

GUEST EDITORIAL

Radhika Parthasarathy & Ipsita Gupta, *Looking to the Future- Development in a Changing World*

Yonov F. Agah, *Trade and Development in the WTO*

ARTICLES

V.S. Seshadri, *Treatment of Trade in Korea's FTAs*

Rafael Leal-Arcas et al., *Aiming at Sustainable Trade in the Context of the Rule of Law: What Role for Citizens and How International Trade Can Help Reduce Fossil-Fuel Consumption*

Joshua P. Meltzer, *The United States-Mexico-Canada Agreement: Developing Trade Policy for Digital Trade*

Jesse Liss, *China's Investment Treaties with Latin America and Implications for South-South Cooperation: Evidence from Firm-Level Data*

Alisher Umirdinov & Valijon Turakulov, *The last bastion of protectionism in Central Asia: Uzbekistan's auto industry in post WTO accession*

Alec Dawson, *Safeguarding the Planet? Renewable Energy, Solar Panel Tariffs, and the World Trade Organisation's Rules on Safeguards*

Michael Goodyear, *Helping David Fight Goliath: Preserving the WTO in the Trump Era*

BOOK REVIEW

Faris Nasrallah, *Book Review of Mesut Akbaba, Giancarlo Capurro (eds.), International Challenges in Investment Arbitration*

TL  
&D

# Trade, Law *and* Development

Vol. 11, No. 2

2019

## **PATRON**

*Hon'ble Prof. Poonam Saxena*

## **FACULTY-IN-CHARGE**

*Rosmy Joan*

## **EDITORS-IN-CHIEF**

*Ipsiata Gupta*

*Radhika Parthasarathy*

## **EDITORS**

*Gautami Govindrajan*

*Ayushi Singh*

(MANAGING)

(SENIOR EDITOR)

*Apoorva Singh*

*Sarthak Singla*

## **ASSOCIATE EDITORS**

*Abilash V.*

*Abhinav Srivastav*

*Alice Kumar*

*Amogh Pareek*

*Anjali Sasikumar*

*Sabil Verma*

*Sukanya V.*

*Tania Gupta*

## **COPY EDITORS**

*Aastha Asthana*

*Aniketa Jain*

*Neerali Nanda*

*Rashmi John*

*Shlok Patwa*

*Suvam Kumar*

*Swikruti Nayak*

## **CONSULTING EDITORS**

*Ali Amerjee*

*Aman*

*Disbi Bhomawat*

*Meghana Sharafudeen*

*Prateek Bhattacharya*

*Shashank P. Kumar*

## **BOARD OF ADVISORS**

*B. S. Chimni*

*Daniel Magraw*

*Glenn Wiser*

*Jagdish Bhagwati*

*M. Sornarajah*

*Raj Bhala*

*Ricardo RamírezHernández*

*Vaughan Lowe*

*W. Michael Reisman*

## ***Published by:***

The Registrar, National Law University, Jodhpur

ISSN : 0976-2329 | eISSN : 0975-3346

Joshua P. Meltzer, *The United States-Mexico-Canada Agreement: Developing Trade Policy for Digital Trade*  
11(2) TRADE L. & DEV. 239 (2019)

## THE UNITED STATES-MEXICO-CANADA AGREEMENT: DEVELOPING TRADE POLICY FOR DIGITAL TRADE

**JOSHUA P. MELTZER\***

*This paper analyses how the United States-Mexico-Canada Agreement (USMCA) supports digital trade and cross-border data flows, while also giving governments the scope to restrict data flows to achieve legitimate regulatory objectives. The USMCA has made significant progress developing rules for digital trade, yet more is needed. In particular, trade policy needs to address the drivers behind the significant growth in restrictions on digital trade by supporting the development of international standards and encouraging international regulatory cooperation as well as good regulatory practice. This paper outlines the key USMCA rules that are applicable to digital trade and analyses what more is needed to support digital trade and data flows consistent with domestic regulatory objectives.<sup>1</sup>*

### TABLE OF CONTENTS

- I. INTRODUCTION
- II. THE ECONOMIC BENEFITS FROM DATA FLOWS AND DIGITAL TECHNOLOGIES
  - A. INTERNATIONAL E-COMMERCE OPPORTUNITIES
  - B. DIGITAL SERVICES TRADE
  - C. THE DIGITISATION OF GOODS EXPORTS
  - D. INCREASED PARTICIPATION IN GLOBAL VALUE CHAINS (GVCs)
  - E. THE GROWTH IN DIGITAL PROTECTIONISM
- III. EXISTING DIGITAL TRADE RULES IN THE WTO

---

\*Joshua P. Meltzer is a senior fellow and the lead of the Digital Economy and Trade Project in the Global Economy and Development Program at the Brookings Institution. The author may be contacted at [jmeltzer\[at\]brookings.edu](mailto:jmeltzer[at]brookings.edu).

<sup>1</sup> This paper is adapted from an earlier 2019 Brookings Working Paper by the author titled 'A WTO Reform Agenda: Data flows and International Regulatory Cooperation'.

#### IV. DIGITAL TRADE RULES IN UNITED STATES-MEXICO-CANADA AGREEMENT (USMCA)

- A. MARKET ACCESS
- B. CROSS BORDER DATA FLOWS
- C. DATA LOCALISATION
- D. SOURCE CODE
- E. INTERACTIVE COMPUTER SERVICES
- F. CYBERSECURITY
- G. OPEN GOVERNMENT DATA
- H. PRIVACY AND CONSUMER PROTECTION
- I. THE USMCA INTELLECTUAL PROPERTY CHAPTER

#### V. BUILDING ON USMCA FOR DIGITAL TRADE GOVERNANCE

- A. DEVELOPING INTERNATIONAL STANDARDS FOR DIGITAL TRADE
- B. LIMITS TO INTERNATIONAL STANDARDS IN ADDRESSING THE REGULATORY CHALLENGES TO DIGITAL TRADE
- C. USING TRADE POLICY TO BUILD INTERNATIONAL REGULATORY COOPERATION
- D. MUTUAL RECOGNITION AGREEMENTS/ARRANGEMENTS (MRA)
- E. U.S.-EU PRIVACY SHIELD
- F. EQUIVALENCE
- G. REGULATORY BEST PRACTICE FOR DIGITAL TRADE

#### VI. CONCLUSION

### I. INTRODUCTION

The use of data and the ability to move data globally has grown as the internet has globalised – over half the world now has internet access,<sup>2</sup> and that access is increasing via mobile devices such as smart phones and other devices that collect large amounts of data.<sup>3</sup>In addition, increasing computer power and algorithmic complexity applied to this big data is developing insights that are of a growing value for businesses, people and governments.

---

<sup>2</sup>*Statistics*, INT’L TELECOMM. UNION, <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx> (last visited Jan. 20, 2020).

<sup>3</sup>*Id.*

The movement of data across borders is also transforming international trade.<sup>4</sup>Data flows themselves can be a services trade such as cloud computing or professional service, and data flows enable international trade by supporting global communication, access to information, tracking and tracing along supply chains and opportunities for collaboration and innovation. Yet at the same time, there is a global growth in regulations that restrict data flows. These data flow restrictions are being driven by a range of reasons, such as protection of privacy and addressing cybersecurity risks. The first part of this paper expands on how data affects and transforms international trade, and how and why governments are restricting cross-border data flows.

Regulations that restrict cross-border data flows can raise the cost for businesses that rely on these data flows to export or conduct their business operations. Moreover, the application of some data restrictions discriminates against digital imports, which may breach trade commitments in the World Trade Organization (WTO) and in Free Trade Agreements (FTAs).The rising impact and importance of data flows for trade has led a number of countries to include new commitments to digital trade in their trade agreements. The second part of this paper discusses the application of WTO commitments to digital trade as well as its limitations. The USMCA is the most recent FTA to include ambitious new digital trade commitments. While the third part of the paper analyses these digital rules and shows how they build on existing WTO commitments and on those in previous FTAs. While the USMCA develops digital trade rules, more is needed to effectively govern digital trade and to adequately respond to the concerns motivating governments to restrict cross-border data flows in the first case. The fourth part of the paper outlines how trade policy can do more to develop digital trade governance. And finally, the last part concludes the paper.

## II. THE ECONOMIC BENEFITS FROM DATA FLOWS AND DIGITAL TECHNOLOGIES

In this part, an overview of the economic significance of data access and use for innovation, productivity, economic growth, and trade will be provided and analysed. Although not discussed further in this paper, data also provides new opportunities to improve government policy design, implementation and enforcement.<sup>5</sup>For instance, Artificial Intelligence (AI)—a data-driven technology which could add trillions of dollars to global output over the next ten years and

---

<sup>4</sup> Joshua P. Meltzer, *Governing Digital Trade*, 18 WORLD TRADE REV. S23 (2019) [hereinafter Meltzer].

