especially developed countries, in addressing data localization barriers in the WTO. However, other Members, particularly the Africa Group, have strongly resisted the establishment of new multilateral rules on e-commerce in the WTO. Rwanda circulated a statement to this effect on behalf of the Africa Group on 6 December 2017, which condemned the establishment of 'hard rules' prohibiting data localization requirements amongst other things.[25] Given this North–South rift on what is achievable in the WTO on e-commerce and data flows, it is difficult to foresee the development of new disciplines on data localization in the near future.

2.2 *The applicability of GATS rules to data localization measures*

As most digital trade does not involve the transfer of physical goods, the most relevant WTO Agreement for addressing data localization restrictions is the GATS.[26]

22 Wunsch-Vincent, 'WTO E-Commerce and Information Technologies', supra n. 18, 319–320.

23 Work Programme on Electronic Commerce, Non-Paper from the United States, JOB/GC/94, circulated 4 July 2016; Work Programme on Electronic Commerce, Non-Paper on Trade Policy, the WTO and the Digital Economy from Canada, Chile, Colombia, Côte d'Ivoire, the European Union, the Republic of Korea, Mexico, Paraguay, and Singapore, JOB/GC/97/Rev.1, circulated 22 July 2016; Work Programme on Electronic Commerce, Non-Paper from Brazil, JOB/GC/98, circulated 20 July 2016. See Marilia Maciel, 'E-Commerce in the WTO: the Next Arena of Internet Policy Discussions?', Diplomacy Blog (20 September 2016), www.diplomacy.edu/blog/e-commerce-wto-next-arena-internet-policy-discussions (accessed 5 March 2018).

24 See Maciel, 'E-Commerce in the WTO', supra n. 23. See also Dan Cooper, 'Brazil Enacts Marco Civil Internet Civil Rights Bill', Inside Privacy (28 April 2014), www.insideprivacy.com/international/brazil-enacts-marco-civil-internet-civil-rights-bill/ (accessed 5 March 2018).

25 Work Programme on E-Commerce, Statement by the Africa Group WT/MIN(17)/21, circulated 6 December 2017.

26 Given that data can be integrated into goods such as smartphones, the GATT is also relevant to disciplining data transfers; however, for expediency this article does not assess the possible application of other WTO agreements to data localization measures. Hosuk Lee-Makiyama advocates that the goods

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

The GATS, which entered into force in January 1995, extended the multilateral trading system to trade in services. GATS disciplines apply to data localization measures in two ways. First, digital technologies are covered to the extent they enable other categories of services, such as electronic payment services to be delivered across borders (considered in section 2.2.1 below). Secondly, some data services, such as database and data processing services, are specifically disciplined in Members' schedules of specific commitments (schedules) which list Members' market access and national treatment commitments with respect to all other Members. The applicability of market access commitments to data localization measures is considered in section 2.2.3 and the applicability of national treatment commitments to such measures is considered in section 2.2.4. The circumstances in which a prima facie breach may be justified under the GATS exceptions is analysed in sections 2.2.5 and 2.2.6.

2.2.1 Data processing or transferring integral to the supply of a service

The GATS applies to 'measures affecting trade in services'.[27] While the term 'services' is not itself defined in the GATS, Article 1.2 of the GATS clarifies the scope of the Agreement, defining 'trade in services' by reference to four modes through which services can be supplied.

Of the four, the mode most relevant to internet services trade is that referred to as 'mode 1'.[28] These services are delivered on a cross-border basis, with the service supplier and consumer in different countries. Data transfers may be captured in Members' mode 1 commitments to the extent that they enable the cross-border delivery of other services. This inclusion is significant given that approximately half of global trade in services is enabled by technologies dependent on the internet.[29] Furthermore, Article XXVIII(b) of the GATS states that the 'supply of a service' includes the 'production, distribution, marketing, sale and delivery of a service'. Hence, data flows are encompassed in Members' mode 1 commitments insofar as they enable another kind of service to be sold, distributed, or delivered across borders.[30]

Cross-border service supply under the GATS includes services supplied through electronic means. This understanding was endorsed by the Panel in *US–Gambling*, which considered whether a US measure prohibiting online gambling services was

and services aspects of data transfers should be considered under a single horizontal framework. See Hosuk Lee-Makiyama, 'Cross-Border Data Flows in the Post Bali Agenda', in Simon Evenett and Alejandro Jara, *Building on Bali* (VOX ebook, 18 December 2013) 165.

27 Article 1.1 of the GATS.

28 While it is also arguable that internet services can fall within consumption abroad ('mode 2'), in *US–Gambling* the Panel considered online gambling services fell within mode 1; Panel Report, *US–Gambling*, paras. 3.43, 6.415, 6.666.

29 Cory and Atkinson, 'Financial Data does not Need or Deserve Special Treatment in Trade Agreements', supra n. 9, 2.

30 See also Daniel Crosby, 'Analysis of Data Localization Measures under WTO Services Trade Rules and Commitments', E15 Initiative Policy Brief (March 2016) 2.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

in breach of the USA's market access commitments.[31] The Panel concluded that unless a Member explicitly specified a restriction on a certain mode of supply in its schedule, the Member would be presumed to have taken a commitment with respect to all means of delivery, including via electronic means.[32] Notably, the Panel stated:

> we conclude that mode 1 includes all means of delivery. We are of the view that when a Member inscribes the word "None" in the market access column of its schedule for mode 1, it commits itself not to maintain measures which prohibit the use of one, several or all means of delivery under mode 1 in a committed sector or sub-sector. This is especially so in sectors and sub-sectors where cross-border supply is effected essentially if not exclusively through the Internet.[33]

In reaching this conclusion, the Panel applied the concept of 'technological neutrality' to its interpretation of GATS disciplines.[34] The Panel cited the *Work Programme on Electronic Commerce – Progress Report to the General Council*, adopted by the Council for Trade in Services on 19 July 1999, which endorsed the principle of technological neutrality in interpreting GATS commitments.[35]

The decision remains influential jurisprudence suggesting that the GATS will be interpreted in an evolutionary way. While the Appellate Body did not pronounce on the Panel's discussion on the principle of technological neutrality in the subsequent appeal in *US–Gambling*, five years later the Appellate Body reinforced the applicability of this principle to the GATS in *China–Publications and Audiovisual Products*. In that dispute, the Appellate Body held that China's scheduled commitment for 'sound recording distribution services' also encompassed electronic distribution.[36]

The principle of technological neutrality is an important doctrine for assessing the extent to which data localization measures are disciplined by Members' GATS commitments. The principle extends Members' sectoral commitments to encompass the online delivery of services, even where the emergence of an online industry could not have been foreseen by GATS negotiators. In relation to data flows, application of the principle of technological neutrality suggests that a data localization measure which impedes the online delivery of a service could arguably breach a Member's mode 1 commitment unless the Member explicitly specified a restriction in its schedule.

31 Panel Report, *US–Gambling*, para. 6.287.

32 Panel Report, *US–Gambling*, para. 6.285.

33 Ibid. para. 6.287. The Panel's reference to technological neutrality was not referred to by the Appellate Body in its review of this decision; Appellate Body Report, *US– Gambling*, WT/DS285/AB/R, adopted 7 April 2005.

