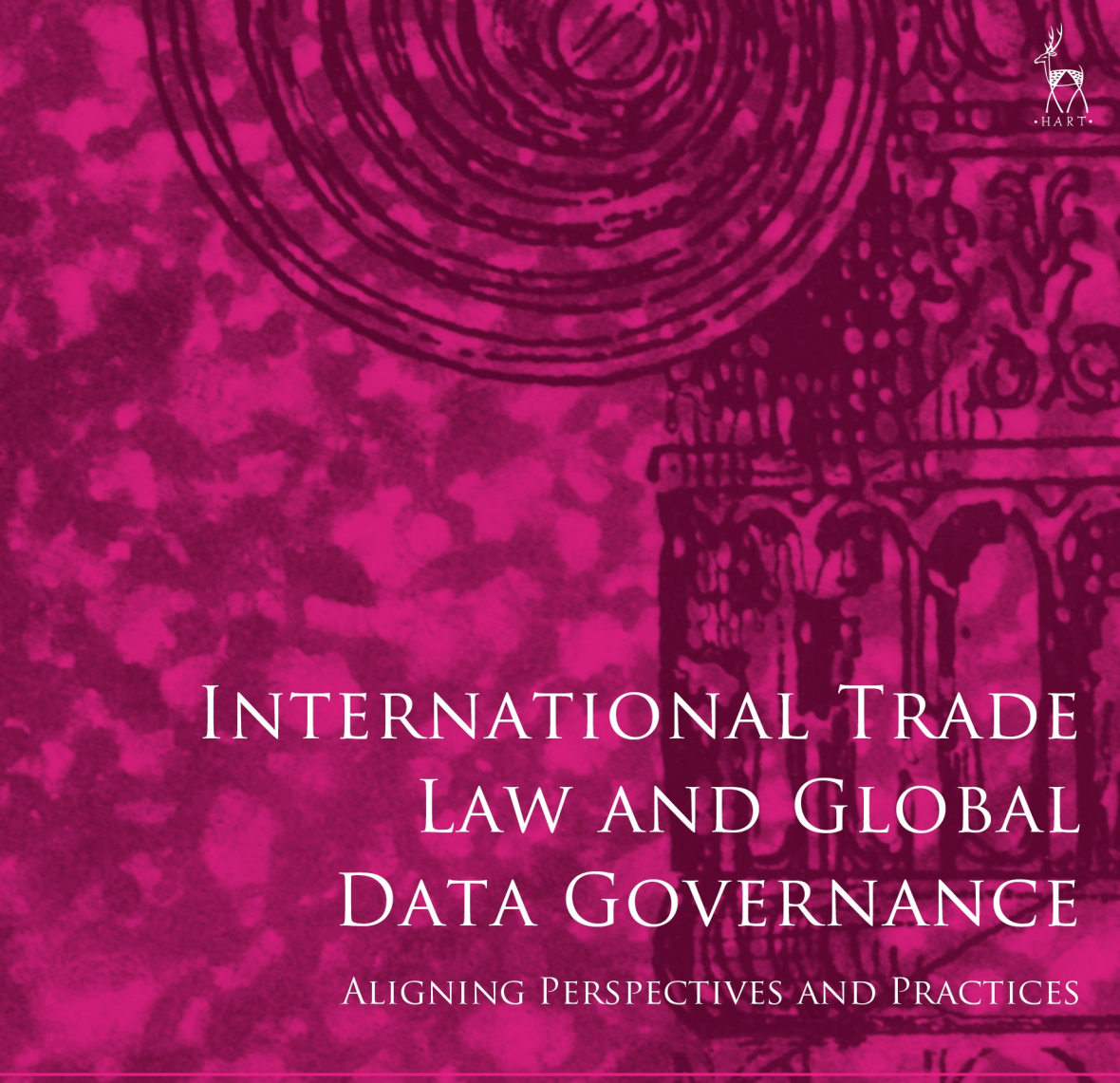

International Trade Law and Global Data Governance

Aligning Perspectives and Practices

Studies in International Trade and Investment Law

Neha Mishra

INTERNATIONAL TRADE LAW AND GLOBAL DATA GOVERNANCE

This open access book examines how international trade agreements apply to domestic regulations on cross-border data flows and then proposes a multilayered framework to align international trade law with evolving norms and practices in global data governance.

Digital trade and global data governance are at a unique crossroads, raising significant policy challenges. The book focuses on five policy areas at the interface of digital trade and global data governance: privacy, cybersecurity, governmental access to data, data divide, and competition. In five separate chapters, the book analyses how different types of domestic laws in each of these policy areas interface with existing provisions in international trade law. Thereafter, each of these chapters explores the challenges and possibilities for aligning international trade law with evolving norms, standards and best practices in that specific area of data regulation, both at the domestic and transnational level.

Drawing upon these findings, the final chapter proposes a multilayered framework for aligning international trade law with evolving norms and practices in global data governance. The key message of the book is that international trade law can and should meaningfully align with and contribute to the development of transnational data governance norms and practices. It can also foster robust regulatory cooperation among various stakeholders of the digital economy.

As the book offers a broad perspective on the significance of digital trade rules in a datafied world, it will benefit scholars, practitioners and policymakers working on digital trade and data regulation, helping its readers explore fresh avenues in the future development of digital trade rules.

Studies in International Trade and Investment Law: Volume 31

Studies in International Trade and Investment Law

Series Editors
Gabrielle Marceau
Krista Nadakavukaren Schefer
Federico Ortino
Gregory Shaffer

This series offers a forum for publication of original and scholarly analyses of emerging and significant issues in international trade and investment law – broadly understood to include the whole of the law of the WTO, the public international law of foreign investment, the law of the EU common commercial policy and other regional trade regimes, and any legal or regulatory topic that interacts with global trade and foreign investment. The aim of the series is to produce works which will be readily accessible to trade and investment law scholars and practitioners alike.