<sup>5</sup> Nick Johnstone et al., *Using Digital Technologies to Improve the Design and Enforcement of Public Policies*, 274 OECD DIGITAL ECON. PAPER (2019).

accelerate the transition towards a services-driven global economy.<sup>6</sup>The McKinsey Global Institute estimates that AI could add around 16%, or US \$13 trillion, to global output by 2030.<sup>7</sup>Cloud computing, another technology that relies on cross-border data flows, is already delivering economic benefits.<sup>8</sup>

Increasingly, global data flows and the emerging technologies are key drivers of international trade. McKinsey estimated that, in 2014, cross-border data flows were worth around US \$2.8 trillion—more than trade in goods.<sup>9</sup>According to a 2019 United Nations Conference on Trade and Development (UNCTAD) report, e-commerce globally was worth US \$29 trillion in 2017, with around 1.3 billion people shopping online—up by 12% from the previous year.<sup>10</sup>According to the WTO, using digital technologies to reduce trade costs could increase world trade by up to 34% by 2030.<sup>11</sup> This includes using digital technologies to reduce transport by increasing the efficiency of logistics, using robots to optimise storage and inventory, and using blockchain to facilitate customs processing. For example, by using AI, businesses are improving the management of supply chain risk, developing smart manufacturing, and using AI language translation services to increase exports to countries where language was a barrier to commerce.<sup>12</sup>

---

<sup>6</sup>Jacques Bughin et al., *Notes from the AI Frontier: Modeling the impact of AI on the world economy*, MCKINSEY GLOB. INST. (Sep., 2018), <https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy> [hereinafter Bughin et al.]; See Paul Daugherty & Mark Purdy, *Why AI is the Future of Growth?*, ACCENTURE (Sep. 28, 2016), [https://www.accenture.com/t20170524t055435\\_\\_w\\_\\_/ca-en/\\_acnmedia/pdf-52/accenture-why-ai-is-the-future-of-growth.pdf](https://www.accenture.com/t20170524t055435__w__/ca-en/_acnmedia/pdf-52/accenture-why-ai-is-the-future-of-growth.pdf).

<sup>7</sup>Bughin et al., *supra* note 6, at 7.

<sup>8</sup>Kevin L. Jackson, *The Economic Benefit of Cloud Computing*, NJVC EXECUTIVE WHITE PAPER (Sep., 2011) [http://www.njvc.com/sites/default/files/NJVC\\_The\\_Economic\\_Benefit\\_of\\_Cloud\\_Computing.pdf](http://www.njvc.com/sites/default/files/NJVC_The_Economic_Benefit_of_Cloud_Computing.pdf).

<sup>9</sup>Susan Lund et al., *Digital globalization: the new era of global flows*, MCKINSEY GLOB. INST. (Feb., 2016), <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows> [hereinafter Lund et al.].

<sup>10</sup>United Nations Conference on Trade and Development, *Global E-Commerce Sales Surged to \$29 Trillion*, UNCTAD (Mar. 29, 2019), <https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=2034>.

<sup>11</sup>WTO Secretariat, *World Trade Report 2018 on Future of World Trade: How Digital Economies Are Transforming Global Commerce* (Oct. 3, 2018), [https://www.wto.org/english/res\\_e/publications\\_e/world\\_trade\\_report18\\_e.pdf](https://www.wto.org/english/res_e/publications_e/world_trade_report18_e.pdf).

<sup>12</sup>Brynjolfsson et al., *Does Machine Translation Affect International Trade? Evidence from a Large Digital Platform*, NAT'L BUREAU ECON. RESEARCH (Aug. 1, 2018), [http://ide.mit.edu/sites/default/files/publications/Machine\\_Translation\\_NBER.pdf](http://ide.mit.edu/sites/default/files/publications/Machine_Translation_NBER.pdf) [hereinafter Brynjolfsson et al.].

The economic opportunities of global data flows and access to digital technologies is also transforming international trade in the following ways.

#### A. International E-Commerce Opportunities

Already, around 12% of global goods trade is via international e-commerce.<sup>13</sup> Businesses can have their website or use digital platforms to become global. This is comprised of purchasing online and having the goods delivered offline. E-commerce provides a potentially significant opportunity to increase the participation of small businesses in international trade.<sup>14</sup> For instance, having a website gives small businesses an instant international presence without having to establish a physical presence overseas. In addition, the internet provides access to advertising and communication services, as well as information on foreign markets—all of which helps small businesses participate in international trade.<sup>15</sup>

In the United States, for instance, 97% of small businesses export on eBay as compared to 4% of the offline peers.<sup>16</sup> Similar results play out across developed and developing countries. Furthermore, increasing the ability of companies of all sizes to be able to sell goods online across borders supports the participation of Micro, Small and Medium Enterprises (MSMEs) in digital trade as larger companies incorporate smaller companies into their supply chains.<sup>17</sup> AI is also relevant here. For example, eBay's machine translation service has increased eBay based exports to Spanish speaking Latin America by 17.5%.<sup>18</sup> To put this growth into context, a 10% reduction in distance between countries is correlated with increased trade

---

<sup>13</sup>Lund et al., *supra* note 9.

<sup>14</sup>Joshua P. Meltzer, *Supporting the Internet as a Platform for International Trade: Opportunities for Small and Medium-Sized Enterprises and Developing Countries*, GLOBAL ECONOMY & DEVELOPMENT, WORKING PAPER NO. 69, (2014), <https://www.brookings.edu/wp-content/uploads/2016/07/02-internet-international-trade-meltzer.pdf>.

<sup>15</sup>OECD, *Top Barriers and Drivers to SME Internationalisation, Report by the OECD Working Party on SMEs and Entrepreneurship* (2009) <https://www.oecd.org/cfe/smes/43357832.pdf>; Bilitis Schoonjans et al., *Formal Business Networking and SME Growth*, 41(1) SMALL BUS. ECON. 169 (2011).

<sup>16</sup> eBay, *Empowering People and Creating Opportunity in the Digital Single Market: An eBay Report on Europe's Potential*, EBAY MAIN STREET (Oct. 2015), [https://www.ebaymainstreet.com/sites/default/files/policy-papers/ebay\\_europe\\_dsm\\_report\\_10-13-15.pdf](https://www.ebaymainstreet.com/sites/default/files/policy-papers/ebay_europe_dsm_report_10-13-15.pdf).

<sup>17</sup>Emmanuelle Ganne & Kathryn Lundquist, *The digital economy, GVCs and SMEs*, in GLOBAL VALUE CHAIN DEVELOPMENT REPORT 2019: TECHNOLOGICAL INNOVATION, SUPPLY CHAIN TRADE AND WORKERS IN A GLOBALIZED WORLD 121, 122 (Apr. 15, 2019).

<sup>18</sup>Brynjolfsson et al., *supra* note 12.

revenue of 3.51%—so a 13.1% increase in revenue from eBay’s machine translation is equivalent to reducing the distance between countries by over 35%.<sup>19</sup>

### B. *Digital Services Trade*

Internet access and cross-border data flows are going to be particularly significant for growth in services trade.<sup>20</sup> Services can increasingly be purchased and consumed online. This is particularly true for Information Technology (IT), professional, financial, retail, and education services.<sup>21</sup> New digital services such as cloud computing are becoming crucial business inputs.<sup>22</sup> The finance industry relies on the ability to transfer data across borders in order to complete electronic transactions and make money transfers.<sup>23</sup> AI requires access to large data sets because machine learning needs to be able to incorporate as many past outcomes into future predictions as possible.<sup>24</sup>

Figure 1 shows opportunities for exports of digitally deliverable services (DDS)—services that could be delivered online.

Figure 1: Digitally deliverable services exports

---

<sup>19</sup>*Id.*

<sup>20</sup> Aaditya Mattoo & Sacha Wunsch-Vincent, *Pre-empting Protectionism in Services: The GATS and Outsourcing*, 7(4) J. INT’L ECON. L. 765 (2004).

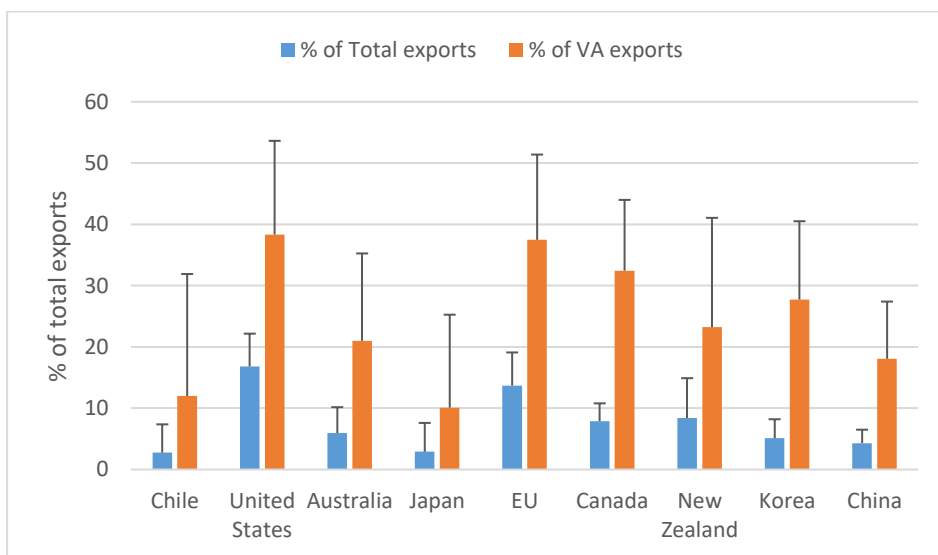
<sup>21</sup> Digital Trade in the U.S. and Global Economies, ¶42, Inv. No. 332-540, USITC Pub. 4485, (Aug., 2014).