34 Ibid. para. 6.285.

35 Ibid. para. 6.285 footnote 846.

36 Appellate Body Report, *China–Publications and Audiovisual Products,* paras. 408, 412.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

While WTO panels and the Appellate Body have not yet explicitly considered the extent to which data transfers are encompassed in Members' GATS commitments, in *China–Electronic Payments* the Panel held that Members' scheduled commitments would encompass component services which are integral to the supply of the relevant service. The Panel in *China–Electronic Payments* applied the principle of technological neutrality to reach the conclusion that China's commitment for 'payment and money services' included electronic payment services (EPS). The USA argued that to interpret China's commitment as excluding EPS would frustrate the commitment, as 'EPS is integral to the processing of credit, charge, debit and other payment card transactions'.[37] China argued that EPS did not have the character of a single, integrated service as it was comprised of inputs commonly supplied by more than one supplier.[38] The Panel endorsed the USA's argument that EPS is covered by China's financial services commitments, concluding:

> [i]n our view, there cannot be any "payment service" and "money transmission service" if the payment is not effected and the money not transferred from the customer's account to the merchant's account […] these activities, even though they are not explicitly listed in subsector (d), are necessarily included within the scope of the definition of that subsector because they must operate together for the payment and money transmission service to be supplied.[39]

In finding that EPS amounted to a single 'integrated service', the Panel stated that the determination of whether a service amounts to an integrated service involves an assessment of 'whether the component services, when combined together, result in a new and distinct service'.[40] The fact that inputs were supplied by more than one supplier did not preclude such a finding.[41] Hence, the Panel decision in *China–Electronic Payments* suggests that a scheduled commitment includes data transfers where such transfers constitute part of an integrated service; that is, if combined together the inputs (including the data transfers) result in a new and distinct service. Data transfers will also be covered to the extent they are integral to the supply of a service in a committed sector.

2.2.2 Commitments on computer and other related services and telecommunications services

The current GATS services sectoral classification list (W/120) is based on the Central Product Classification (CPC) system, which was first published by the

37 Panel Report, *US–Gambling*, Annex E-1 Executive Summary of the Oral Statement of the United States at the Second Substantive Meeting, para. 3.

38 Panel Report, *China–Certain Measures Affecting Electronic Payment Services*, WT/T/DS413/R, adopted 16 July 2012, para. 7.182 (*China–Electronic Payment Services*).

39 Panel Report, *China–Electronic Payment Services*, para. 7.180. See also Crosby, 'Analysis of Data Localization Measures under WTO Services Trade Rules and Commitments', supra n. 30, 4.

40 Ibid. para. 7.184.

41 Ibid. para. 7.184.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

United Nations Statistical Division in 1991. As the internet was in its infancy when the CPC was developed, the CPC does not include internet services. Such services are not neatly accommodated within Members' schedules, as they are both an enabler of other services as well as a distinct services sector.[42] In examining the deficiency of the W/120 framework in this regard, Hosuk Lee-Makiyama of ECIPE states: '[a]s neither the internet nor data flows are always a 'sector' or a mode of delivery, current GATS architecture represents a systemic problem'.[43]

In addition to the W/120's artificial distinctions between services and modes of supply, the ambiguity in housing internet services within a W/120 services category has resulted in intractable and seemingly irreconcilable debates about whether such services should fall within the categories of 'computer and related services' or 'telecommunications services'.[44] Differences in view are rooted in divergent cultural and philosophical positions, including between major players such as the USA and the EU and, as with analogous debates about other new services, seem likely to impede any efforts to update the W/120 in the near future.[45]

Most WTO Members have taken at least partial commitments for 'computer and related services' in their GATS schedules.[46] Depending on the nature of the restriction and its impact on trade, a data localization measure could breach a Member's market access and national treatment commitments for the subsectors of data processing services (CPC 843), database services (CPC 844), and data preparation services (CPC 849). Members' commitments for the above subsectors vary, so assessing whether a data localization measure is inconsistent with a Member's commitments necessarily depends on a determination of which W/120 subsector the relevant internet service falls within. For example, China has made full commitments on the cross-border supply of 'data processing services' but has made no such commitments for 'database services'. Therefore, if an internet service was deemed to be a 'data processing service', China would be obliged not to restrict

42 Tim Wu, 'The World Trade Law of Internet Filtering', 7 *Chicago Journal of International Law* (2006) 263, 281–282.

43 Lee-Makiyama, 'Cross-Border Data Flows in the Post Bali Agenda', supra n. 26, 165.

44 WTO, *Work Programme on Electronic Commerce – Progress Report to the General Council*, WT/GC/103, adopted 27 July 1999, 3.

45 Mira Burri *et al*., 'The Protection and Promotion of Cultural Diversity in a Digital Networked Environment: Mapping Possible Advances to Coherence', in Thomas Cottier and Panagiotis Delimatsis, eds., *The Prospects of International Trade Regulation* (Cambridge University Press, 2011) 369, 369–393.

46 The W/120 breaks down this sector into the following subsectors:

i. Consultancy services related to the installation of computer hardware (CPC 841).
ii. Software implementation services (CPC 842).
iii. Data processing services (CPC 843).
iv. Database services (CPC 844).
v. Maintenance and repair services of office machinery and equipment including computers (CPC 845).
vi. Other computer services, including data preparation services (CPC 849).

For analysis of members' commitments on 'computer and related services', see Crosby, 'Analysis of Data Localization Measures under WTO Services Trade Rules and Commitments', supra n. 30, 11–16.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

its cross-border supply. However, if the service in question was categorized as a 'database service', China would have no such obligation.[47]

Commitments on 'telecommunications services', specifically those relating to 'online information and database retrieval', may also be relevant in disciplining digital trade barriers.[48] However, here again Members' views diverge as to whether commitments on basic telecommunication services include internet services, a question which has not been resolved in WTO negotiations.[49]

Members' commitments for telecommunications services tend to be less liberal than for computing and related services. This is partially attributable to telecommunications being a sensitive sector which is often monopolized by an incumbent state-owned enterprise. In addition, Mira Burri of the University of Lucerne suggests that WTO Members generally made more liberal commitments for computing and related services as at the time services schedules were negotiated during the Uruguay Round this was a new sector which was largely devoid of regulation.[50]

2.2.3 *Market access*

The first WTO obligation under which data localization measures might be captured is market access. Paragraph 2 of Article XVI of the GATS provides an exhaustive list of limitations that constitute a breach of market access for sectors in which a Member has undertaken market access commitments in their schedule.

Where a Member has made full market access commitments for the relevant sector in its schedule, the Member cannot impose a market access barrier which would restrict foreign firms from entering or operating in the market in accordance with paragraph 2 of Article XVI. For example, if a Member which has made full market access commitments for computing services introduced a measure requiring foreign suppliers to enter into a joint venture with a local firm in order to supply database services, the Member would be in breach of subparagraph 2(e) of Article XVI which disciplines 'measures which restrict or require specific types of legal entity or joint venture through which a service supplier may supply a service'.