Recent titles in this series:

Patent Games in the Global South: Pharmaceutical Patent Law Making in Brazil, India and Nigeria
Amaka Vanni

The Nationality of Corporate Investors under International Investment Law
Anil Yilmaz Vastardis

The Regulation of Product Standards in World Trade Law
Ming Du

Investors' International Law
Edited by Jean Ho and Mavluda Sattorova

Rethinking, Repackaging, and Rescuing World Trade Law in the Post-Pandemic Era
Edited by Amrita Bahri, Weihan Zhou and Daria Boklan

Flexible Regional Economic Integration in Africa: Lessons and Implications for the Multilateral Trading System
Timothy Masiko

International Investment Law: An Analysis of the Major Decisions
Edited by Hélène Ruiz Fabri and Edoardo Stoppioni

State Capitalism and International Investment Law
Edited by Panagiotis Delimatsis, Georgios Dimitropoulos and Anastasios Gourgourinis

The European Union and International Investment Law: The Two Dimensions of an Uneasy Relationship
Francesco Montanaro

Financial Market Infrastructure and Economic Integration: A WTO, FTAs, and Competition Law Analysis
George A Papaconstantinou

International Trade Law and Global Data Governance

Aligning Perspectives and Practices

Neha Mishra

• HART •
OXFORD • LONDON • NEW YORK • NEW DELHI • SYDNEY

HART PUBLISHING

Bloomsbury Publishing Plc

Kemp House, Chawley Park, Cumnor Hill, Oxford, OX2 9PH, UK

1385 Broadway, New York, NY 10018, USA

29 Earlsfort Terrace, Dublin 2, Ireland

HART PUBLISHING, the Hart/Stag logo, BLOOMSBURY and the Diana logo are trademarks of Bloomsbury Publishing Plc

First published in Great Britain 2024

Open access was funded by the Swiss National Science Foundation.

A catalogue record for this book is available from the British Library.

A catalogue record for this book is available from the Library of Congress.

Library of Congress Control Number: 2023949175

ISBN: HB: 978-1-50996-169-6
ePDF: 978-1-50996-171-9
ePub: 978-1-50996-170-2
Book DOI: 10.5040/9781509961726

Typeset by Compuscript Ltd, Shannon

For my dearest Aja

Foreword: Pathways to Aligning International Trade Law and Contemporary Data Governance

We live in a world where data has become the lifeblood of our interconnected existence, driving innovation, economic growth and societal transformation. The ability to harness the immense power of data has the potential to propel nations and companies into new frontiers of prosperity and technological advancement. Yet, the data governance landscape is far from straightforward, and the regulatory framework is complex and continuously evolving, marked with technological breakthroughs, geopolitical shifts and a myriad of rulemaking initiatives across different domains and levels of governance. In such a dynamic environment, it takes a special kind of scholar to not only comprehend the intricacies of the data-driven economy but also to offer a comprehensive understanding of the rules that govern it. The author of this book, Neha Mishra, is that special scholar. With a deep commitment to the subject of international trade law but also with a profound understanding of the developments in other legal domains, Neha has approached the new field of data governance with incredible intellectual rigour and a keen eye for detail. Her work is a testament to the power of scholarship to dissect complex issues, engage in well-grounded legal analyses but also in forward-looking debates that can transform international trade law and its role in the broader field of data governance.

This book provides on the one hand a panoramic view of the challenges and opportunities that the data-driven economy presents, as well as the legal and policy measures that are essential to its governance. On the other hand, and quite innovatively so, Neha's work delves deep into the regulatory dilemmas standing before international trade law and its intersection with key areas of data governance – data privacy; cybersecurity; governmental access to data, the global data divide and competition law. Neha not only examines the legal and policy issues pertinent to these domains but also skillfully links the discussions and in this way overcomes and bridges existing silos.

The book builds upon existing scholarship and shows clearly that international trade law is relevant for our datafied world. Neha does not stop there, however, but thinking outside the box, charts pathways as to how international trade law and global data governance can be aligned. In this future-oriented exercise, Neha is innovative but also very pragmatic – she is sensitive to the

different objectives that sovereign states may wish to pursue in the field of data governance and well aware of both the different capacities across countries and the constraints of legal regimes. In this sense, the book puts forward a sensible and potentially feasible agenda to combine conventional trade law disciplines with other soft law norms, best practices and institutional innovations, so as to enable a more decentralised and multilayered framework for digital trade. In suggesting interoperability mechanisms, Neha also highlights the importance of multistakeholder participation and recommends various channels to incorporate private norms and standards by referencing them in trade provisions, in order to make the entire framework more balanced, inclusive and sustainable over time. The paths that Neha's work chart do tackle the currently present costly regulatory fragmentation in data governance and therewith linked legal uncertainty. On the positive side, Neha's agenda contributes in a meaningful way to strengthening international cooperation and trust, which again addresses the challenge of the sustainability of the regime complex of data governance.

In closing, Neha's book is a remarkable contribution to the ongoing discussions about the regulation of the data-driven economy and the role of international trade law in this landscape. It is a beacon of knowledge and understanding in a complex environment and offers an invaluable resource to anyone seeking to navigate the digital trade law frontier. One ought to highlight here that Neha has achieved an almost optimal level of granularity in her analyses, so that the book's enquiries will add value to both experienced trade law experts and experts from other legal and policy domains but also remain accessible for curious readers who would like to know more about the present and the future of regulatory framework of our data-dependent societies.

I am confident that Neha's work will inform, provoke thought and inspire. It certainly did so for me.

Mira Burri
30 October 2023

Preface

Digital trade is everywhere. At the heart of digital trade is the Internet. As a globally interconnected network, the Internet has facilitated cross-border data flows and thereby enabled the growth of a gigantic data-driven economy. We are all consumers in this data-driven economy, consciously or unconsciously. Almost every country today is devising grand strategies to maximise economic and, potentially, political benefits from this data-driven economy and eventually fulfil their dream of becoming important players in the global digital economy. More companies and entrepreneurs are now able to offer their products and services online to users across the world. Similarly, consumers now have a wide choice of digital products and services from across the world at competitive prices.

Although the promise of digital trade has created numerous opportunities for economic growth, it is not without its challenges. As this book highlights, the increased 'datafication' of our world has created several threats to the integrity and stability of the global economic order. We increasingly see countries engaging in geopolitical conflicts in the technological domain. The last few years have seen a rapid rise in inward-looking domestic regulatory measures, which fragment the global regulatory framework for digital trade. Some of these governmental measures also adversely affect the global network of the Internet and prejudice its seamless connectivity by restricting cross-border data flows. These restrictions are expectedly creating impediments to digital trade. However, governments often implement these measures with seemingly legitimate domestic policy objectives in mind, thus creating a dilemma between liberalising digital trade flows and protecting public policy objectives.