<sup>22</sup> Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions, ¶¶ 58-66, Inv. No. 332-561, USITC Pub. 4716, (Aug., 2017).

<sup>23</sup> Daniel Gozman & Jonathan Mangan, *The Role of Big Data in Governance: A Regulatory and Legal Perspective of Analytics in Global Financial Services*, SWIFT INSTITUTE, WORKING PAPER NO. 2014-009(2015), <https://www.swiftinstitute.org/wp-content/uploads/2015/12/SIWP-2014-009-The-Role-of-Big-Data-in-Governance-FINAL.pdf>.

<sup>24</sup> Generative adversarial networks or use of digital twins can minimise need for large data sets to train AI.





Source: OECD TiVA,<sup>25</sup> own calculations

As ascertainable from the table above, in the U.S., for instance, the DDS could be as high as 23% of total exports, and the value of DDS embodied in goods and services exports could account for 55% of total exports.

Engaging in digital services trade is also a development opportunity for some countries. For instance, India’s Information and Communication Technologies (ICT) enabled exports in 2016-2017 were US \$103 billion, i.e. 63% of total services exports, and 80% of these digital services were delivered via Mode 1—the cross-border supply of a service from the territory of one WTO member into the territory of another WTO member over the internet.<sup>26</sup> More specifically, the key role of services as inputs into production means that the opportunity for digital trade to liberalise services alongside effective regulation can contribute to broad-based improvements in efficiency and economic growth for developed and developing countries.<sup>27</sup>

<sup>25</sup> *Trade in Value Added*, OECD, <https://www.oecd.org/sti/ind/measuring-trade-in-value-added.htm> (last visited Feb. 8, 2020).

<sup>26</sup> Indian Ministry of Commerce and Industry, *India’s Exports of ICT-enabled Services, An All-India Survey: 2016-2017* (June, 2018), <http://dgciskol.gov.in/Writereaddata/Downloads/IctExportReport.pdf>.

<sup>27</sup> Aaditya Mattoo, *Developing Countries in the New Round of GATS Negotiations: Towards a Pro-Active Role*, 23(4) *WORLD ECON.* 471 (2000).

### C. *The Digitisation of Goods Exports*

Data collection and analysis are allowing new digital services to add value to goods exports. Data flows across border enables digitisation of the entire manufacturing enterprise, faster lifecycles, and collaborative and connected supply chains.<sup>28</sup> For example, data collected from sensors attached to mining and farming equipment allows businesses to improve their operations, and thereby, the value from the use of such equipment. Digital services are increasingly becoming key inputs in the manufacturing processes. This includes commercial services such as research and development (R&D), design, marketing, and sales. A 2016 Pricewater House Coopers survey of more than two thousand companies identified ‘data and data analytics’ as the key for successful transformation to smart manufacturing.<sup>29</sup> This reflects the importance of digital services in manufacturing for increasing productivity, which affects the capacity of firms to compete domestically and overseas.<sup>30</sup> In fact, taking account of the value of services embedded into goods exports (such as design, professional services and IT), the services that are exported by the European Union (EU) make up over 55% of its total exports.<sup>31</sup>

### D. *Increased Participation in Global Value Chains (GVCs)*

Global data flows underpin GVCs, thereby creating new opportunities for participation in international trade.<sup>32</sup> For many economies, such participation in GVCs is the decisive factor for trading internationally. More than 50% of trade in goods, and over 70% of trade in services is in intermediate inputs.<sup>33</sup> Data and digital technologies are affecting GVC participation in several ways. The

<sup>28</sup> Yan Lu et al., *Current Standards Landscape for Smart Manufacturing Systems*, NISTIR/ 8107 (Feb. 23, 2016), <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8107.pdf>.

<sup>29</sup> *Industry 4.0: Building the Digital Enterprise, 2016 Global Industry 4.0 Survey*, PWC <https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf> (last visited Jan. 10, 2019).

<sup>30</sup> Bernard Hoekman & Aaditya Mattoo, *Services Trade and Growth*, WORLD BANK POL’Y RESEARCH, WORKING PAPER NO. 4461, (2008), <https://openknowledge.worldbank.org/handle/10986/6460>; Xuepeng Liu et al., *Services Development and Comparative Advantage in Manufacturing*, NAT’L. BUREAU OF ECON. RESEARCH, WORKING PAPER NO 26542, (2018), [https://www.k-state.edu/economics/seminars/Liu\\_Xuepeng\\_Paper\\_Services%20Development%20and%20Comparative%20Advantage%20in%20Manufacturing.pdf](https://www.k-state.edu/economics/seminars/Liu_Xuepeng_Paper_Services%20Development%20and%20Comparative%20Advantage%20in%20Manufacturing.pdf).

<sup>31</sup> Joshua P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment*, GLOB. ECON. & DEV. AT BROOKINGS, WORKING PAPER 79, (2014), <https://www.brookings.edu/wp-content/uploads/2016/06/internet-transatlantic-data-flows-version-2.pdf>.

<sup>32</sup> RICHARD BALDWIN, *THE GREAT CONVERGENCE: INFORMATION TECHNOLOGY AND THE NEW GLOBALIZATION 1 passim* (2016).

<sup>33</sup> OECD, *Mapping Global Value Chains, Policy Dialogue on Aid for Trade*, 9 TAD/TC/WP/RD (2012), [https://www.oecd.org/dac/aft/MappingGlobalValueChains\\_web\\_usb.pdf](https://www.oecd.org/dac/aft/MappingGlobalValueChains_web_usb.pdf).

development of GVCs has been enabled by global connectivity and cross-border data flows that facilitate communications and can be used to coordinate logistics, particularly for more complex GVC activity which often involves high levels of innovation and inputs of digital services.<sup>34</sup>

Global data flows are also enabling the so-called ‘Supply Chain 4.0’—where information flows are integrated and omnidirectional, instead of linear flows from supplier to producers to consumers and back.<sup>35</sup> Integrated information flows enabled by the Supply Chain 4.0 are creating new opportunities to enhance productivity and expand employment opportunities. There is a trend towards increasing the use of imported services inputs in manufactured goods exports, suggesting that digital services are being traded within GVCs as well.<sup>36</sup> This includes allowing SMEs to plug into GVCs to offer their own specific service or to strengthen more traditional e-commerce offerings. Global data flows have also allowed digital platforms to source key digital services globally, creating entirely digital value chains. For instance, take Gojek, an Indonesian ride sharing platform. Gojek’s digital supply chains include a cloud-based company from Singapore, a payment service based in Singapore and New York, and a mapping service and software application based interface (API) from the Silicon Valley.

#### E. *The Growth in Digital Protectionism*

As the opportunities presented by global data flows and digital technologies grow, governments are increasingly regulating the ways in which they restrict global data flows.<sup>37</sup>

There are various forms of restrictions on data flows, such as measures that disallow the transfer of data outside national borders; measures that allow cross-border transfers but require a copy to be maintained domestically; and requirements of prior consent before data can be transferred overseas. There are also data localisation restrictions that often include restrictions on data flows.

---

<sup>34</sup>Xin Li et al., *Recent Patterns of Global Production and GVC Participation*, in THE GLOBAL VALUE CHAIN DEVELOPMENT REPORT 2019, TECHNOLOGICAL INNOVATION, SUPPLY CHAIN TRADE AND WORKERS IN A GLOBALIZED WORLD 9, 10 (Apr. 15, 2019).

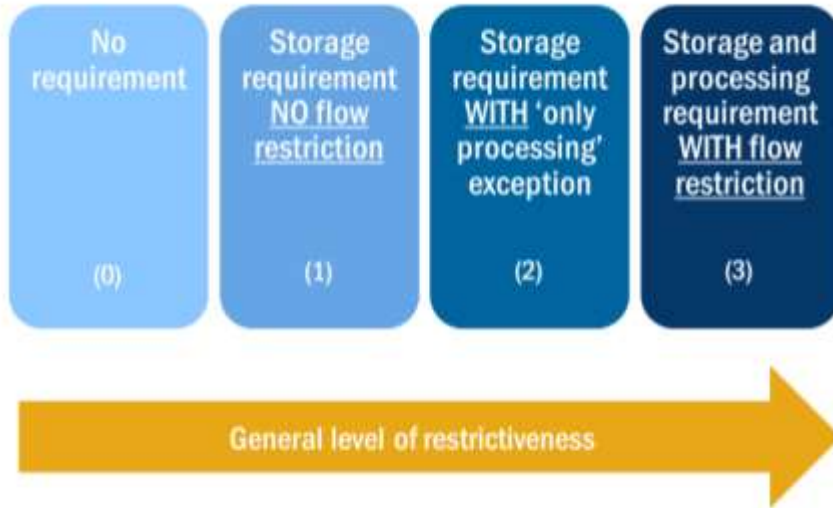
<sup>35</sup>Michael J. Ferrantino & Emine Elcin Koten, *Understanding Supply Chain 4.0 and its Potential Impact on Global Value Chains*, in THE GLOBAL VALUE CHAIN DEVELOPMENT REPORT 2019, TECHNOLOGICAL INNOVATION, SUPPLY CHAIN TRADE, AND WORKERS IN A GLOBALIZED WORLD 105, 106 (Apr. 15, 2019).

<sup>36</sup>Sebastien Miroudot & Charles Cadestin, *Services in Global Value Chains: From Inputs to Value-Creating Activities*, 197 OECD TRADE POL’Y PAPER 16 (2017).