As outlined above, WTO panels and the membership have confirmed that a market access commitment for mode 1 (cross-border supply) encompasses all means of delivery, including via electronic means unless otherwise specified.[51] Therefore, a prohibition or licensing restriction on cross-border data transfers

47 Wu, 'The World Trade Law of Internet Filtering', supra n. 42, 282, 283. See also, Fredrik Erixon, Brian Hindley, and Hosuk Lee-Makiyama, *Protectionism Online: Internet Censorship and International Trade Law*, ECIPE (2009) 16, 10.

48 Central Product Classification 7523.

49 WTO, *Work Programme on Electronic Commerce – Progress Report to the General Council*, WT/GC/103, adopted 27 July 1999, 3.

50 Mira Burri, 'The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation', 51, *UC Davis Law Review* (2017) 51, 84.

51 See Panel Report, *US–Gambling*, para. 6.287; WTO, *Work Programme on Electronic Commerce – Progress Report to the General Council*, WT/GC/103, adopted 27 July 1999, 33.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

could breach a Member's mode 1 market access commitments for computing services if it effectively prohibited the delivery of database services through electronic means.

In particular, a measure which prohibited services from being delivered via electronic means could be deemed to constitute a quota on the 'total number of service operations or on the total quantity of service output' under subparagraph 2(c). This view was endorsed by the Appellate Body in *US–Gambling*, which found that the USA's prohibition on the supply of all online gambling services fell within the scope of subparagraph 2(c) of Article XVI as the measure effectively constituted a 'zero quota'. In reaching this conclusion, the Appellate Body reasoned:

> the measures at issue, by prohibiting the supply of services in respect of which a market access commitment has been taken, amount to a "zero quota" on service operations or output with respect to such services. As such, they fall within the scope of Article XVI:2(c).[52]

Similarly, in *Mexico–Telecoms*, the Panel found that a Mexican government measure, which required international telecommunications traffic to be routed through the facilities of a licenced carrier, was inconsistent with subparagraphs 2(a), (b), and (c) of Article XVI as it effectively established a zero quota on cross-border supply of these services by restricting their provision to suppliers commercially present in Mexico.[53] However, ultimately the Panel ruled that Mexico did not violate its obligations because it had not scheduled commitments for the cross-border supply of telecommunications services over capacity leased by the supplier.[54]

The jurisprudence developed in *US–Gambling* and *Mexico–Telecoms* suggests that a measure which impedes the supply of a certain class of services electronically, for example through prohibiting the transfer or storage of certain classes of data, could constitute a 'zero quota' in breach of a market access commitment. As discussed above however, determining whether a data localization measure breaches a Member's market access commitment would necessarily involve an examination of which W/120 subsector the relevant services fell within and what market access commitments the Member had made for that subsector.

2.2.4 National treatment

The second WTO obligation relevant to disciplining data localization measures is the national treatment obligation, which prohibits discrimination against foreign suppliers. Article XVII, which is the cornerstone of the GATS, prohibits discrimination against foreign suppliers in sectors for which Members have taken commitments in their schedules.

52 Appellate Body Report, *US–Gambling*, para. 251.

53 Panel Report, *Mexico–Measures Affecting Telecommunications Services,* WT/DS204/R, adopted 2 April 2004, para. 4.124 (*Mexico–Telecoms)*.

54 Panel Report, *Mexico–Telecoms*, para. 7.294.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

Unlike the equivalent provision in the GATT, the GATS national treatment obligation only applies to measures which affect trade in services to the extent that a Member has listed a commitment to provide national treatment for the relevant sector in its schedule. In *China–Electronic Payment Services*, the Panel emphasized that the national treatment obligation applies to both de facto and de jure discrimination, and stated that the objective of the obligation was to 'ensure equal competitive opportunities for like services of other Members'.[55]

In *Korea–Various Measures on Beef*, the Appellate Body stated that the determination of whether foreign firms receive 'less favourable' treatment than domestic firms requires an examination of 'whether a measure modifies the conditions of competition in the relevant market to the detriment of imported products'.[56] The Appellate Body held that a measure will be deemed to accord less favourable treatment to foreign suppliers where a less trade-restrictive alternative was 'reasonably available', though the burden of proof to establish that such an alternative exists would fall on the complainant.[57] The Panel in *China–Electronic Payment Services* endorsed the application of this test to Article XVII of the GATS, stating:

> the examination of whether a measure involves 'less favourable treatment'[…] must be grounded in close scrutiny of the 'fundamental thrust and effect of the measure itself'. This examination cannot rest on simple assertion, but must be founded on a careful analysis of the contested measure and of its implications in the marketplace.[58]

This jurisprudence suggests that determining whether a data localization measure accords less favourable treatment under Article XVII requires close analysis of the effect and trade impact of the measure. A far-reaching data localization measure which impedes international trade and is motivated by protectionist impulses is more likely to fall foul of the national treatment obligation than a narrower data localization measure which targets a legitimate regulatory objective and has a more limited impact on trade.

Footnote 10 to Article XVII further clarifies that Members are not required to redress inherent competitive disadvantages attributable to the 'foreign character' of service suppliers. Hence, the fact that it may be more costly for foreign suppliers to meet a data localization requirement by virtue of their 'foreign character', including their lack of local infrastructure or familiarity with the operating environment, would not necessarily constitute a breach of a Member's national treatment commitment.

55 Panel Report, *China–Electronic Payment Services,* para. 7.700.

56 Appellate Body Report, *Korea–Various Measures on Beef*, WT/DS161/AB/R, adopted 11 December 2000, para. 137 (*Korea–Various Measures on Beef*).

57 Ibid. paras. 163, 166.

58 Panel Report, *China–Publications and Audiovisual Products*, para. 7.1131, endorsing Appellate Body Report, *United States–Tax Treatment for 'Foreign Sales Corporations' (Article 21.5),* WT/DS108/AB/RW, adopted 14 January 2002, para. 215 (*US–Foreign Sales Corporations*).

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

2.2.5 *General exceptions*

If a measure constitutes a prima facie breach of the market access or national treatment provisions of the GATS, the breach may nonetheless be exempted under the general or national security exceptions contained in Article XIV and Article XIV*bis* of the GATS respectively. The circumstances in which these exceptions apply are considered below.

The general exceptions contained in Article XIV of the GATS permit Members to deviate from market access and national treatment commitments in order to adopt or enforce measures necessary to protect a range of policy interests. In the case of restrictions on the transfer or storage of data, the most relevant provisions are those contained in subparagraphs (a) and (c)(ii) of Article XIV relating to measures necessary to protect 'public morals or to maintain public order' and the 'privacy of individuals' respectively.

The 'public morals' exception in subparagraph (a) may exempt a measure restricting cross-border data transfers where the measure blocks content or services which are considered to conflict with societal values. *US–Gambling* is one of the few disputes to have considered the application of the GATS public morals exception. In this dispute, the USA invoked the public morals exception in order to attempt to justify the prima facie breaches of its market access and national treatment commitments resulting from its ban on online gambling services.