With the datafication of the economy, several transnational and domestic legal and policy concerns have come to the forefront in global data governance. This has motivated governments across the world to take urgent legal and policy actions. The examples of such concerns are endless. Internet users are increasingly at risk of falling prey to cybercrimes and data breaches. Some of the biggest digital technology companies now act as data monopolies and exploit their users, including by illegally surveilling them and creating self-contained digital ecosystems, where individual and group privacy is at risk. Further, governments are seeking control of our data to monitor and shape several aspects of our lives for both good and bad reasons. While all these changes are happening rapidly, a large part of the developing world continues to have limited digital/data infrastructure and regulatory capacity, and thus cannot benefit from the data-driven economy in a meaningful manner.

The regulatory and policy problems of our datafied world can be viewed from various disciplinary and ideological lenses. This book explores how international trade law is relevant for our datafied world. It focuses on the rise in governmental measures to regulate and restrict cross-border data flows through the globally interconnected network of the Internet, and its repercussions for both global digital trade and global data governance. In doing so, the book identifies not only how international trade law can discipline unnecessary barriers to cross-border data flows, but also, more importantly, how it can make a meaningful contribution to building a robust, coherent and inclusive global framework for data governance.

We live in a world in which the narrative of data and digital sovereignty is increasingly becoming common in both autocratic and democratic countries. This narrative has the potential to fragment not only the global economic order, but also the technical infrastructure of the Internet. It is against such a complex background that this book seeks to evaluate the role and relevance of international trade law in navigating the complexity of global data governance. In exploring this question, it looks at data regulation and its intersection with trade treaties in light of data protection/privacy, cybersecurity, governmental access to data, bridging the global data divide and competition regulation. While data protection and cybersecurity have long been discussed in the context of data/Internet governance, concerns of data divide, governmental access to data and digital competition are the more recent hot topics in global data governance.

The book provides readers with a cautiously optimistic take on why international trade law continues to be relevant for the data-driven world. It proposes that a shift in perspective and practices can help redefine the relevance of international trade law for the global digital economy. In particular, it emphasises the need to shift the digital trade narrative from conflicts and geopolitical divides to regulatory alignment, digital trust, digital inclusion and meaningful international cooperation. It seeks to build a multilayered framework for global digital trade, taking into account the multidimensional aspects of global data governance and the role of various stakeholders that enable and regulate cross-border digital flows.

This book will be of interest to not only policymakers and experts on digital trade and international economic law, but also a larger audience that wishes to learn more about the intersection of digital trade and data regulation in the modern world. Further, the broader message and policy proposals of the book is applicable in other areas of trade law and policy. While it is framed as a holistic research endeavour to explore the role of international trade law in regulating cross-border data flows, experts outside the field of international economic law may also have specific interest in specific chapters focusing on a particular area of data regulation. In the current digital world in which we seem to accept tech wars, regulatory fragmentation and the data divide as a given,

this book is a conscious effort to present ideas for aligning perspectives and practices in international trade law and global data governance.

Neha Mishra
Geneva
31 July 2023

Acknowledgements

This book is a culmination of several years of thinking and research on different aspects of digital trade and data regulation that I began at the start of my doctoral studies in April 2016. While this book develops several ideas of my doctoral thesis, it ventures into several new topics that I did not explore in my doctoral research. However, when I trace back the inspiration of this project, my doctoral thesis is perhaps still the most important foundation of this project.

At the outset, therefore, I would like to thank my PhD supervisors, Prof Tania Voon and Prof Andrew D Mitchell, for their unwavering support, and providing me with invaluable guidance, mentoring and encouragement throughout my academic career. Further, I benefited from various other inputs during my doctoral studies, especially from Prof Margaret Young as the internal commentator. I learnt immensely from my visiting fellowships at the WTO and Max Planck Institute Luxembourg, as well as my friends and colleagues at Melbourne Law School.

Several exceptional academics have played an instrumental role in shaping my thoughts and understanding of digital trade and international economic law. In particular, my thesis examiners, Prof Mira Burri and Prof Shin-yi Peng, not only generously provided me with excellent reports on my doctoral research, but since then have also provided extremely helpful feedback and guidance on other papers that have shaped my academic work.

Although the discipline of digital trade law is still emerging, several thought leaders in the field have been a constant source of inspiration for me. In particular, I would like to thank Prof Anupam Chander, who has constantly helped me think differently and innovatively on this subject both through his exceptional research and through inputs on different pieces of scholarship that I have written. Over the years, several academics and experts in the field have selflessly provided me with inputs at numerous conferences and workshops. While it is impossible to name everyone, my academic development would not have been possible without them.

A large part of this book was conceptualised while I was working as a lecturer at Australian National University (ANU) in Canberra in 2021–22. My colleagues at ANU provided me with helpful advice regarding publishing a monograph. I wrote most of this book during my time at the Geneva Graduate Institute in both 2022 and 2023. During this time, I benefited immensely from the rich academic culture at the Institute and the generous support and guidance of my colleagues, especially at the Department of International Law, for which I am extremely

grateful. I am also extremely grateful to the Swiss National Science Foundation for funding the open access publication of this monograph. A special note of thanks to Binit Agarwal for providing me with invaluable research assistance for this book project. Finally, this book would not have been possible without the support of the series editors of international economic law at Hart Publishing, as well as Roberta Bassi, Verity Stuart and Linda Goss. I am grateful to them for the opportunity and their support in publishing this work.

On a more personal note, I thank the four most important teachers in my life: my grandparents, Aai and Aja, and my parents, Bou and Nana. They have unwaveringly stood by my side and believed in me more than I ever could. Finally, I cannot end this note without thanking Prajat, who has been lovingly and patiently by my side in my life journey and has always encouraged me to be the best version of myself in everything that I do.