<sup>37</sup>Martina F. Ferracane, *Cross-border Data Flows: A Taxonomy*, EUROPEAN CENTRE FOR INT’L POL. ECON., WORKING PAPER NO. 1, (2017), <https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf>.

Figure 2 below provides a taxonomy of local storage requirements and their impacts on cross-border flows.

Figure 2: Taxonomy of data localisation requirements



*Source:* Casalina and Gonzalez, OECD 2018.<sup>38</sup>

Measures that restrict data flows and require data to be localised are implemented for a range of reasons. One reason is to prevent data flows to jurisdictions with lower levels of regulatory protection. For example, the EU General Data Protection Regulation (GDPR), which came into effect in April 2018, and specifically Article 45, prohibits businesses that collect personal data in EU from transferring it outside EU unless the receiving country has an equivalent level of privacy protection.<sup>39</sup>

Governments can also require data to be localised by arguing that regulators need access to data in order to perform their regulatory functions. One increasingly used data restriction is seen in the financial services sector, which is often justified on the basis that financial regulators require financial data to remain local in case they

<sup>38</sup> Francesca Casalini & Javier López González, *Trade and Cross-Border Data Flows*, OECD TRADE POLY PAPERS, PAPER NO. 220, (2018).

<sup>39</sup> General Data Protection Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR]. Personal data can also be transferred under Binding Corporate Rules (BCRs), Standard Contractual Clauses (SCCs) and in a limited number of other circumstances. *See* GDPR, art. 47.

need access to the data for supervisory and regulatory purposes.<sup>40</sup>In 2018, India introduced a requirement - whereby payment system operators must store data locally in order to allow financial regulators to effectively perform their supervisory function.<sup>41</sup> China requires that insurers localise data in order for the insurance regulator to perform its responsibilities.<sup>42</sup>In contrast to the Indian and Chinese policies and their impact, Turkey's requirements of financial data localisation led PayPal to exit the country's market.<sup>43</sup>

Ensuring cybersecurity is another rationale for requiring data to be local. The view here is that data localisation decreases the risks of unauthorised access. Cybersecurity is another reason that India provided for requiring financial data to be localised. China's Cyber Security Law (CSL) requires data localisation and access to source code for 'critical information infrastructure'.<sup>44</sup>

Another reason for data flows restrictions is to control access to certain types of online content, usually on moral, religious, or political grounds. For example, Iran's censorship aimed at creating the 'Halal internet' limits access to content deemed offensive to Islam.<sup>45</sup> China blocks access to eleven of the top twenty-five global websites among an estimated three thousand prohibited foreign websites.<sup>46</sup> This is done in part to restrict access to political speech directed at the Communist Party of China (CPC). Vietnam's 2018 Cybersecurity Law requires local retention of a range of personal and other data of Vietnamese users, in part so that the State can

---

<sup>40</sup> Harsh Walia et al., *RBI Mandates Data Localization for Payment Systems*, MONDAQ (Apr. 17, 2018),

<http://www.mondaq.com/india/x/692872/Financial+Services/RBI+Mandates+Data+Localisation+For+Payment+Systems>.

<sup>41</sup> Reserve Bank of India, *Storage of Payment Systems Data*, RBI/2017-18/153 (Apr. 6, 2018), <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0>.

<sup>42</sup> Zhong Len, *China to Implement Widespread Data Localization for Personal Information and Important Data*, MONDAQ (Jan. 31, 2018), <https://www.mondaq.com/china/Privacy/668910/China-To-Implement-Widespread-Data-Localization-For-Personal-Information-And-Important-Data>.

<sup>43</sup> Emre Peker, *PayPal to Exit Turkey After Regulator Denies Payments License*, WALL ST. J. (May 31, 2016), <https://www.wsj.com/articles/paypal-to-exit-turkey-after-regulator-denies-payments-license-1464720574>.

<sup>44</sup> Draft for Measures on Cybersecurity Review, art. 10, Cyberspace Administration of China (May 21, 2019).

<sup>45</sup> Jon Gambrell, *Iran Deploys 'Halal' Internet in Latest Bid to Rein in Citizens' Web Freedoms*, INDEPENDENT (Jan. 29, 2018), <https://www.independent.co.uk/news/world/middle-east/iran-halal-internet-national-information-network-web-freedoms-citizens-access-social-media-telegram-a8182841.html>.

<sup>46</sup> OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE, 2017 NATIONAL TRADE ESTIMATE REPORT ON FOREIGN TRADE BARRIERS (2017), <https://ustr.gov/sites/default/files/files/reports/2017/NTE/2017%20NTE.pdf>.

regulate online content, which could include information opposing or offending the Socialist Republic of Vietnam or to block ‘defamatory propaganda,’ such as any critical or dissenting statements made against the government.<sup>47</sup>

Data flow restrictions such as those proposed in Brazil and implemented in Russia, are also being driven by law enforcement needs. Here, the issue is the challenge in getting access to data for law enforcement purposes in a timely manner when that data resides in a third country.

Data localisation measures are also being enacted for protectionist reasons. China’s blocking or degrading internet access has supported the development of local champions. For instance, blocking access to Google, Facebook and Netflix has been to the benefit of Baidu, Renren, Tencent, Alibaba and Sina Weibo. India’s data localisation laws also seem in part aimed at supporting the development of local businesses.

Many of the reasons that lead governments to require data flows to be restricted or localised, such as protection of privacy and law enforcement, are themselves legitimate goals. Yet, whether data restrictions are an optimal way of achieving these goals is less clear. For instance, in the case of law enforcement demands, instead of requiring all data to be local, governments could require data mirroring, where a copy of the data is retained locally. In other cases, such as cybersecurity, requiring data to be localised can be counter-productive where local data centres are less secure. Further, it misses on the opportunity for stronger cybersecurity protection provided by disaggregating data across global data centres.

Such a data regulation can also have an impact similar to the one behind the border regulation that raises compliance costs for exporters. For instance, GDPR applies to all businesses targeting the EU market using the internet.<sup>48</sup> GDPR also requires business processing EU personnel to have a representative in the EU for enforcement purposes.<sup>49</sup> Such requirements may also be discriminatory where they raise costs only for digital exporters.<sup>50</sup>

### III. EXISTING DIGITAL TRADE RULES IN THE WTO

---

<sup>47</sup> Meltzer, *supra* note 4, at 3.

<sup>48</sup> GDPR, *supra* note 39, at art. 3.

<sup>49</sup> *Id.* at art. 27.

<sup>50</sup> Holger P. Hestermeyer & Laura Nielsen, *The Legality of Local Content Measures under WTO Law*, 48(3) J. WORLD TRADE 553, 588 (2014) [hereinafter Hestermeyer et al.].

While the negotiations that ushered in the establishment of the WTO were conducted in the 1980s and early 1990s, before much of the commercial internet existed, there are several WTO agreements that are still relevant for digital trade. These include: The General Agreement on Tariffs and Trade (GATT); the General Agreement on Trade in Services (GATS); the Annex on Telecommunications, Information Technology Agreement (ITA) I & II; and the Agreement on Technical Barriers to Trade (TBT).<sup>51</sup> The most important WTO agreement, when it comes to providing a legal framework supporting cross-border data flows is the GATS.

In particular, GATS commitments are technologically neutral with respect to delivery. This means that where WTO members have scheduled a Mode 1 services (services supplied from the territory of one member into the territory of any other member) commitment, there is also a commitment to allow the data to flow in order to deliver that service.<sup>52</sup> Data flows restrictions and data localisation requirements can place international suppliers of digital services at a competitive disadvantage, in breach of a WTO member's GATS national treatment and market access obligation.<sup>53</sup> In addition, there is a WTO specific commitment to allow financial information to be transferred across borders where such transfers are "necessary for the conduct of the ordinary business of a financial service supplier."<sup>54</sup>

GATS commitments are also subject to a GATS article XIV style exception that provides space to restrict data flows where necessary in order to achieve legitimate public policy goals such as protecting privacy and public morals. The WTO Understanding on commitments in financial services includes a commitment by Members not to "take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means.

---

<sup>51</sup> Meltzer, *supra* note 4, at 3.

<sup>52</sup> Appellate Body Report, *United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶ 202, WT/DS285/R, (adopted Apr. 25, 2013); Appellate Body Report, *China — Measures Affecting Trading Rights and Distribution Services for certain Publications and Audiovisual Entertainment Products*, ¶ 151, WTO Doc. WT/DS363/AB/, (adopted Dec. 21, 2009).

<sup>53</sup> Hestermeyer et al., *supra* note 50, at 12.

<sup>54</sup> Understanding on Commitments in Financial Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, 1867 U.N.T.S. 154.

The WTO's commitment to allow transfers of financial data can be restricted to protect personal data and for prudential reasons<sup>55</sup>. These WTO exceptions are the framework for balancing the data flows commitments with WTO members' other regulatory goals.

The GATS, however, is limited in terms of its capacity to support the range of data flows that enable digital trade. For one, in many services sectors, GATS commitments are limited.<sup>56</sup> Even in sectors where GATS commitments are made, it is unclear where (if at all) new digital services such as cloud computing or online gaming are to be classified under the 1991 United Nations Provisional Central Product Classification (CPC Prov.) System or the Services Sectoral Classifications List used by most WTO members, to schedule their commitments.<sup>57</sup>

So far at least, these WTO rules are yet to be used to meaningfully constrain growth in data flows restrictions. As will be discussed in more detail, developing effective digital trade governance requires a comprehensive and clear data flow commitment, appropriately tailored exceptions to this commitment as well as support for mechanisms of international regulatory cooperation.