The Panel in *US–Gambling* found that Members have broad discretion to determine the level of protection they consider appropriate to uphold public morals and public order under Article XIV.[59] In the more recent dispute of *EC–Seals,* which considered the equivalent GATT exception, the Appellate Body endorsed the jurisprudence developed in *US–Gambling*, reiterating that Members have autonomy to define the concept of public morals 'according to their own systems and scales of values'.[60] In addition, the Appellate Body rejected the argument that a Member must be consistent in its regulatory protections of various public morals concerns, concluding that 'Members may set different levels of protection even when responding to similar interests of moral concern.'[61] This jurisprudence suggests that a measure which mandates the localization of a certain class of data (for example health records) but not other data which may give rise to similar policy concerns (for example social security records) may nonetheless benefit from the public morals exception.

Laws or regulations which limit the transfer or storage of data in order to protect the privacy of individuals may also fall within GATS exceptions contained in subparagraph (c)(ii), provided they are not applied in a manner which constitutes

59 Panel Report, *US–Gambling*, para. 6.461.

60 Appellate Body Report, *European Communities – Measures Prohibiting the Importation and Marketing of Seal Products*, WT/DS400/AB/R, adopted 22 May 2014, para. 5.199 (*EC–Seals*).

61 Ibid. para. 5.200.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

arbitrary or unjustifiable discrimination or a disguised restriction on trade in services. While there is no universally accepted definition of 'privacy', this term is generally considered to encompass the protection of personal information.[62] Paragraph (c)(ii) could arguably provide an exception for restrictions such as that imposed under the EU Data Protection Directive, which prevents the transfer of personal data outside the EU to countries which the European Commission has determined do not provide an adequate level of protection for personal data.[63] However, the scope of the GATS privacy exception has not yet been tested in WTO jurisprudence.[64]

The ambit of the Article XIV exceptions is qualified by a proportionality requirement that a measure must be 'necessary' to fulfil the objective of protecting public morals. In *Korea–Various Measures on Beef*, the Appellate Body held that determining whether a measure meets the necessity standard involves a process of weighing and balancing a series of factors including: the measure's contribution to the regulation at issue, the importance of the values protected, and the measure's trade impact.[65] The Appellate Body characterized this weighing and balancing test as one 'comprehended in the determination of whether a WTO-consistent alternative measure which the Member concerned could "reasonably be expected to employ" is available', with the burden of proof falling to the complainant to establish that such an alternative exists.[66] Though initially developed in respect of the equivalent GATT exemption, the Appellate Body subsequently applied the jurisprudence developed in *Korea–Various Measures on Beef* to Article XIV of the GATS in *US–Gambling*.[67]

In assessing whether a less trade-restrictive measure is 'reasonably available' to a Member, a panel would consider whether the measure imposes an undue burden on the Member, such as prohibitive costs or substantial technical challenges. In *China–Publications and Audiovisual Products*, the Appellate Body concluded that China's censorship measures, which required importers of audiovisual products to monitor content, were not necessary to protect public morals as less trade-restrictive alternatives were reasonably available to China. In particular, it endorsed the USA's argument that a less restrictive, reasonably available alternative would have been for China to implement a system giving the Government, rather than importers, responsibility for monitoring imported reading materials for prohibited content.

62 Rolf H. Weber, 'Regulatory Autonomy and Privacy Standards under the GATS', 7, *Asian Journal of WTO and International Health Law and Policy* (2012) 1, 30.

63 European Parliament and Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data 1995 OJ L 281 (European Communities).

64 Selby, 'Data Localization Laws', supra n. 16, 218.

65 Appellate Body Report, *Korea–Various Measures on Beef*, paras. 163, 166.

66 Ibid. para. 166.

67 Appellate Body Report, *US–Gambling*, para. 306.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

Hence, a requirement to store certain data within a Member's territory may not satisfy the necessity test in Article XIV if the measure has a significant adverse impact on international trade and contributes little to the policy objective pursued. Given that industry analysts have argued that the way in which data are managed is a more important determinant of data security than where data are stored, it is conceivable that a data localization measure which does not of itself improve data security could potentially fall short of the necessity test in Article XIV.[68] Moreover, far-reaching blanket local storage requirements such as those implemented by China and Russia may not meet the necessity test if more targeted data regulations could achieve the same policy objectives in a less trade-restrictive manner.[69]

2.2.6 *Essential security exception*

Article XIV*bis* of the GATS provides an exception for substantive breaches of GATS rules for certain measures implemented on national security grounds. The notion that national security interests take precedence over trade liberalization objectives has been a central tenet of trade law and policy since the GATT was first established in 1947.[70] Accordingly, both the GATT and the GATS provide broad exceptions for measures introduced to protect national security.

While the security exception has been raised in the early stages of several GATT and WTO disputes, no WTO panel or Appellate Body jurisprudence has opined on the scope of the security exception.[71] In those cases where the security exception has initially been invoked, it has generally been withdrawn in the early stages of disputes.[72]

The essential security exception in Article XIV*bis* is generally considered to be subjective and self-defining as it refers to action which a Member 'considers necessary' for the protection of its essential security interests.[73] The subjective nature of security exceptions was endorsed by one of the first GATT panel reports, the Panel Report in *US–Export Restrictions (Czechoslovakia)*, which stated: 'every country must have the last resort on questions relating to its own security'.[74]

68 Nigel Cory and Robert Atkinson, 'Financial Data does not Need or Deserve Special Treatment in Trade Agreements', Information Technology and Innovation Foundation (2016), www2.itif.org/2016-financial-data-trade-deals.pdf (accessed 5 March 2018).

69 For an overview of the data localization measures which have been introduced by China and Russia, see Chander and Le, 'Data Nationalism', supra n. 16.

70 Peter Van den Bossche and Werner Zdouc, *The Law and Policy of the World Trade Organization* (Cambridge University Press, 2014) 595.

71 Roger P. Alford, 'The WTO Self-Judging Security Exception', *Utah Law Review* (2011) 697, 699.

72 Ibid. 727.

73 Andrew Mitchell and Jarrod Hepburn, 'Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Flows', 19 *Yale Journal of Law and Technology* (2017) 182, 205; Alford, 'The WTO Self-Judging Security Exception', supra n. 71, 699.

74 GATT, *United States: Export Restrictions (Czechoslovakia)*, Report of the Panel (8 June 1949) GATT Doc CP3/SR22 - II/28, 3; cited in Van den Bossche and Zdouc, above n. 80, 597.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

Some commentators have suggested that subparagraph 1(b)(iii) could be interpreted as having 'evolved' to encompass new kinds of 'war or other emergency in international relations', including cyber warfare.[75] Such an expansive interpretation of the security exception would suggest that the exception could provide broad justification for measures which require certain classes of data to be stored in a Member's territory to safeguard national security interests. For example, a measure requiring all data relating to key infrastructure to be physically stored within a Member's territory may arguably be exempt under subparagraph 1(b)(iii). However, Members may be reluctant to invoke Article XIV*bis* in defence of a data localization measure for fear of establishing unhelpful jurisprudence on the scope of the security exception, or subjecting their national security interests to scrutiny.[76]

2.3 *Conclusion on the effectiveness of WTO rules*

Despite the absence of specific disciplines on digital trade, GATS commitments can provide some protection against data localization measures. Panels and the Appellate Body have taken an evolutionary approach to interpreting the GATS, construing commitments broadly to encompass the online supply of services.[77] However, the lack of progress in WTO negotiations on e-commerce issues means that this jurisprudence has not yet been transposed into binding obligations in the WTO agreements. Relying on WTO dispute settlement processes to determine the coverage of internet services under the GATS rather than consensus-based WTO negotiations is suboptimal as it leads to outcomes which do not necessarily reflect the views of the WTO membership and, as a consequence, diminishes legal certainty.[78]

The effectiveness of GATS rules in addressing data localization will turn on how panels and the Appellate Body interpret the national treatment and market access disciplines, as well as respondents' scheduled commitments under the W/120. If a dispute were brought against a data localization measure which was alleged to constitute a prima facie breach of a Member's national treatment or market access commitments, much would turn on the interpretation of the GATS exceptions. But the absence of any jurisprudence expressly considering data localization measures means significant legal uncertainty remains about how such measures would be treated under the GATS.