Contents

List of Abbreviations

AB	Appellate Body
AHKFTA	ASEAN–Hong Kong, China Free Trade Agreement
AI	artificial intelligence
APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
BCR	Binding Corporate Rules
CBPR	Cross-Border Privacy Rules
CEPA	India–UAE Comprehensive Economic Partnership Agreement
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
CPC Prov	Provisional Central Product Classification
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
DEA	digital economy agreement
DEPA	Digital Economy Partnership Agreement
DFFT	Data Free Flow with Trust
DMA	Digital Markets Act, 2022
DPA	Data Protection Authority
ECHR	European Convention on Human Rights
ECJ	Court of Justice of the European Union
EU–Korea FTA	European Union–South Korea Free Trade Agreement
EU–NZ FTA	EU–New Zealand Trade Agreement
EU–UK TCA	Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part
FED	Friends of Ecommerce for Development

FTA	Free Trade Agreement
G20	Group of 20
G7	Group of 7
GATS	General Agreement on Trade in Services
GATT	General Agreement on Tariffs and Trade
GDP	gross domestic product
GDPR	General Data Protection Regulation
GPA	Global Privacy Assembly
GVC	global value chain
IACEPA	Indonesia–Australia Comprehensive Economic Partnership Agreement
ICCPR	International Covenant on Civil and Political Rights
ICN	International Competition Network
ICT	information and communications technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IJPN	Internet Jurisdiction & Policy Network
IP	Internet Protocol
IRDAI	Insurance Regulatory and Development Authority
ISO	International Organization for Standardization
ITU	International Telecommunication Union
JSI	Joint Statement Initiative (JSI) on e-Commerce
KSDPA	Korea–Singapore Digital Partnership Agreement
LDC	least developed country
MFN	most-favoured nation
MLAT	Mutual Legal Assistance Treaty
MSME	micro-, small and medium enterprise
OECD	Organisation for Economic Co-operation and Development
PAFTA	Peru–Australia Free Trade Agreement

PRP	Privacy Recognition for Processors
PTA	preferential trade agreement
RBI	Reserve Bank of India
RCEP	Regional Comprehensive Economic Partnership
SADEA	Singapore–Australia Digital Economy Agreement
SCC	standard contractual clause
SDT	special and differential treatment
SME	small and medium enterprise
TBT	Technical Barriers to Trade
TCP	Transmission Control Protocol
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights
UDHR	Universal Declaration of Human Rights
UK–NZ FTA	United Kingdom–New Zealand Free Trade Agreement
UKSDEA	UK–Singapore Digital Economy Agreement
UNCTAD	United Nations Conference on Trade and Development
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNGA	United Nations General Assembly
UNODC	United Nations Office on Drugs and Crime
UNSC	United Nations Security Council
USITC	United States International Trade Commission
USMCA	Agreement between the United States of America, the United Mexican States, and Canada
W3C	World Wide Web Consortium
WEF	World Economic Forum
WHO	World Health Organization
WTO	World Trade Organization

Table of Cases

WTO Law

Domestic/EU Law

Table of Legislation

International Treaties

EU Law

Domestic Laws and Regulations

1

Introduction: Setting the Narrative

I. INTRODUCTION

Cross-border data flows constitute a key driving force behind the digitalisation of the global economy.[1] Data is increasingly seen as constituting the 'intangible asset[s]' and 'infrastructure' underlying the digitalised economy.[2] At the same time, the myriad policy challenges arising from ubiquitous flows of data have engendered a trust deficit among various participants of the global digital economy and hinder digital innovation and growth.[3] This book examines how international trade law can address various trade barriers arising due to governmental restrictions on cross-border data flows covering five core policy objectives related to data regulation: data privacy, cybersecurity, governmental access to data, bridging the global data divide, and competition law. With international trade law becoming one of the most visible and significant sites for the regulation of cross-border data flows, it has also become important to understand the role and relevance of international trade law in global data governance, as well as the interplay between the two. Therefore, the broader question that this book will answer is whether international trade law and global data governance can be aligned and, if so, how and to what extent.

Digital trade and data flows are ubiquitous today and fundamentally interlinked with each other, with the Internet becoming a key platform for trade

[1] See generally ML Mueller and K Grindal, 'Data Flows and the Digital Economy: Information as a Mobile Factor of Production' (2018) 21(1) *Digital Policy, Regulation and Governance* 71, 82; U Ahmed, 'The Importance of Cross-Border Regulatory Cooperation in an Era of Digital Trade' (2019) 18(S1) *World Trade Law Review* s99; J Bughin and S Lund, 'The Ascendancy of International Data Flows' (McKinsey Global Institute, 9 January 2017) www.mckinsey.com/mgi/overview/in-the-news/the-ascendancy-of-international-data-flows; Kommerskollegium, 'No Transfer, No Production – a Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods' (2015:4).

[2] D Ciuriak, 'Rethinking Industrial Policy for the Data-driven Economy' (Centre for International Governance Innovation (CIGI), October 2018) CIGI Paper No 82, 6.

[3] See generally World Bank, *World Development Report 2021: Data For Better Lives* (2021); G Shaffer, 'Trade Law in a Data-Driven Economy: The Need for Modesty and Resilience' (2021) 20(3) *World Trade Review* 259; N Mishra, 'International Trade, Internet Governance and the Shaping of the Digital Economy' (2017) UNESCAP ARTNeT Working Paper No 168; T Nakanishi and S Hori, 'Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows' (WEF, 2023).

transactions. Most countries place utmost importance in maximising the socio-economic (and increasingly, political) benefits of digital and cross-border data flows for their communities. It is in view of this bigger goal that this book offers various proposals to find stronger alignment between international trade law and global data governance. However, it does not claim that international trade law can or must, by itself, address all the policy dilemmas underlying the regulation of cross-border data flows. Nor does it claim that a one-size-fits-all approach is possible to address the various challenges faced by countries at different stages of digital development or with varied ideological preferences. Similarly, it acknowledges that certain kinds of cross-border data flows may pose genuine policy risks, and governments may thus strictly regulate them despite the adverse impact on digital trade.

The conflict between a globally interconnected Internet and territorial borders lies at the heart of global data governance.[4] This tension is increasingly reflected in the way governments regulate the Internet and the data flowing through it. For instance, as several studies indicate, direct and indirect governmental measures restricting cross-border data flows through the Internet have sharply increased in the last few years.[5] A study published by the World Bank, for instance, indicates that approximately only 20 per cent countries now have an open regulatory framework for data transfers.[6]

The widespread proliferation of data-restrictive regimes across countries directly impacts the ability of businesses and consumers to conduct various online transactions, thus hampering digital trade.[7] Therefore, such regulations may violate various rules contained in various international trade treaties that apply to digital trade. As demonstrated in various chapters of this book, this interface raises many complex legal questions and entails a sensitive policy balancing exercise between digital trade and data governance concerns.

In this introductory chapter, section II introduces certain key concepts used throughout the book, such as data, cross-border data flows, data regulation and digital trade. It also explains the meaning and scope of international trade law

[4] L Porciuncula and BD La Chapelle, 'We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty' (Internet and Jurisdiction Policy Network, 2021) 5.