#### IV. DIGITAL TRADE RULES IN UNITED STATES-MEXICO-CANADA AGREEMENT (USMCA)

Many governments have already made various digital trade commitments in various FTAs. Since the first standalone e-commerce chapter in an FTA between Australia and Singapore in 2013, there are now more than seventy FTAs with e-commerce chapters,<sup>58</sup> of various scope and ambition.<sup>59</sup>

The USMCA is one of the most recent and comprehensive FTA addressing digital trade rules. It expands upon the digital trade commitments in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). The USMCA

---

<sup>55</sup>Uruguay Round Ministerial Decisions and Declarations on Financial Services, art. 2(a) (Dec. 15, 1993), Marrakesh Agreement Establishing the World Trade Organization, 1867 U.N.T.S. 154.

<sup>56</sup> OECD Working Party of the Trade Committee, *Electronic Commerce – Existing GATS Commitments for online Supply of Services*, Doc. TD/TC/WP (99)37/Final (2000).

<sup>57</sup> WTO Secretariat, *Report of the Meeting held on 18 September 2014*, S/CSC/M/71 (Nov. 5, 2014); Shin-yi Peng, *GATS and the Over-the-Top (OTT) Services – A Legal Outlook*, 50(1) J. WORLD TRADE 10 (2016).

<sup>58</sup> In USMCA, it is called the digital trade chapter.

<sup>59</sup> Mark Wu, *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System*, ICTSD (2017), <http://e15initiative.org/wp-content/uploads/2015/09/RTA-Exchange-Digital-Trade-Mark-Wu-Final.pdf> [hereinafter Wu].



digital trade chapter applies to covered investments, investors of a party to the USMCA, and service suppliers of a party. In terms of what is covered by the chapter, it applies broadly to ‘measures adopted or maintained by a party that affect trade by electronic means’, but does not apply to government procurement or to information held by a party or processed by or on behalf of a party to the USMCA.<sup>60</sup>

A number of USMCA commitments are not new and have been included in previous United States’ FTAs. These include commitments to having domestic laws and regulations for electronic contracts consistent with the UNCITRAL Model Law on Electronic Commerce 1996,<sup>61</sup> and laws that provide for acceptance of electronic signatures.<sup>62</sup> The USMCA also includes a commonly found commitment to adopt measures to limit the receipt of unsolicited commercial electronic communication.<sup>63</sup> Also like many other FTAs, the USMCA includes a commitment to non-discriminatory treatment of digital products, consistent with the national treatment rule, and the most-favoured-nation status (MFN).<sup>64</sup>

#### A. Market Access

Parties have agreed not to impose customs duty fee or other charges on imports trade in digital products between persons from either parties to the USMCA.<sup>65</sup> This commitment applies to all digital products, irrespective of where the product was encoded or produced. Such a commitment stands in contrast to the current situation in the WTO, where there is only a moratorium on tariffs on international electronic transmissions, which the members have so far agreed to renew at successive WTO Ministerial meetings.

#### B. Cross Border Data Flows

A key USMCA commitment that builds on CPTPP is an agreement not to restrict cross-border transfers of information, including personal information, by electronic means.<sup>66</sup> This commitment, is however, limited to the information that is transferred for an activity for the conduct of the business of a person covered under the agreement. In other words, the commitment applies only amongst the parties and not on an MFN basis.

---

<sup>60</sup> United States-Mexico-Canada Agreement, art. 19.2, Sept. 30, 2018 (H.R./5430) (2019) [hereinafter USMCA].

<sup>61</sup>*Id.* at art. 19.5.

<sup>62</sup>*Id.* at art. 19.6.

<sup>63</sup>*Id.* at art. 19.13.

<sup>64</sup>Wu, *supra* note 59, at 14.

<sup>65</sup> USMCA, *supra* note 60, at art. 19.6.

<sup>66</sup> USMCA, *supra* note 60, at art. 19.11.

This data flow commitment is subject to an exception modelled on the GATT Article XX/GATS Article XIV exceptions provision, whereby the parties can restrict data flows to achieve a legitimate public policy objective, provided the measure restricting the cross-border flow of information is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination, or a disguised restriction on trade, and/or does not impose a restriction on transfers of information greater than are necessary to achieve the objective. Worth noting here is that the GATT Article XX/GATS Article XIV requirement of ‘necessity’ also includes the least trade restrictive assessment.<sup>67</sup>

### C. Data Localisation

Another important digital trade commitment in the USMCA is that the parties agreed not to require the domestic location of computing facilities as a condition for doing business. While there is no specific exception in the USMCA digital trade chapter to this data localisation requirement, it is still subject to the FTAs general exception provision, which in turn applies GATS Article XIV.<sup>68</sup>

In FTAs, financial services have experienced a slightly different treatment when it comes to data flows and data localisation. In CPTPP, for instance, financial institutions and cross-border financial services suppliers are carved out from the e-commerce chapter that includes data flows and data localisation commitments. The CPTPP financial services chapter does contain a rule that parties must allow information transfers in electronic or any other form for business purposes but does not include a prohibition on forced data localisation.<sup>69</sup> These commitments in the e-commerce and financial services chapters are subject to exceptions.

An updated approach to data flows in the USMCA financial services chapter includes a commitment to the free flow of information as well as a prohibition on data localisation requirements, subject to appropriate exceptions.<sup>70</sup> The prohibition against data localisation is subject to the party’s financial regulatory authorities, for regulatory and supervisory purposes, having immediate, direct, complete and ongoing access to relevant information used by a covered person outside its territory. Before imposing data localisation, the parties also commit to providing a

---

<sup>67</sup> Appellate Body Report, *Brazil — Measures Affecting Imports of Retreaded Tyres*, WTO Doc. WT/DS33/AB/R (adopted Dec. 17, 2007) [hereinafter *Brazil-Retreaded Tyres*]; Appellate Body Report, *US — Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WTO Doc. WT/DS285/AB/R (adopted Apr. 20, 2005) [hereinafter *US-Gambling*].

<sup>68</sup> USMCA, *supra* note 60, at art. 32.1.2.

<sup>69</sup> Comprehensive and Progressive Agreement for Trans-Pacific Partnership, Dec. 30, 2018, <https://www.iilj.org/wp-content/uploads/2018/03/CPTPP-consolidated.pdf> [hereinafter *CPTPP*].

<sup>70</sup> USMCA, *supra* note 60, at art. 17.17.

reasonable opportunity to covered entities to remediate any lack of information access.

#### D. Source Code

The USMCA also includes a commitment by the parties to not require transfer to or access to the source code of software owned by a person of another party as a condition for import, distribution or sale of the software or products containing the software.<sup>71</sup> This commitment does not exclude the right of a regulatory body or judicial body of a party from requiring access to the software for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorised disclosure. Here, we see the parties seeking a balance between addressing legitimate government need for access to source code, such as to assess cybersecurity risks on the one hand, and the risk that access to source code leads to intellectual property (IP) theft on the other hand. This commitment is also subject to the USMCA general exceptions provision, modelled on GATS Article XIV provision.

#### E. Interactive Computer Services

A commitment completely new to the USMCA is that with respect to Interactive Computer Services (ICS).<sup>72</sup> This addresses the issue of intermediary liability for platforms in cases where users publish information that aids or abets illegal activity, such as circulating defamatory information. In the US, §230 of the Communications and Decency Act, 1996 immunises online publishers from torts such as defamation that arises from the material on their site.<sup>73</sup> The USMCA commitment in effect reflects this US domestic law, requiring that the parties must not hold suppliers or users of the ICS liable for harm related to information stored or processed by the ICS, except where the supplier or user has created the information.<sup>74</sup>

This USMCA commitment also requires that exemption from harm extends to action taken to edit harmful or objectionable material as well as actions that enable content providers to restrict access. This allows for actions to restrict content without being deemed as publisher that voids the liability exemption required under paragraph 2.

#### F. Cybersecurity

---

<sup>71</sup>*Id.* at art. 19.16.

<sup>72</sup> USMCA, *supra* note 60, at art. 19.17.

<sup>73</sup> Communications Decency Act of 1996, Pub. L. No. 104-104, § 502, § 223(a), (e)(5), 110 Stat. 56, 133–34 (1996) (codified as amended at 47 U.S.C. § 223 (2006)).

<sup>74</sup> USMCA, *supra* note 60, at art. 19.17.2.

CPTPP is the first trade agreement to recognise the importance of building co-operation on cybersecurity.<sup>75</sup> The USMCA builds on this and includes a hortatory commitment to developing risk-based approaches to cybersecurity threats that rely on consensus-based standards and risk management best practices.<sup>76</sup> This is consistent with the focus on risk-based cybersecurity measures by the Organization for Economic Co-operation and Development (OECD) as well as the U.S. National Institute of Standards and Technology (NIST).<sup>77</sup>

### G. *Open Government Data*

USMCA is the first trade agreement to include a commitment on improving access to and sharing of government data.<sup>78</sup> This commitment does not compel any of the parties to provide access to government data. However, the recognition that public access to and the use of government information “fosters economic and social development, competitiveness and innovation”, could support more targeted domestic efforts to develop the laws and regulations needed to improve access. The commitment includes a hortatory commitment to making data available in a format that is “machine-readable and open format” and includes an agreement to cooperate further to identify ways to expand access to and the use of government information.