The lack of progress at the multilateral level has prompted some Members to pursue FTAs as vehicles for developing more ambitious disciplines on a range of

75 Shin Yi Peng, 'Cybersecurity Threats and the WTO National Security Exceptions', 18 *Journal of International Economic Law* (2015) 449, 450, 453. See also Mitchell and Hepburn, 'Don't Fence Me In', supra n. 73, 205.

76 Alford, 'The WTO Self-Judging Security Exception', supra n. 71, 727.

77 Panel Report, *US–Gambling*, para. 6.287; Appellate Body Report, *China–Publications and Audiovisual Products*, para. 412.

78 See Burri, 'The Regulation of Data Flows Through Trade Agreements', supra n. 16, 417.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

contemporary trade issues, including data localization. Such provisions provide clearer guidance on the circumstances in which Parties may be permitted to restrict the transfer and storage of data, beyond the national treatment and market access provisions of the GATS. The effectiveness of these provisions, particularly those included in the CPTPP, are analysed below.

3 FTA provisions on cross-border data flows

The last 20 years have seen more than 400 bilateral and regional FTAs negotiated. The shift towards regionalism has increased the feasibility of reaching agreement on issues which remain unresolved in multilateral negotiations, including e-commerce disciplines.[79] Just like the exponential growth that has occurred in internet-based technologies, e-commerce chapters have also evolved significantly since the first FTAs came into force. Early e-commerce chapters were comparatively limited, focusing primarily on high-level provisions for online consumer protection, electronic authentication, and customs duties on electronic transmissions.[80] More recent e-commerce chapters are more ambitious and address a broader range of contemporary barriers to digital trade, including the expropriation of source code, regulation of unsolicited 'spam' messages, and cooperation on cybersecurity.[81]

The first FTA to include a provision specifically addressing cross-border data flows was the *Korea–US FTA* (KORUS).[82] However, this provision is a soft 'best endeavour' style clause, which does not impose binding obligations on Parties. The CPTPP data framework went significantly beyond the KORUS outcome as it developed binding and substantive provisions limiting the circumstances in which a Party can restrict data flows or require data to be stored within its territory. The CPTPP provides an innovative precedent for addressing data localization and represents the frontier of FTA disciplines on data transfers to date.

The CPTPP data rules have already been incorporated into, and influenced, other FTA negotiations which have been launched since the original TPP data framework was developed. One such agreement, the recent review of the *Singapore–Australia FTA*, has already entered into force, making it the first treaty to transpose the CPTPP data rules into law.[83] The CPTPP data framework could also influence

79 The first FTA containing an e-commerce chapter was the *Australia – Singapore Free Trade Agreement*, signed 17 February 2003 [2003] (entered into force 28 July 2003).

80 Article 14.14 of the CPTPP E-Commerce Chapter.

81 Articles 14.14, 14.17 and 14.16 of the CPTPP E-Commerce Chapter.

82 Article 15.8 of the E-Commerce Chapter of the *Free Trade Agreement between the United States of America and the Republic of Korea*, signed 30 June 2007 [2012] (entered into force 15 March 2012) states: 'Recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.'

83 *Third Review of the Australia – Singapore Free Trade Agreement*, signed 13 October 2016 [2017] (entered into force 1 December 2017).

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

negotiating positions for the Trade in Services Agreement (TiSA), a services-only trade agreement under negotiation between 23 Parties, including seven CPTPP signatories as well as the USA. Negotiations have been on hold since late 2016 and are intended to resume when the political context permits.[84] Although a limited subset of the overall WTO membership, the 23 TiSA Parties, which include major non-CPTPP economies such as the EU, Republic of Korea, Turkey, and Hong Kong, account for approximately 70% of global trade in services.[85] According to media reports, one of the most contentious issues in the TiSA negotiations has been divergences in views on cross-border data transfers and privacy protections.[86] Given the involvement of the EU and other European economies which were not Parties to the CPTPP, the TiSA outcome on data flows has the potential to set a new precedent on data protection.

It is worth noting that although the CPTPP is the first FTA to include binding rules on data flows and storage for all sectors, these provisions are not entirely novel. Many earlier FTAs included narrower provisions regulating the transfer of information specifically in relation to financial services.[87] These provisions, which are often overlooked, originate from the WTO Understanding on Commitments on Financial Services and permit transfers of financial information where necessary for the ordinary business of a financial service supplier. Such provisions are not considered in detail in this article given their limited scope.

3.1 CPTPP history and ratification

The original TPP was signed by trade ministers in New Zealand on 4 February 2016, following six years of negotiations. However, the agreement was subsequently overtaken by political developments, with President Trump announcing the USA's withdrawal from the TPP in January 2017.[88] This led to the collapse of the TPP given that its ratification articles effectively precluded its entry into force without the USA.[89]

84 European Commission, 'Trade Policy in Focus: Trade in Services Agreement', http://ec.europa.eu/trade/policy/in-focus/tisa/ (accessed 2 June 2018).

85 Department of Foreign Affairs and Trade, Australia, *Trade in Services Agreement*, http://dfat.gov.au/trade/agreements/trade-in-services-agreement/pages/trade-in-services-agreement.aspx (accessed 4 March 2018).

86 Inside US Trade, 'Leak Reveals TISA Parties at odds over Language on Cross-Border Data Flows', World Trade Online (30 January 2017).

87 This is part of the standard FTA practice of economies, including Australia, Canada, the European Union, Japan, the Republic of Korea, and the United States, amongst others.

88 White House (United States) 'Presidential Memorandum Regarding Withdrawal of the United States from the Trans-Pacific Partnership Negotiations and Agreement' (Press Release, 23 January 2017), www.whitehouse.gov/the-press-office/2017/01/23/presidential-memorandum-regarding-withdrawal-united-states-trans-pacific (accessed 5 March 2018).