[5] SJ Evenett and J Fritz, 'Emergent Digital Fragmentation: The Perils of Unilateralism' (Hinrich Foundation, 28 June 2022); N Cory and L Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them' (ITIF, 19 July 2021) www.ITIF.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/; MF Ferracane et al, 'Digital Trade Restrictiveness Index' (ECIPE, 2018) www.ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf.

[6] MF Ferracane and EVD Marel, 'Regulating Personal Data: Data Models and Digital Services Trade' (World Bank, 2021) 19.

[7] See generally Cory and Dascoli (n 5); Office of the USTR, 'Key Barriers to Digital Trade' (March 2017) www.ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade; J Fritz, 'The State of Digital Trade Barriers and Internet Fragmentation' (*Digital Policy Alert*, 3 April 2022) www.digitalpolicyalert.org/blog/4-the-state-of-digital-trade-barriers-and-internet-fragmentation; I Borchert, 'Addressing Impediments to Digital Trade: A New eBook' (*VoxEU*, 27 April 2021) www.cepr.org/voxeu/columns/addressing-impediments-digital-trade-new-ebook.

and global data governance. After explaining these basic terms, the section sets out the role and relevance of the Internet in enabling digital trade and cross-border data flows.

Section III then focuses on the political economy of global data governance in the context of digital trade by highlighting two conflicting narratives pertaining to how governments think about cross-border data flows. On the one hand, several open, liberal economies (usually advocating democratic values) have historically supported the free flow of data across borders. It is perceived as a foundation for both economic freedom and protection of basic human rights. On the other hand, and especially in recent times, more countries are inclined towards implementing tighter control over data flows and the Internet infrastructure within the country. The latter narrative is often framed as the data sovereignty narrative.

While free flow of data and data sovereignty lie at the opposite ends of the spectrum, most countries are influenced by numerous, often-conflicting policy considerations and thus adopt data regulatory frameworks all along the spectrum. For example, advocates of data sovereignty may be concerned about the competitiveness of their domestic companies in global digital markets,[8] while countries advocating for the free flow of data may adopt restrictive measures to address political tensions with other digital powers.[9]

Two key forces are at play in the increasing popularity of the data sovereignty narrative. First, the increasing digitalisation of the economy and the various socioeconomic and geopolitical challenges that come with it, including dependence on certain foreign digital powers, has led to increased calls for data sovereignty, especially in fast-emerging digital economies. Second, awareness among governments that the Internet can be used as a tool of domestic control (for both right and wrong reasons) has led to more emphasis on state control over the Internet and data flows. Interestingly, the data sovereignty narrative is popular not only among authoritarian or fast-growing digital economies, but also among developed, liberal countries across the world. This section investigates how these conflicting values on data flows influence the digital economy. Section III outlines the framework of the Data Free Flow with Trust (DFFT) initiative as a potential response to this clash. The DFFT was proposed by Japan at the G20 meeting in 2019.[10] Since then, various policy bodies have explored how it may be operationalised to enable data flows.[11]

[8] See, eg X Lu, 'Is China Changing Its Thinking on Data Localization?' (*The Diplomat*, 4 June 2020) www.thediplomat.com/2020/06/is-china-changing-its-thinking-on-data-localization/.

[9] See, eg D Castro and N Cory, '"Clean Network" Initiative Risks Undermining US Digital Trade' (ITIF, 31 August 2020) www.ITIF.org/publications/2020/08/31/clean-network-initiative-risks-undermining-us-digital-trade/.

[10] Ministry of Foreign Affairs Japan, 'Speech by Prime Minister Abe at the World Economic Forum Annual Meeting' (23 January 2019) www.mofa.go.jp/ecm/ec/page4e_000973.html.

[11] Nakanishi and Hori (n 3); UK Government, 'G7 Roadmap for Cooperation on Data Free Flow with Trust' (2021); OECD, 'Fostering Cross-Border Data Flows with Trust' (2022) OECD Digital Economy Papers No 343.

Finally, section IV focuses on the key policy rationales relevant to governing data, at both the domestic and transnational levels, focusing on five policy objectives discussed in greater detail in the successive chapters of the book: data privacy; cybersecurity; governmental access to data; the data divide; and competition law. The section provides an overview of why these areas are important to global data governance. I conclude this chapter by explaining why this book adopts a multilayered, pragmatic approach to addressing the relationship between international trade law and global data governance.

II. KEY CONCEPTS

At the outset, we must understand some key concepts used consistently throughout the book. Each of these concepts are often defined or understood differently (depending, for instance, on the disciplinary tradition or the ideological leaning). Therefore, it is important to explain how the book uses each of these concepts.

A. Data and Data Flows

The very first question is what constitutes data. It is defined as 'any raw material produced by abstracting the world into categories, measures, and other representations forms – numbers, characters, symbols, images, sounds, electromagnetic waves, bits – that constitute the building block from which information and knowledge are created'.[12] The majority of data is born digital today. For the purposes of this book, therefore, data refers to digital data, referring to the data contained in data packets, encoded in 0s and 1s.[13] Certain experts have drawn a distinction between data and information, knowledge and wisdom.[14] However, for the purposes of this book, it is not necessary to draw this distinction as data refers to both the digitised content in the digital service and the data generated by users as well as processed by companies when users access different digital services, applications and websites on the Internet.

Some scholars compartmentalise data into different categories and further suggest that different types of data should be treated differently. For example, Sen classifies data into personal data (referring to individual data), company data (data shared between corporations), business data (eg digitised content

[12] R Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences* (London, Sage Publications, 2014) 1.

[13] J Mines, 'It's All 1s and 0s: How Computers Map the Physical World' (Medium, 1 March 2018) www.medium.com/@jonathanmines/its-all-1s-and-0s-how-computers-map-the-physical-world-18a361fae3a5.

[14] J Rowley, 'The Wisdom Hierarchy: Representations of the DIKW Hierarchy' (2006) 33(2) *Journal of Information Science* 163, 164.

such as software) and social data (behavioural patterns determined by using personal data).[15] Aaronson and Leblond categorise data into personal, public, confidential business, machine-to-machine, and metadata, although they do not specifically define each of these terms.[16] Usually, domestic laws safeguard personal and confidential business data more stringently than other types of anonymised or day-to-day business data.