### H. *Privacy and Consumer Protection*

Commitments to protection of consumers engaging in e-commerce have been a feature of previous FTAs and are included in the USMCA as well.<sup>79</sup> The USMCA commitment clarifies that the commitment in the chapter on competition policy that requires each party to have laws proscribing fraudulent or deceptive practices, also applies to digital trade.<sup>80</sup> The USMCA also affirms that commitments to cooperation across borders on enforcement of consumer protection laws applies to cross-border digital trade.

A number of FTAs also include commitments to the protection of personal information, and these are also in the USMCA. The core commitment is for each party to adopt or maintain a legal framework for the protection of the personal information of users of electronic commerce.<sup>81</sup> The USMCA also requires that a

---

<sup>75</sup> CPTPP, *supra* note 69.

<sup>76</sup> USMCA, *supra* note 60, at art. 19.15.

<sup>77</sup> NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1, Apr. 25, 2019; OECD, DIGITAL SECURITY RISK MANAGEMENT FOR ECONOMIC AND SOCIAL PROSPERITY: OECD RECOMMENDATION AND COMPANION DOCUMENT (2015).

<sup>78</sup> USMCA, *supra* note 60, at art. 19.18.

<sup>79</sup> *Id.* at art. 19.7; Wu, *supra* note 59, at 14.

<sup>80</sup> USMCA, *supra* note 60, at art. 19.7.1.

<sup>81</sup> *Id.* at art. 19.8.

domestic privacy framework take into account principles and guidelines of relevant international bodies such as the Asia Pacific Economic Co-operation (APEC) Privacy Framework and the OECD Privacy Principles.<sup>82</sup> The USMCA also lists the key privacy principles, and includes a recognition by the parties that restrictions on cross-border flows of personal information should be ‘necessary and proportionate to the risks presented.’ This commitment in effect leverages progress on developing common privacy principles in the OECD and APEC into an international trade commitment. The USMCA also recognises that despite agreement on common privacy principles, countries may still end up with different legal approaches to privacy and the need to therefore develop mechanisms to promote compatibility, such as one that occurs with the APEC Cross-Border Privacy Rules system arises.<sup>83</sup>

These commitments to establishing domestic regulations are a key element in building trust in digital trade. In particular, the privacy commitment includes a commitment to non-discriminatory protection of users of digital trade from violations occurring within its territory, which would require that domestic privacy legislations protect all users of digital trade, and not only citizens or those physically present.

#### I. *The USMCA Intellectual Property Chapter*

A country’s domestic IP regime is a key legal underpinning for the development of digital economy and digital trade.<sup>84</sup> On the one hand, one of the key IP challenges from the internet has been the ease with which copying can occur of copyright protected content such as music, software and film. Yet, on the other hand, making search engines liable for all copyright infringing material would have likely doomed these businesses and more broadly, the development of the digital economy. As the OECD has noted, IP policy can discourage innovation if pursued too strongly or too weakly.<sup>85</sup> For example, in an era of routine copying of text, data and images, copyright law may hinder the emergence of new kinds of internet-based firms. It may also make scientists and other researchers reluctant to use text and data-mining techniques.<sup>86</sup> As such, it is important to strike a balance between IP protection that encourages innovation and maintaining competition and the diffusion of ideas over the internet.

---

<sup>82</sup>*Id.* at art. 19.8.2.

<sup>83</sup>*Id.* at art. 19.8.6; Aaditya Mattoo & Joshua P. Meltzer, *Data Flows and Privacy: The Conflict and its Resolution*, 21(4) J. INT’L ECON. L 769 (2018) [hereinafter Mattoo].

<sup>84</sup> Anupam Chander, *How Law Made Silicon Valley*, 63(3) EMORY L. J. 639, (2013).

<sup>85</sup> OECD, *New Sources of Growth: Knowledge-Based Capital*, OECD Publishing Synthesis Report (Oct., 2013), <https://www.oecd.org/sti/inno/knowledge-based-capital-synthesis.pdf>. at 44.

<sup>86</sup>*Id.*

The balance struck in the USMCA regarding copyright is also reflected in § 512 of the Digital Millennium Copyright Act, 1998 (DMCA). The DMCA gives online service providers (OSPs) a safe harbour from secondary liability for their users' copyright infringement and, in return, OSPs are required to take down infringing material from their website upon receipt of a takedown notice.<sup>87</sup> The USMCA requires the parties to have a similar legal framework in place.<sup>88</sup>

## V. BUILDING ON USMCA FOR DIGITAL TRADE GOVERNANCE

These digital trade commitments in the USMCA are significant and will help underpin growth in digital trade. However, there are other areas where trade policy can support digital trade. As outlined above, regulatory needs and regulatory differences between countries in areas such as privacy and cybersecurity are key drivers of restrictions on cross-border data flows. Until regulators have confidence that allowing data to leave their jurisdiction will not undermine domestic regulatory goals, there will remain a strong incentive to restrict data flows and the opportunities for digital trade.<sup>89</sup> Without getting at these regulatory drivers of data restrictions, even with commitments to cross-border data flows, governments will either seek significant carve outs – as happened with respect to Vietnam's data flows commitments under CPTPP, or are expected to rely on the exception provisions to continue to justify data flows restrictions, risking that the exception will become the rule. For example, the EU proposal in the WTO ecommerce negotiations includes a broad self-judging exception to data flows commitment with respect to the protection of personal data and privacy.<sup>90</sup>

The exceptions in the USMCA applicable to digital trade require trade restrictions to be 'necessary' – that no alternatives that are less restrictive exist that would make it possible to achieve the WTO Members' legitimate regulatory objective. In order for this requirement to be meaningful, it requires developing alternatives and less trade-restrictive options that support domestic regulatory goals while minimising the impact on digital trade and cross-border data flows. Developing less trade restrictive options that achieve the Members' desired regulatory goals will require more comprehensive cross-border cooperation amongst regulators as well as setting international standards in areas such as cybersecurity, privacy, AI, and consumer protection.

---

<sup>87</sup> Digital Millennium Copyright Act, 17 U.S.C. §§ 512(a)-(d) (1998).

<sup>88</sup> USMCA, *supra* note 60, at art. 20.89.

<sup>89</sup> Mattoo, *supra* note 83, at 18.

<sup>90</sup> EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, Communication from the European Union, INF/ECOM/22 (Apr. 26, 2019).

Making progress will require moving beyond typical mercantilist trade negotiating dynamics that are focused on balancing domestic reductions in barriers with identifying market access for exports elsewhere. Domestic regulators care less about market access overseas than they do about ensuring the effectiveness of domestic regulation.<sup>91</sup> Instead, domestic regulators need to assess the impact of reform of domestic regulation—in this case, reducing restrictions on data flows—on domestic regulatory goals, alternative courses of action, examination of what has worked in other countries and the cost/benefit of these approaches.

*A. Developing International Standards for Digital Trade*

One solution for achieving domestic goals (like privacy protection) while optimising cross-border data flows is to globally harmonise standards being developed by governments and private sector bodies. The goal of the international harmonisation of standards to minimise trade barriers is not new but takes on additional urgency in a world where cross-border data flows are large and data flow restrictions are potentially very costly.

International standards can help address data flow restrictions. In areas such as cybersecurity and privacy, many of these standards are needed in order to build and maintain trust and in this respect, they are also constitutive of markets. International standards can reduce the information cost for consumers by determining whether digital products are safe for instance, or whether they adequately protect personal data or not. Standards will also be needed to enable Supply Chain 4.0 and smart manufacturing.

The TBT Agreement provides a useful framework for thinking about how to use trade rules and how to develop forms of international regulatory cooperation that can address the impact of divergent domestic standards on cross-border data flows and trade in digital services. The key TBT commitments have also been replicated in FTAs, including Chapter 11 of the USMCA.

One aspect of the TBT Agreement that is relevant for digital trade is the commitment, that where international standards exist, members will use the standards as a basis for their technical regulations.<sup>92</sup> This then creates a presumption that the technical regulation is not an unnecessary barrier to trade.<sup>93</sup> The TBT Agreement does not define international standards. The WTO TBT

---

<sup>91</sup> Geza Feketekuty, *Needed: A new approach to reduce regulatory barriers to trade*, VOX CEPR POLY PORTAL (June 19, 2010), <https://voxeu.org/article/needed-new-approach-reduce-regulatory-barriers-trade>.

<sup>92</sup> Agreement on Technical Barriers to Trade, art. 2.4, 1868 U.N.T.S. 120, Jan. 1, 1995 [hereinafter TBT Agreement].

<sup>93</sup>*Id.* at art. 2.5.