89 The ratification provisions contained in Article 30.4 of the TPP require at least six of the original signatories accounting for 85% of the combined GDP to ratify, effectively precluding the TPP's entry into force without the USA, which accounts for approximately 62% of the total GDP of TPP signatories.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

In response to the USA's late withdrawal, the 11 remaining TPP Parties negotiated the revised CPTPP without the USA, which was signed on 8 March 2018 in Santiago, Chile. The revised agreement incorporates the bulk of the original TPP provisions (including the TPP data framework and remainder of the E-Commerce Chapter) *mutatis mutandis* with a handful of provisions suspended.[90]

Unlike the TPP, the CPTPP does not require any particular signatory to ratify in order for the Agreement to enter into force. CPTPP signatories are in the process of undertaking their domestic treaty ratification processes and the Agreement will enter into force 60 days after at least six, or at least 50% of the original signatories (whichever is smaller), have notified the completion of their domestic legal procedures.[91]

3.2 CPTPP data framework

Articles 14.11 and 14.13 of the CPTPP E-Commerce Chapter establish the framework which facilitates businesses' ability to transfer and store data across national borders.

The first element of the CPTPP data framework is Article 14.11, titled 'cross-border transfer of information by electronic means'. This article requires CPTPP Parties to 'allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business'.[92] In effect, this provision facilitates cross-border data flows by enabling service suppliers to transfer business data between the territories of CPTPP Parties. For example, if a Peruvian transport services supplier sought to transfer data relating to its operations in Vietnam to the supplier's headquarters in Peru, it would be permitted to do so unless an exception applied.

The second element of the CPTPP data framework is Article 14.13, which focuses on the location where data are stored. This article, titled 'location of computing facilities', addresses data localization measures requiring computing facilities, such as servers or data centres, to be stored within a Party's territory. It prohibits a CPTPP Party from requiring a business to 'use or locate computing facilities in that Party's territory' as a condition of conducting business there.[93] For businesses, this generates operational efficiencies by negating the costs associated with building and maintaining separate data centres in every country where they choose to operate.

Data localization measures requiring data to be stored within a country's borders necessarily restrict the transfer of data across borders, meaning there is

90 Kaori Kaneko and Takashi Umekawa, 'Trans-Pacific Trade Pact, Without the US, to be Signed in March', Reuters (23 January 2018).

91 Article 3 of the CPTPP.

92 Paragraph 2 of Article 14.11.

93 Paragraph 2 of Article 14.13.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

considerable overlap in the coverage of articles 14.11 and 14.13. Both articles are accordingly structured in a similar way and are subject to certain exceptions, outlined in section 3.3 below. Given the CPTPP data framework is novel and equivalent language cannot be found in the multilateral agreements, there remains a degree of uncertainty about how these rules will operate in practice. In order to establish whether a data localization measure is prohibited under the CPTPP data rules, Articles 14.11 and 14.13 must be interpreted in their context, in light of the CPTPP's object and purpose.[94]

Other articles of the CPTPP E-Commerce Chapter may provide relevant context for interpreting the CPTPP data rules. In particular, paragraph 1 of the 'Scope Article' (Article 14.2) recognizes the overarching importance of 'avoiding unnecessary barriers' to the use and development of e-commerce. Such a commitment may be interpreted as providing insight into the overall object of the E-Commerce Chapter, including the CPTPP data rules. In addition, Article 14.8, which is a standard FTA provision addressing the protection of personal information, may provide further context for the interpretation of Articles 14.11 and 14.13 in respect of their application to measures concerning the treatment of personal data. Paragraph 1 of Article 14.8 recognizes 'the economic and social benefits of protecting the personal information of users of electronic commerce' and paragraph 2 obliges Parties to adopt or maintain a legal framework for the protection of personal information. These provisions could be considered if a data localization measure requiring personal information to be stored within a Party's territory were to be challenged under the CPTPP's dispute settlement provisions.

Paragraphs 5 and 6 of Article 14.2 clarify that the CPTPP data rules are subject to the non-conforming aspects of Parties' schedules. While the legal drafting of these paragraphs is somewhat awkward, in effect they permit Parties to maintain measures that are otherwise inconsistent with the provisions of the CPTPP data framework where such measures are covered by a reservation scheduled in respect of another obligation under the Agreement, namely the market access, national treatment, performance requirements or senior management and board of directors obligations. However, a Party is not able to schedule such a reservation solely against articles 14.11 or 14.13.

Paragraph 3 of Article 14.2 expressly carves out government procurement and government information from the scope of the CPTPP E-Commerce Chapter.[95] This is an important exclusion from the CPTPP data rules as it clarifies that the provisions do not prevent a government from requiring any official information, such as critical infrastructure plans, classified policy advice, or social security information, to be stored on servers within a Party's territory.

94 Article 31 of the Vienna Convention on the Law of Treaties states: 'A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in light of its object and purpose.'

95 Paragraph 3 of Article 14.2 of the CPTPP E-Commerce Chapter.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

Furthermore, the definition of 'covered persons' in Article 14.1 of the E-Commerce Chapter provides an additional exclusion for financial institutions from the CPTPP data provisions. According to industry representatives involved in the US Government's CPTPP consultations, this provision was introduced in the negotiations by the USA at the instigation of the Federal Reserve, which sought to exclude financial services from the CPTPP data provisions for prudential reasons, especially in light of the difficulties regulators faced in accessing data held offshore by failing American banks during the 2008 global financial crisis.[96] In response to a backlash from the financial services industry about the potential misuse of this carve-out to justify protectionism,[97] former US Treasury Secretary Jack Lew announced a proposal to include financial services within the scope of data provisions in the USA's future free trade agreements in May 2016, but said it was too late to fix this issue in the CPTPP.[98]

The CPTPP data rules operate in parallel with the CPTPP's Cross-Border Trade in Services (CBTS) Chapter, which replicates the GATS national treatment and market access disciplines. Party-specific schedules (annexes) list non-conforming measures on a 'negative-list' basis, meaning that all services are liberalized except where Parties have specifically listed particular trade barriers or protected sectors. This approach, common to North American FTA practice, is considered to promote greater transparency and extends liberalization to new services that don't fall within the W/120 classification list. In addition, CPTPP Parties commit to a 'ratchet mechanism' which means that if the measure becomes less restrictive in the future, the more liberal treatment will become the new benchmark as well as a 'standstill mechanism' which prevents backsliding. A detailed analysis of individual Parties' scheduled commitments is not attempted in this section, which instead focuses on the substantive provisions and exceptions relevant to data transfers and storage.

3.3 Exceptions

If a data localization measure were challenged under the CPTPP dispute settlement provisions, the exception provisions would likely be pivotal in assessing whether the measure is permitted. The CPTPP data rules are subject to two categories of exceptions. First, they are subject to an article-specific exception for measures intended to achieve a 'legitimate public policy objective'. This is a novel exception, which is not included elsewhere in the CPTPP nor in any other FTA precedents. Secondly, the CPTPP data rules are subject to the horizontal general and security exceptions

96 Cory and Atkinson, 'Financial Data does not Need or Deserve Special Treatment in Trade Agreements', supra n. 9, 1, 5; Baker Donelson, 'Data Localization and the CPTPP: Financial Institutions Beware' (20 April 2016).