Implementing measures that treat different categories of data differently can be quite complex in practice as data categories often overlap. One such example is the murky distinction between personal data and other types of data (eg non-personal data), especially as Big Data technologies can be used to identify individuals in anonymised (thus, non-personal) datasets.[17] Similarly, metadata combined with geolocation technologies can provide details of an individual's life with reasonable accuracy.[18] Further, personal data is often a component of business/company data such as employee records. Personal data generates business value, given that it is traded extensively via various digital services and is an important driver of the digital economy. With the rapid innovations of Big Data analytics, digital targeting is less reliant on personal data, focusing rather on group behaviours. Thus, in this book, I use the term 'data' as a broader reference to all categories of data, unless the description makes a specific reference to a particular kind of data.

The term 'data flows' refers to the transfer of data packets from one point or end device to another using the network of the Internet.[19] Data flows can take various forms. For instance, both the provision of the digital service itself (as encoded in bits and bytes) and the data generated while using a service, such as business, personal and other kinds of user-generated data, constitute data flows.[20] For the purposes of this book, we are interested in the Internet as a transmission medium for data across the world. The Internet is a multilayered medium, consisting of: a physical layer, which contains the physical infrastructure carrying data packets, including cables, satellites and ethernet; a network or Internet layer, consisting of Internet Protocol (IP), which determines the path of data packets; a transport layer, consisting of protocols that ensure the

[15] N Sen, 'Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path' (2018) 21(2) *Journal of International Economic Law* 323, 323–24.

[16] SA Aaronson and P Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO' (2018) 21(2) *Journal of International Economic Law* 245, 249–50.

[17] See generally P Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 *UCL Law Review* 1701.

[18] N Aguilar, 'You Might Be Giving Up Your Location When You Share Photos on Your iPhone' (CNET, 22 February 2023) www.CNET.com/tech/mobile/you-might-be-giving-up-your-location-when-you-share-photos-on-your-iphone/.

[19] S Sacks and J Sherman, 'Global Data Governance Concepts, Obstacles, and Prospects' (New America, 2019) 7.

[20] N Mishra, 'Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows' (2019) 52(2) *Vanderbilt Journal of Transnational Law* 463, 472.

sequencing and delivery of data packets (eg Transmission Control Protocol, TCP); and an applications layer, consisting of the programs that users see while using the Internet.[21] These different layers must be 'interoperable' to enable data flows through the Internet.[22] This definition of the Internet excludes the deep web.[23]

The Internet is an open, decentralised network grounded in the principles of 'efficiency' and 'non-discrimination'.[24] Engineers refer to this as an 'end-to-end' architecture in which 'information pushed into one end of the internet should come out the other without modification', thus ensuring seamless connectivity.[25] The Internet therefore transfers information through the most efficient route, but the routing protocols do not 'know' anything about the content of the data packets, hence 'cannot by architecture – discriminate or differentiate traffic generated by different applications'.[26] Therefore, the Internet is a 'big, fat, dumb, digital pipe',[27] with only the applications residing at the ends of the network possessing the 'intelligence' to process the data packets.[28]

Cloud computing services storing and processing data today also usually mirror the decentralised architecture of the Internet. For instance, companies often replicate data in diverse locations to enhance efficiency, minimise costs or increase security, or split it into distributed chunks while processing.[29] Thus, while governments can impose specific requirements to store data in local cloud servers, such measures often interfere with efficiency and security.

B. Cross-Border Data Flows

This book will consistently emphasise the 'cross-border' nature of data flows. This emphasis reflects the global, interconnected and instantaneous nature of data flows through the Internet, in turn obscuring the difference between cross-border and domestic data flows. Data flows are driven by protocols that determine the most efficient path for Internet traffic without consideration of geographical boundaries. In cloud computing, typically, data packets are broken down into smaller parts (in a process known as 'sharding'), which are then stored in and

[21] ibid 470.
[22] ibid 470.
[23] A Patrizio, 'Deep Web' (TechTarget) www.TechTarget.com/whatis/definition/deep-Web.
[24] CIGI and Chatam House, 'Global Commission on Internet Governance: One Internet' (2016) vi.
[25] TechTarget, 'End-to-End Principle', www.TechTarget.com/whatis/definition/end-to-end-principle#:~:text=The%20end%2Dto%2Dend%20principle,intermediate%20nodes%20pass%20data%20randomly.
[26] LB Solum, 'Models of Internet Governance' in L Bygrave and J Bing (eds), *Internet Governance: Infrastructure and Institutions* (Oxford, Oxford University Press, 2009) 48, 63–64.
[27] S Garfinkel, 'The End of End-to-End?' (2003) *MIT Technology Review* 234174.
[28] Solum (n 26) 58.
[29] Porciuncula and La Chapelle (n 4) 17.

routed through multiple servers to ensure data security.[30] Further, even if data is finally stored in one server, data transits through multiple servers across countries during routine processing.[31] Consequently, a very small portion of data flows are purely domestic in nature. Thus, regulating data flows based on territorial boundaries, such as requiring data to be stored and processed within one's borders (as is common in many domestic laws), is fundamentally opposed to the interconnected nature of the Internet.[32] New technological developments and data-driven business models have further magnified the volume of cross-border data flows.[33]

C. Data-Restrictive Measures

This book highlights several laws, regulations, rules, policies, administrative practices and any other governmental measures that directly or indirectly restrict cross-border data flows. Such measures are broadly referred to as 'data-restrictive' measures. Some simple examples of direct restrictions on Internet data flows include data localisation laws requiring storage of data on domestic servers[34] and measures blocking digital services or specific digital content.[35] Indirect restrictions on data flows usually require digital service suppliers to comply with various conditions for transferring data across borders, for instance, under domestic data protection[36] and cybersecurity laws[37] or through

[30] R Awati and J Denman, 'Sharding' (TechTarget) www.TechTarget.com/searchoracle/definition/sharding#:~:text=Sharding%20is%20a%20type%20of,small%20part%20of%20a%20whole.%22.

[31] R Sheldon and N Rando, 'Cloud Load Balancing' (TechTarget) www.TechTarget.com/searchcloudcomputing/definition/cloud-load-balancing.

[32] Sacks and Sherman (n 19) 10.

[33] Expert Group on Data Free Flow with Trust, 'Interim Report of the Expert Group on Data Free Flow with Trust' (METI, 28 February 2022) 3.

[34] See various examples in Cory and Dascoli (n 5), including Bangladesh's Draft Data Protection Act, 2020, mandating data localisation and mirroring; Indian regulations requiring financial firms to store data within India; South Korea's requirement to store public sector data physically in Korea; and Vietnam's Decree 72, 2020, requiring telecom companies and digital platforms to have local caching servers.