Committee Decision on International Standards provides principles and guidelines for the development of international standards for the purposes of the TBT Agreement.<sup>94</sup> The Appellate Body in *Tuna-Dolphin II*, found that this WTO Committee Decision is a ‘subsequent agreement’ within the meaning of Article 31(3)(a) of the Vienna Convention on Law of Treaties and thereby informs the interpretation of the TBT Agreement.<sup>95</sup> The USMCA incorporates this TBT Committee Decision by defining an international standard as “a standard that is consistent with the TBT Committee Decision on International Standards”.<sup>96</sup> The USMCA makes the principles and criteria in this TBT Committee Decision as the sole determinant as to whether a standard is an international standard or not.<sup>97</sup>

However, the regulatory challenges raised by digital trade do not map cleanly onto the approach in the TBT Agreement for dealing with regulatory issues affecting trade in goods.<sup>98</sup> One difference is that many of the domestic regulatory issues leading to restrictions on data flows are not obviously amenable to being standardised globally by technically focused bodies such as the International Organization for Standardization (ISO). In some areas, such as cybersecurity, the ISO has had success, such as with its ISO/IEC 27000 set of cyber and information security standards which provide a common baseline and approach that governments can follow when developing domestic cyber regulations. Yet, in areas such as privacy, consumer protection, and AI, the issues at stake—such as how to balance privacy and other values such as free speech and economic development—raise values that need to be traded-off, or balanced, in a more explicit political process. This may be why privacy, consumer protection, and AI principles have instead been initially developed in the OECD and the U.N., where the types of government-to-government bargaining, reason giving, and voting better reflect the interests at stake—underpinning the potential power of such norms.<sup>99</sup> The fact that some outcomes are expressed as general principles (such as the OECD

---

<sup>94</sup> WTO Secretariat, *Decisions and Recommendations adopted by the WTO Committee on technical barriers to trade since 1 January 1995*, ¶ 47, G/TBT/1/Rev.12 (Jan. 1, 2015).

<sup>95</sup> Appellate Body Report, *United States — Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products*, ¶ 372, WTO Doc. WT/DS381/AB/R, (adopted June 13, 2012) [hereinafter *US-Tuna II (Mexico)*].

<sup>96</sup> USMCA, *supra* note 60, at art. 11.1.

<sup>97</sup> *Id.* at art. 11.4.3.

<sup>98</sup> Bernard Hoekman & Petros C. Mavroidis, *A Technical Barriers to Trade Agreement for Services?*, ROBERT SCHUMAN CENTRE FOR ADVANCED STUDIES, Research Paper No. RSCAS 2015/25 (2015).

<sup>99</sup> Martha Finnemore & Duncan B Hollis, *Constructing Norms for Global Cybersecurity*, 110(3) AM. J. INT’L L. 425 (2016).



privacy principles) underscores the challenges of building a common ground on some of these issues.<sup>100</sup>

This suggests that when it comes to developing global international services standards, flexibility is needed to include standards (and principles) that are developed in a forum among a subset of WTO members. In fact, the TBT Agreement also applies to standards not adopted by consensus and the WTO Appellate Body has been prepared to consider non-consensually developed standards as well.<sup>101</sup> But, the Appellate Body has also indicated a greater scrutiny of the process of standards setting-before a standard will be deemed to be the relevant benchmark.<sup>102</sup>

Where international standards are developed using only a subset of WTO Members, those WTO Members that are not party to these standards should not be required to use them as a basis for their domestic regulation. However, requiring consideration of such standards when developing domestic regulation, including reasons for departing from such standards in domestic regulation would facilitate learning and dialogue aimed at minimising regulatory diversity and its impact on digital trade. For example, in USMCA, where there are no applicable international standards, the parties have agreed to consider whether a standard developed by a standards body situated within one of the parties can fulfil its legitimate objective, and where this standard is considered but rejected, they are to provide a written explanation.<sup>103</sup> A similar commitment could be extended as well to standards developed in regional standards bodies that do not otherwise meet the definition of an international standard. In addition, such standards could be predicated on having in place procedures for voting, transparency, openness, and deliberation, which support the legitimacy of the output of these bodies.<sup>104</sup>

---

<sup>100</sup> Whether expressed as principles or as standards, what constitutes an ‘international standard’ for the purposes of the TBT agreement is determined by whether the process for agreeing the outcome complies with the TBT Agreement and related WTO TBT Decision.

<sup>101</sup> Appellate Body Report, *European Communities — Trade Description of Sardines*, WTO Doc. WT/DS231/AB/R (adopted Oct. 23, 2002) [hereinafter EC-Sardines].

<sup>102</sup> See US-Tuna II (Mexico), *supra* note 95, at 21.

<sup>103</sup> USMCA, *supra* note 60, at art. 11.5.4.

<sup>104</sup> WTO Committee on Technical Barriers to Trade, *Decisions of the Committee on Principles for the Development of International Standards, Guides and Recommendations with Relation to Article 2, 5 and Annex 3 of the Agreement*, WTO Doc. G/TBT/9 (Nov. 13, 2000), which agreed six principles that should be observed by international standards setting bodies: transparency; openness, impartiality and consensus; effectiveness and relevance; and addressing the concerns of the developing world. FTAs such as CPTPP and USMCA references this TBT Decisions as laying out the process for establishing standards.

B. *Limits to International Standards in Addressing the Regulatory Challenges to Digital Trade*

While there has been progress in developing international services standards, such as in the OECD on privacy principles, these outcomes also reveal their limits in creating an enabling environment for digital trade. In particular, much of the regulatory heterogeneity between countries that leads to data flows restrictions also reflects different underlying values, which is a break on the extent that international services standards can drive convergence at the local level. In the EU, for example, privacy and data protection are constitutional rights guaranteed in the Charter of Fundamental Rights of the European Union.<sup>105</sup> In contrast, in the U.S., there is a limited constitutional right to privacy—focused on the right of privacy as against the government, and when it comes to data protection by commercial enterprises, privacy regulation needs to be consistent with the constitutional right to free speech.<sup>106</sup> These differences have meant that the agreement on privacy in the OECD was a set of principles that left governments with significant flexibility to craft privacy regulations to reflect domestic values and laws.

For example, the updated 2013 OECD Privacy Principles articulate core standards of privacy, the mechanisms for cross-border data flows, and under what conditions restrictions on such data flows are necessary. The OECD privacy principles affirm the accountability of the data controller for personal data under its control and recognise two cases where restrictions on cross-border transfers of personal data should be avoided—where the recipient country ‘substantially’ observes the OECD privacy principles, or where there are safeguards to ensure that the recipient continues to protect personal data consistent with the OECD privacy principles.<sup>107</sup> As these OECD privacy principles are voluntary baselines, some OECD governments have chosen to go further in their domestic privacy regulation. For instance, the EU GDPR requirements of explicit consent—which limits the purposes to which personal data once collected can be used, as well as the right to forget—are some areas where the GDPR has gone beyond the OECD privacy standards.<sup>108</sup> As a result, the GDPR diverges from where other OECD members such as the U.S. and Australia have ended up in their domestic privacy regulations, yet which regulations are also consistent with the OECD privacy principles.

---

<sup>105</sup> Charter of Fundamental Rights of the European Union, art. 8, 2000/C 364/01, Dec. 7, 2000.

<sup>106</sup> Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011).

<sup>107</sup> OECD, *The OECD Privacy Framework*, ¶¶69-80 (2013) [https://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf).

<sup>108</sup> GDPR, *supra* note 39, at art. 15-20.

These differences in the approach to privacy among OECD members meant that instead of the EU allowing cross-border transfers of personal data to countries that ‘substantially’ observe the OECD privacy principles, the GDPR requires that third countries provide ‘adequate’ privacy protection, which requires having in place, levels of privacy protection that are substantially equivalent to those provided under the GDPR.<sup>109</sup> Marrying this much tighter requirement of a fit between the GDPR and the recipient country’s privacy regulation, along with the ratcheting up of data privacy standards in the GDPR has limited the potential of the OECD privacy principles to bridge differences in privacy regulations and facilitate cross-border data flows.

Despite these limitations, the development of a common baseline on privacy principles has been useful. While not leading to common approaches in practice, the OECD privacy principles have minimised regulatory heterogeneity, making the process of developing interoperability mechanisms that can bridge the difference between domestic privacy regimes and make it less challenging than it would otherwise be. In fact, Privacy Shield (and Safe Harbour before that) was facilitated by much of what is common (and OECD consistent) between the U.S. and EU on privacy. In other areas such as cybersecurity, which is more technically orientated than privacy, success developing a number of international standards such as the ISO/IEC 27000 series (ISMS Family of Standards), indicates that there may be even greater scope for international standards leading to common global cybersecurity practice that gives cyber regulators confidence that cross-border data flows do not undermine cybersecurity.

### *C. Using Trade Policy to Build International Regulatory Cooperation*

As outlined, there are not insignificant challenges in developing international services standards, and there are limits on the extent standards can overcome the regulatory diversity that leads to restrictions on data flows. This also underscores the need to develop rules in the WTO and in FTAs, that underpin the international regulatory cooperation and interoperability mechanisms, such as the APEC Cross-Border Privacy Rules, that can bridge differences in domestic regulations which lead to data flows restrictions.<sup>110</sup>

Building bridges between countries with different regulatory systems to minimise trade costs is not new. The OECD has identified eleven forms of international regulatory cooperation which includes Mutual Recognition Agreements (MRAs)

---

<sup>109</sup> Schrems v. Data Protection Comm’r, ¶ 73, [2014] I.E.H.C. 310.

<sup>110</sup> *What is cross-border privacy rules system?*, APEC (Apr. 15, 2019), <https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System>.

and recognition of equivalency.<sup>111</sup> Both of these interoperability mechanisms are the focus here due to their specifically intergovernmental nature, and as examples of types of international regulatory cooperation that the WTO can enable.