97 Cory and Atkinson, 'Financial Data does not Need or Deserve Special Treatment in Trade Agreements', supra n. 9, 5.

98 Inside US Trade, 'Treasury Floats Financial Services Data Fix For CPTPP', The Howard Baker Forum (25 May 2016).

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

which, though based on the GATS exceptions outlined above, deviate from GATS language in some important ways. The effect of these exceptions is analysed below.

3.3.1 Public policy exception

The CPTPP's data localization and transfer rules are subject to an article-specific exception for measures implemented in pursuit of a 'legitimate public policy objective'. This exception clarifies that the CPTPP data rules do not prevent a Party from adopting or maintaining inconsistent measures in pursuit of a legitimate public policy objective, providing that such measures do not constitute 'arbitrary or unjustifiable discrimination or a disguised restriction on trade' or impose restrictions on information transfers 'greater than are required' to achieve the objective.[99]

This exception operates in parallel with the horizontal agreement-wide exceptions. However, the horizontal exceptions (discussed below) apply to an exhaustive list of policy objectives, whereas the article-specific exception may apply broadly to any measure intended to achieve a legitimate public policy objective, thereby providing Parties with greater autonomy to pursue a broader range of policy objectives.

If a data localization measure implemented in pursuit of a public policy objective were to be challenged under the CPTPP dispute settlement mechanism, a tribunal would need to make an initial assessment of whether the policy objective is 'legitimate'.[100] The ordinary meaning of 'legitimate' suggests this imposes a relatively low bar which could encompass a wide range of policy goals, such as the protection of personal information and information security, amongst others. The obvious policy objective which would fall short of this threshold is protectionism, although it may also be difficult to establish that protectionism is the sole or even dominant policy objective where there is more than one policy goal. In one of the leading analyses of the CPTPP data provisions, Shin-Yi Peng and Han-Wei Liu of National Tsing Hua University in Taiwan suggest that CPTPP negotiators may have deliberately kept the public policy exception vague to create 'constructive ambiguity' about what policy objectives Parties may be permitted to pursue in what remains an evolving and potentially controversial area.[101]

The article-specific public policy exception replicates the requirement found in the GATS exceptions in Article XIV that measures must not be applied in a manner which would constitute 'arbitrary or unjustifiable discrimination or a disguised restriction on

99 Paragraph 3 of Articles 14.11 and 14.13 state: 'Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

a. is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

b. does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.'

100 Peng and Liu, 'The Legality of Data Residency Requirements', supra n. 13, 196.

101 Ibid.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

trade'. However, the article-specific exception deviates from GATS language by replacing the necessity test in GATS Article XIV with an alternative qualification that a measure cannot impose restrictions 'greater than are required' to achieve the policy objective. Peng and Liu infer that the term 'required' is commensurate with 'necessary' in this context.[102] However, I disagree that this can be assumed, suggesting it is inconclusive whether a tribunal would apply a necessity test if the meaning of this term were subject to a challenge. In the event of a dispute, a CPTPP tribunal would not be bound by WTO precedents and would make its own determination of the ordinary meaning of the term 'required' in its context and in light of the treaty's object and purpose. Given that negotiators selected the term 'required' rather than 'necessary', a tribunal may conclude that CPTPP Parties did not intend to apply a necessity standard here.[103]

Commentators including Burri and Andrew Mitchell and Jarrod Hepburn of the University of Melbourne suggest that the CPTPP's public policy exception is ambiguous and may be abused by Parties for protectionist purposes.[104] While I agree that there is some ambiguity about what may constitute a legitimate policy objective, the inclusion of a broad public policy exception is essential given the ongoing rapid evolution of digital technologies and the associated uncertainty surrounding the future intersections of trade liberalization and societal interests in this area. Future governments may well face increasing pressure to localize certain categories of data to address public policy concerns, for example to protect citizens' health or social security records. If a trade agreement were perceived to inhibit a government's ability to regulate in such sensitive areas, it would face a strong backlash from community stakeholders.

3.3.2 Horizontal exceptions

The E-Commerce Chapter is also subject to the exceptions contained in Chapter 29 of the CPTPP (Exceptions and General Provisions). Paragraph 3 of Article 29.1 incorporates paragraphs (a), (b), and (c) of Article XIV of the GATS *mutatis mutandis*. Hence, the GATS exceptions outlined in section 2 also apply to the CPTPP data provisions.

In addition, Article 29.7 also provides an exception for information disclosure, which does not exist in the GATS.[105] This exception clarifies that the data rules could not be interpreted to require firms to disclose trade secrets or oblige

102 Ibid. 195.

103 The Appellate Body has found that the 'necessary' test in Article XIV of the GATS imposes a relatively high standard which involves a comparison with reasonably available WTO-consistent alternatives; Appellate Body Report, *US–Gambling*, para. 317. See also Mitchell and Hepburn, 'Don't Fence Me In', supra n. 73, 210.

104 See Burri, 'The Regulation of Data Flows through Trade Agreements', supra n. 16, 433; Mitchell and Hepburn, 'Don't Fence Me In', supra n. 73, 210.

105 Article 29.7 states: 'Nothing in this Agreement shall be construed to require a Party to furnish or allow access to information, the disclosure of which would be contrary to its law or would impede law

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

governments to provide information in a way that would be contrary to their law or public interests.

Article 29.2 of the CPTPP also provides an exception for measures related to national security. The CPTPP does not incorporate the GATS national security exception in Article XIV *mutatis mutandis* as it does for the other general exceptions. Instead, the Parties adopted a different formulation of the security exception in Article 29.2 which clarifies that the CPTPP data rules cannot be construed to require a Party to either disclose information contrary to its security interests or prevent a Party from applying measures which it considers necessary for the protection of its security interests.[106] Like the equivalent exception in Article XIV*bis* of the GATS, this exception is seemingly self-determinative as it refers to actions which a Member 'determines to be contrary to its essential security interests'. This exception, which operates in parallel with the article-specific public policy exception, provides a Party with broad scope to justify data localization measures implemented to protect its essential security interests. However, as with the equivalent GATS exception, CPTPP Parties may be reluctant to invoke this defence for fear of being forced to explain the security considerations underlying a decision to restrict data flows, where in some cases such explanation may itself be prejudicial to national security interests or foreign relations.[107]

4. Does the CPTPP framework improve on GATS disciplines?

Table 1 compares the coverage of GATS and CPTPP provisions relevant to data localization measures. It includes both the horizontal disciplines contained within the CPTPP CBTS Chapter as well as the specific data rules contained in the E-Commerce Chapter.

The most salient difference between the CPTPP and the GATS disciplines on data localization measures is the CPTPP's inclusion of specific rules on data transfers and storage. The CPTPP framework expressly recognizes data localization as a trade issue and provides greater certainty to businesses in relation to their ability to store and transfer data across national borders. Furthermore, the CPTPP moves away from the archaic terminology, classifications, and distinctions between modes of supply and service sectors which are found in the GATS.

enforcement, or otherwise be contrary to the public interest, or which would prejudice the legitimate commercial interests of particular enterprises, public or private.'

106 Article 29.2 states: 'Nothing in this Agreement shall be construed to:

a. require a Party to furnish or allow access to any information the disclosure of which it determines to be contrary to its essential security interests; or

b. preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests.'