[35] See, eg G McDermott and A Larsson, 'The Quiet Evolution of Vietnam's Digital Authoritarianism' (The Diplomat, 19 November 2022) www.thediplomat.com/2022/11/the-quiet-evolution-of-vietnams-digital-authoritarianism/; BBC, 'TikTok and WeChat: US to Ban App Downloads in 48 hours' (18 September 2020) www.bbc.com/news/technology-54205231; S Chabba, 'Pakistan Passes Strict Social Media Regulations' (DW, 24 February 2020) www.dw.com/en/pakistans-new-internet-laws-tighten-control-over-social-media/a-52375508.

[36] See, eg J Subramanian, 'Challenges in Cross Border Data Flows and Data Localization amidst New Regulations' (SAP, 19 January 2022) https://blogs.sap.com/2022/01/19/challenges-in-cross-border-data-flows-and-data-localization-amidst-new-regulations/.

[37] See, eg TJ Treutler and GTH Tran, 'Update on the Implementation of Vietnam's New Cyber security Law and Status of Implementing Decrees' (Tilleke & Gibbins, 24 December 2019) www.tilleke.com/insights/update-implementation-vietnams-new-cybersecurity-law-and-status-implementing-decrees/; P Swire and D Kennedy-Mayo, 'Hard Data Localization May Be Coming to the EU – Here Are 5 Concerns' (IAPP, January 26 2021) www.iapp.org/news/a/hard-data-localization-may-be-coming-to-the-eu-here-are-five-concerns/.

mandatory imposition of indigenous technical standards.[38] Further, governments may require certain data to be stored within the borders of the country to enable ready access to data for regulatory supervision and law enforcement.[39] Governments may also restrict data transfer to certain jurisdictions, especially when there is a national security risk.[40]

Data-restrictive measures can potentially affect different layers of the Internet. Certain measures directly affect the physical or network layer of the Internet. For example, certain governments may exercise enormous control over the Internet Exchange Points (physical infrastructure that allows Internet traffic exchange between two networks) for various policy reasons, including preventing the circulation of banned or offensive online content.[41] Similarly, a data localisation measure requiring local routing (of sensitive data, for instance) will most likely interfere with the transfer protocols that route Internet traffic based on efficiency rather than geographic location, thereby adversely affecting the transport layer of the Internet.[42] Other restrictive measures do not directly interfere with the technical or physical infrastructure of the network but impose specific requirements on digital service suppliers, for instance, to incorporate specific privacy or security requirements in their services, to alter their terms of service or to comply with specific technical or policy requirements.[43] These measures therefore affect the applications layer of the Internet.

[38] N Cory, 'How the EU Is Using Technology Standards as a Protectionist Tool in Its Quest for Cybersovereignty' (ITIF, 19 September 2022) www.ITIF.org/publications/2022/09/19/how-the-eu-is-using-technology-standards-as-a-protectionist-tool/.

[39] For example, Indonesia's Ministry of Communication and Informatics Regulation No 5 of 2020 requires electronic system organisers to take down content flagged by the government within 24 hours or, in urgent cases, within four hours. Further, electronic system organisers must give law enforcement agencies access to their electronic system and electronic data if requested, effectively requiring companies to localise data. See RO Manurung et al, 'New Regulation on Electronic System Organizers in the Private Sector' (Makarim & Taira S, January 2021) makarim.com/storage/uploads/7b6937fc-15ba-41ab-a8ba-96f29d9c746c/583428_Jan-2021---New-Regulation-on-Electronic-System-Organizers-in-the-Private-Sector-(final).pdf.

[40] In the USA, the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) requires taking into account control over sensitive personal data in the review of a foreign investment. US lawmakers have also proposed introducing export licensing for bulk exports of personal data to certain high-risk countries. See Title XVII – Review of Foreign Investment and Export Controls (FIRRMA) [2018] HR 5515–38.

[41] N Sonnad and K Collins, 'How Countries Like China and Russia Are Able to Control the Internet' (Quartz, 05 October 2016) www.qz.com/780675/how-do-internet-censorship-and-surveillance-actually-work.

[42] Internet Society, 'Internet Way of Networking Use Case: Data Localization' (20 September 2020) www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-data-localization/.

[43] See, eg S Saraf, '7 Countries Unite to Push for Secure-by-Design Requirement' (CSO, 17 April 2023) www.csoonline.com/article/575051/7-countries-unite-to-push-for-secure-by-design-development.html; A Robinson, 'Government to Strengthen UK Data Protection Law' (UK Safety Internet Centre, 14 August 2017) saferinternet.org.uk/blog/government-to-strengthen-uk-data-protection-law; S Livingstone, 'To Be 13 or 16, That Is the Question' (LSE Blogs, 23 November 2016) blogs.lse.ac.uk/parenting4digitalfuture/2016/11/23/to-be-13-or-16-that-is-the-question/.

Data localisation is one of the most commonly used data-restrictive measures.[44] It can be understood as any measure 'that specifically encumber(s) the transfer of data across national borders', thus including both de jure and de facto measures.[45] The European Commission previously defined data localisation as

> any obligation, prohibition, condition, limit or other requirement … [contained in the] laws, regulations or administrative provisions of the Member States, which imposes the location of data storage or other processing requirements in the territory of a specific Member State or hinders storage or other processing of data in any other Member State.[46]

Data localisation thus involves some or all of these elements: requirement to store and/or process data locally; route data through domestic servers; and prevent foreign cloud computing companies from offering certain data services or compel them to form joint ventures with local partners.

D. Global Data Governance

The terms 'data governance' and 'global data governance' can be construed in various ways. The World Bank defines data governance as norms, infrastructure policies, laws and regulations for data, related economic policies and institutions that can effectively enable the safe, trustworthy use of various types of data.[47] It consists of four main tasks: strategic planning; developing rules and standards; developing mechanisms of compliance and enforcement; and generating the learning and evidence needed to gain insights and address emerging challenges.[48] This definition offers a very comprehensive account of data governance.[49]

[44] A report by McKinsey in 2022 stated that at least 75% of countries have implemented data localisation measures. See S Parekh et al, 'Localization of Data Privacy Regulations Creates Competitive Opportunities' (McKinsey & Co, 30 June 2022) www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities?cid=other-soc----oth---&sid=9075025049&linkId=203901147#/. See also various examples discussed in AD Mitchell and J Hepburn, 'Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer' (2017) 19 *Yale Journal of Law and Technology* 182, 188–94.