#### D. *Mutual Recognition Agreements/Arrangements (MRA)*

There are various forms that an MRA can take. MRAs can be built on countries harmonising underlying regulations and recognising the conformity assessment done in the exporting country of compliance with the regulation. Such comprehensive MRAs are relatively rare and have been realised in the EU internal market and under the Trans-Tasman Mutual Recognition Agreement (TTMRA). Less ambitious MRAs do not result in any changes in the underlying regulation and instead recognise conformity assessment of compliance by the exporting country of compliance with the importing country's regulation.<sup>112</sup> Recognition of conformity assessment can be government-to-government or can involve arrangements between private conformity assessment bodies from different countries. MRAs can also be legally binding – such as the TTMRA, or voluntary, such as the APEC TEL MRA.<sup>113</sup>

An MRA for digital trade would require the data destination country to apply the data source regulations to data imports, and consequently the data source country recognising it would then allow the data to flow. To work effectively, this requires not only an application by the data destination country of the data source standards, but the data source country must also recognise the capacity of the regulator in the data destination country to assess conformity. The U.S.-EU Privacy Shield arrangement is one example where what is in effect is an MRA whereby participating U.S. businesses comply with standards equivalent to the GDPR and the EU recognises enforcement/oversight by the US Department of Commerce and Federal Trade Commission.<sup>114</sup>

#### E. *U.S.- EU Privacy Shield*

The Privacy Shield (which replaced the EU-U.S. Safe Harbour framework) allows for flow of personal data between the U.S. and the EU. The EU has certified the

---

<sup>111</sup> OECD, *International Regulatory Co-operation – Addressing Global Challenges* (Apr. 24, 2013), <https://www.oecd.org/env/international-regulatory-co-operation-9789264200463-en.htm>.

<sup>112</sup> J. Pelkmans et al., *The Contribution of Mutual Recognition to International Regulatory Co-Operation*, OECD REGULATORY POLY PAPERS, WORKING PAPER NO. 2, (2016) [hereinafter Pelkmans et al.].

<sup>113</sup> APEC, *Mutual Recognition Arrangement for Conformity Assessment of Telecommunications Equipment*, WORKING PAPER NO. 1 APEC#202-TC-01.1, (1998), <http://publications.apec.org/Publications/1998/05/Mutual-Recognition-Arrangement-for-Conformity-Assessment-of-Telecommunications-Equipment>.

<sup>114</sup> Mattoo, *supra* note 83, at 18.

Privacy Shield as ‘adequate’ under the GDPR, thereby allowing transfers of personal data from the EU to U.S. by companies participating in the Privacy Shield. Under the Privacy Shield, U.S. companies, through an industry body or individually, self-certify to the U.S. Department of Commerce that they will protect personal data consistent with the Privacy Framework, which includes the Privacy Shield Principles.<sup>115</sup> Oversight and enforcement is the responsibility of the U.S. Federal Trade Commission and Department of Commerce. An ombudsperson can respond to complaints by EU citizens about access by U.S. intelligence agencies to the personal data of EU citizens.

Another form of MRA – a so-called enhanced MRA – also has regulatory alignment between the participating countries. However, these arrangements are limited to countries where there is a high level of integration, such as exists in the EU and as reflected in the Australia-New Zealand Closer Economic Relations Trade Arrangement.

#### F. *Equivalence*

A data source country can also recognise that a data destination country’s regulation and conformity assessment is equivalent to its own.<sup>116</sup> Equivalency can be granted unilaterally or by agreement. Equivalency is in effect what happens under the GDPR when the European Commission issues a finding of adequacy with respect to another country’s privacy protection regime.

While the WTO has rules on MRAs in the TBT Agreement, most MRAs, for instance, are standalone agreements or have been incorporated into FTAs. This reflects a preference for bilateral arrangements and those ambitious MRAs (in particular enhanced MRAs) require similar regulatory systems and levels of development.

Assuming this trend of MRAs being done outside the WTO continues, countries should focus on developing MRAs in bilateral and regional FTAs relevant for digital trade. The USMCA includes TBT Agreement plus rules on mutual recognition as well as conformity assessment and accreditation, all of which supports the acceptance of standards and conformity assessment procedures amongst the parties, reducing the need for duplicated testing.<sup>117</sup> These rules are not digital trade specific but would also support interoperability when it comes to digital trade and data flows across countries with different regulations.

---

<sup>115</sup> Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield 2016, O.J. (L 207) 1.

<sup>116</sup> Pelkmans et al., *supra* note 112, at 25.

<sup>117</sup> USMCA, *supra* note 60, at arts. 11.16-11.17.

### G. Regulatory Best Practice for Digital Trade

The development of Good Regulatory Practices (GRPs) has received some attention in the WTO TBT Committee, and is an increasing feature of more recent FTAs such as the USMCA.<sup>118</sup> GRPs can include process elements, such as transparency, consultation, and reason giving as well as commitments aimed at improving regulatory outcomes, such as being welfare maximising and cost-effective, and when it comes to trade, being least trade restrictive and not creating unnecessary barriers to trade.<sup>119</sup> In addition, GRPs are likely a building block towards some of the forms of international regulatory cooperation outlined above.<sup>120</sup>

From a narrower digital trade perspective, GRPs should be developed to mainstream consideration of the impact of regulation on data flows as well as access to data. This can be done by requiring regulators to conduct a regulatory impact assessment that includes the impact on cross-border data flows. For instance, the USMCA requires a regulatory impact assessment of a technical regulation's potential impacts but does not specifically require assessment of the impact on data flows or digital trade.<sup>121</sup> Having regulators consider digital trade effects as part of the process of developing the regulation can also help identify less trade restrictive options. In the digital trade context, the increasing economy-wide use of data means that GRPs should also emphasise the importance of coordination among government agencies when developing regulations that affect data flows.

## VI. CONCLUSION

The growth in digital connectivity through expanded internet access and the increasing use of mobile devices is affecting how economies grow, innovate and trade. This paper has focused on how cross-border data flows are transforming international trade, creating new opportunities for more inclusive trade for MSMEs, and developing countries' using platforms to reach consumers globally

---

<sup>118</sup> *Id.* at art. 28.2; WTO Committee on Technical Barriers to Trade, *Fifth Triennial Review of the Operation and Implementation of the Agreement on Technical Barriers to Trade under Article 15.4*, WTO Doc. G/TBT/26, (Nov. 13, 2009).

<sup>119</sup> Robert Basedow & Celine Kauffmann, *International Trade and Good Regulatory Practices: Assessing the Trade Impacts of Regulation*, OECD REGULATORY POLY, WORKING PAPER NO. 4, (2016).

<sup>120</sup> OECD, *International Regulatory Co-operation and Trade: Understanding the Trade Costs of Regulatory Divergence and the Remedies*, ¶ 34 (May 24, 2017), <https://www.oecd.org/gov/international-regulatory-co-operation-and-trade-9789264275942-en.htm>.

<sup>121</sup> USMCA, *supra* note 60, at art. 11.5.1.

and expanding opportunities for participation in GVCs. Cross-border data flows are also supporting growth in services trade, whether directly exported online or as a growing share of the value of goods exports. At the same time, the growing digitization trade is creating challenges for a range of regulatory goals, such as privacy and security. The regulatory response is often to restrict data flows; however, this can undermine the economic opportunities from data flows and digital trade. Such a regulation often operates as a behind-the-border measure. For instance, unnecessary regulatory diversity across countries raises the costs of exporting, particularly for MSMEs that lack the resources to meet different privacy or consumer protection regimes for data in each market.

Such a regulation may also be discriminatory where its primary impact is on imports, in breach of WTO trade rules. Under the WTO, data must be allowed to flow where needed in order to deliver services where GATS commitments have been made. Yet, WTO rules are limited, not least by the limited scope of GATS services commitments and the ambiguity surrounding the extent of existing GATS commitments covering new digital service such as cloud computing or online gaming. A range of governments have responded by developing new digital trade rules in bilateral and regional trade agreements. The USMCA is the latest of these trade agreements which includes the most ambitious set of digital trade rules currently around. Yet, even here, more is needed to support cross-border data flows, as well as the international regulatory cooperation and good regulatory practice that is required to provide an effective mechanism for digital trade governance.

When it comes to developing rules on international regulatory cooperation, this paper draws on WTO and FTA rules in the TBT chapters to develop a pathway for how trade policy could develop trade rules supporting cross-border data flows which still recognise the need for governments to have the space to pursue legitimate regulatory goals. The proposed trade rules include commitments to develop international standards relevant for regulation affecting data flows, such as in areas of privacy, consumer protection and cybersecurity. Yet, international standards are unlikely to be sufficient and regulatory differences are still likely to emerge that restrict data flows.

This paper also outlines how trade rules can go further and support the development of interoperability mechanisms such as MRAs and commitments to good regulatory practices, that can provide ways for data to flow, even in the presence of regulatory diversity. Many of the proposed developments would be beneficial for MSMEs. Yet, participating in interoperability mechanisms could be challenging for some developing countries due to the lack of domestic capacity, pointing to the need for international support to build domestic capacity. These

proposals could be considered as a part of the WTO e-commerce negotiations in the context of future FTAs.