107 Alford, 'The WTO Self-Judging Security Exception', supra n. 71, 699.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

Table 1. Comparing GATS and CPTPP disciplines relating to data localization measures

Relevant provisions	GATS	CPTTP
National treatment obligation	X	X
Market access obligation	X	X
Coverage of new services through 'negative-list' schedules		X
'Ratchet mechanism' applies to schedules		X
'Standstill mechanism' applies to schedules		X
Specific provision permitting cross-border data flows necessary for the conduct of a business (excludes financial institutions)		X
Specific provision preventing requirements for to use or locate computing facilities onshore (excludes financial institutions)		X
Legitimate public policy objective exception		X
Horizontal/general exceptions	X	X[108]
Security exception	X	X[109]

The CPTPP data rules are more expansive than the GATS as they encompass data localization measures which do not amount to a breach of national treatment or market access obligations. A non-discriminatory data localization measure which does not constitute a market access restriction within the meaning of Article XVI of the GATS would not be disciplined under the GATS, but would under the CPTPP, providing it does not fall within the exclusions for financial institutions or government information.

An example of a measure which would be disciplined by the CPTPP data rules but not by the GATS is a requirement for domestic and foreign suppliers to store data relating to private education services on servers within a Party's territory as a condition for conducting business in that country. Such a measure would not amount to a breach of national treatment as it is non-discriminatory. Nor would it amount to a breach of market access as it is not a quantitative restriction or 'zero quota' of the kind contemplated by the Panel in *US–Gambling*.[110] However, it would amount to a breach of CPTPP Article 14.13 as it requires service suppliers to use computing facilities in a Party's territory. It may also violate Article 14.11 as it impedes the cross-border transfer of information by electronic means. As discussed above, the defending Party would not be able to schedule a reservation to exempt the breach as the scope article clarifies that a Party can only rely on their non-conforming measures to the extent they have scheduled a

108 The horizontal/general exceptions in the GATS and the CPTPP are not identical. The differences are outlined in section 3.3.2.

109 The security exceptions in the GATS and the CPTPP are not identical. The differences are outlined in section 3.3.2.

110 Panel Report, *US–Gambling*, para. 6.287.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

reservation against *another* obligation. Parties are not able to schedule a reservation solely against either article 14.11 or 14.13.

The CPTPP article-specific public policy exception, which is not found in the GATS, preserves governments' autonomy to regulate in the public interest. While there is some ambiguity surrounding whether the parameters of the exception mean it could be misused for protectionist purposes, the inclusion of a broad public policy exception is important given that the intersection between the liberalization of trade in data and public interests in sensitive issues such as privacy and security is not yet settled. Moreover, exceptions permitting measures which promote public policy interests, even where such measures constitute barriers to trade, can be found throughout the WTO agreements and FTAs. As former WTO Director-General Peter Sutherland outlined in his 2004 report on the future of the WTO: '[n]either the WTO nor the GATT was ever an unrestrained free trade charter … the rules provide checks and balances including mechanisms that reflect political realism as well as free trade doctrine'.[111]

In addition to introducing specific rules on data transfers and storage, differences between the architecture of the CBTS Chapter and the GATS also result in the CPTPP having more expansive coverage of digital trade barriers, including data localization measures. In particular, the CPTPP's negative-list approach to scheduling liberalizes new and future services as the default. This represents a significant advance on the GATS positive-list approach, which relies on case law or negotiated agreements to update the sectors in Members' services schedules. Furthermore, the CPTPP's ratchet and standstill mechanisms which capture future liberalization and prevent backsliding are not found in the GATS.

5. Conclusions

Given that approximately 50% of global services trade is enabled by technologies that depend on the internet, a common and predictable rules-based framework to facilitate data flows and limit data localization is essential to support continued growth in digital trade.[112]

The CPTPP provides a new model for addressing data localization measures facing global service suppliers. I argue that the CPTPP data framework represents a significant advance on the GATS-based status quo and strikes an appropriate balance between facilitating businesses' growing need to transfer and store data across national borders while preserving governments' right to regulate in the public interest. In particular, the CPTPP improves on GATS disciplines by prohibiting a broader

111 Peter Sutherland and others, 'Report by the Consultative Board to Director-General Supachai Panitchpakdi, The Future of the WTO: Addressing Institutional Challenges in the New Millennium' (2004) 15, www.wto.org/english/thewto_e/10anniv_e/future_wto_e.htm (accessed 5 March 2018).

112 Cory and Atkinson, 'Financial Data does not Need or Deserve Special Treatment in Trade Agreements', supra n. 9, 2.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press

range of data localization measures, including measures which may not otherwise amount to a breach of national treatment or market access disciplines. As a consequence, the CPTPP rules on data flows and data localization also provide a valuable precedent for addressing data localization issues in other trade agreements.

Given that CPTPP negotiations involved only 12 of the 164 WTO Members and it would be difficult for many other Members to achieve the level of ambition of the CPTPP's data provisions, the GATS will continue to provide an important baseline to address data localization measures in the multilateral system. GATS disciplines do provide valuable safeguards against some data localization measures, especially where measures discriminate against foreign suppliers in sectors for which Members have taken national treatment commitments. However, the absence of specific digital trade rules in the GATS means that significant uncertainty prevails with regard to how data localization measures might be interpreted under WTO rules in the event of a dispute.

The Appellate Body has mitigated this uncertainty to some extent by adopting an evolutionary approach when adjudicating disputes relating to internet services.[113] However, the lack of progress in WTO e-commerce negotiations means that judicial decisions have not been transposed into binding provisions. Relying on WTO dispute settlement processes rather than consensus-based WTO negotiations to determine the coverage of online services under the GATS is suboptimal as it leads to outcomes which do not necessarily reflect the views of the WTO membership.[114] In addition, no dispute to date has considered data localization measures. Such a dispute would clarify the circumstances in which the national treatment, market access and exception provisions of the GATS apply to data localization measures and thereby provide greater certainty for digital businesses.

Some commentators have advocated for ambitious progress at the multilateral level to address barriers to data transfers, such as through negotiating a new treaty addressing trade-related aspects of data for both goods and services, or establishing a forum to bring together a broad range of internet governance stakeholders to set rules on data-related trade.[115] While such ideas may theoretically yield a more ambitious and inclusive framework for addressing data-related trade barriers, the many frustrations and setbacks in other multilateral processes suggest that progress on these proposals is unlikely for political reasons. Absent a new multilateral treaty, the GATS will remain the most important, albeit imperfect, international agreement for disciplining data-related trade barriers.

113 Panel Report, *US–Gambling*, para. 6.287. Appellate Body Report, *China–Publications and Audiovisual Products*, para. 412.

114 See Burri, 'The Regulation of Data Flows through Trade Agreements', supra. n. 16, 417.

115 See e.g., Lee-Makiyama, 'Cross-Border Data Flows in the Post Bali Agenda', supra n. 26, 165; Susan Ariel Aaronson, *At the Intersection of Cross-Border Information Flows and Human Rights: CPTPP as a Case Study*, Institute for International Economic Policy (May 2016) 3, 4.

https://doi.org/10.1017/S1474745618000277 Published online by Cambridge University Press