[45] A Chander and UP Lê, 'Data Nationalism' (2015) 64(3) *Emory Law Journal* 677, 680.

[46] European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Framework for the Free Flow of Non-Personal Data in the European Union (COD 2017/0228), Art 3(5).

[47] World Bank (n 3) 10.

[48] ibid 265.

[49] Global governance itself can also be quite broad, and scholars have defined it as the 'sum of the informal and formal values, norms, procedures and institutions that help states, intergovernmental organisations, civil society, transnational corporations identify, understand and address transboundary problems'. See generally A Berman et al (eds), *Rethinking Participation in Global Governance* (Oxford, Oxford University Press, 2022) 4, citing TG Weiss, *Global Governance, Why? What? When?* (Cambridge, Polity Press, 2013).

The Digital Trade and Data Governance Hub (a scholarly network based at George Washington University) defines data governance as any norms, principles and rules governing various types of data.[50] Another definition, offered by Aaronson, is 'principles, policies, standards, laws, regulations and agreements designed to control, manage, share, protect and extract value from various types of data'.[51] The Datasphere Initiative (a multistakeholder network discussing issues of data governance and its impact on human lives) defines data governance as the 'development and implementation of policies, standards, laws, regulations, and agreements that cover the management of data within countries and transfer of data across jurisdictional boundaries'.[52] This is similar to the definition offered by Erie and Streinz, who define data governance as 'rules, norms, practices, and infrastructures governing the collection, storage, transfer, use of, and access to digitalized information'.[53]

For this book, the term 'data governance' refers to different norms, best practices, and laws and regulations shaping both the regulation of data flows and the digital economy that thrives on them. The reason why the term 'global' is appended is because the governance of data is dispersed across various entities globally, including governments, intergovernmental organisations, multistakeholder bodies, private standard-setting organisations, and co-regulatory and transnational networks/institutions regulating different aspects of data flows.[54] It is perhaps unsurprising that the majority of organisations leading discussions and managing different aspects of global data governance are located in the developed world.[55]

In summary, data is governed not only by domestic laws and regulations (implemented by states), but also by several other instruments and initiatives led by non-state entities or global organisations. While the main aspect of global data governance covered in this book is the governmental regulation of cross-border data flows, several references are also made to relevant (often legally non-binding) transnational or international instruments. Although most binding requirements on data flows are typically contained in domestic laws and policies, their effect is often felt beyond domestic borders, thus also justifying the use of 'global' in the context of data governance.[56]

[50] Digital Trade & Data Governance Hub, 'FAQ', www.datagovhub.elliott.gwu.edu/faq/.

[51] SA Aaronson, 'Data Is Disruptive: How Data Sovereignty Is Challenging Data Governance' (Hinrich Foundation, 03 August 2022) 6.

[52] Datasphere Initiative, 'Datasphere Governance Atlas' (2022) 11.

[53] MS Erie and T Streinz, 'The Beijing Effect: China's Digital Silk Road as Transnational Data Governance' (2021) 54(1) *New York University Journal of International Law and Politics* 1, 11.

[54] ibid 13; Sacks and Sherman (n 19) 9. See generally Berman et al (n 49) 22, wherein global governance is defined as covering governance by treaties, transnational regulatory frameworks, multistakeholder bodies and private bodies.

[55] Datasphere Initiative (n 52) 12.

[56] Erie and Streinz (n 53) 13.

For the purposes of this book, the term 'data governance' excludes day-to-day management of data practices by corporations and other private stakeholders, such as through internal corporate codes and industry best practices.[57] Further, this book does not delve into specific questions regarding the physical infrastructure, such as the development and management of physical data infrastructure. Nonetheless, the control of data flows is intrinsically linked to who owns and manages the infrastructure hosting and carrying the data.[58]

E. Digital Trade

To date, no international treaty has specifically defined the term 'digital trade', including more recent trade agreements that contain a chapter specifically dedicated to digital trade. Nonetheless, trade treaties increasingly use the term 'digital trade'.[59] The Organisation for Economic Cooperation and Development (OECD) defines digital trade as 'digitally enabled transactions of trade in goods and services that can either be digitally or physically delivered, and that involve consumers, firms, and governments'.[60] The United States International Trade Commission defines digital trade as 'US domestic commerce and international trade in which the Internet and Internet-based technologies play a particularly significant role in ordering, producing, or delivering products and services'.[61]

The Work Programme on Electronic Commerce at the World Trade Organization (WTO) defined electronic commerce as 'the production, distribution, marketing, sale or delivery of goods and services by electronic means'.[62] Experts consider this definition to be too narrow and not encompassing the important role of digital and data flows in the economy today.[63] In my past

[57] See, eg B Petzold et al, 'Designing Data Governance that Delivers Value' (*McKinsey Digital*, 26 June 2020) www.mckinsey.com/capabilities/mckinsey-digital/our-insights/designing-data-governance-that-delivers-value.

[58] EIT Digital, 'European Digital Infrastructure and Data Sovereignty: A Policy Perspective' (2020) 7, www.eitdigital.eu/fileadmin/files/2020/publications/data-sovereignty/EIT-Digital-Data-Sovereignty-Summary-Report.pdf.

[59] M Burri and A Chander, 'What Are Digital Trade and Digital Trade Law?' (2023) 117 *AJIL Unbound* 99, 100.

[60] OECD, 'The Impact of Digitalisation on Trade', www.oecd.org/trade/topics/digital-trade/#:~:text=What%20is%20digital%20trade%3F,consumers%2C%20firms%2C%20and%20governments.

[61] J Horowitz, 'US International Trade Commission's Digital Trade Roundtable: Discussion Summary' (2015) 4 *Journal of International Commerce and Economics* 1, 2.

[62] WTO, 'Electronic Commerce' (2017) www.wto.org/english/thewto_e/minist_e/mc11_e/briefing_notes_e/bfecom_e.htm.

[63] M Burri, 'Designing Future-Oriented Multilateral Rules for Digital Trade' in P Sauvé and M Roy (eds), *Research Handbook on Trade in Services* (Cheltenham, Edward Elgar, 2016) 331; M Smeets, *Adapting to the Digital Trade Era: Challenges and Opportunities* (WTO, 2021) 6.

work, I have sometimes used the terms 'e-commerce' and 'digital trade' interchangeably.[64] However, for the purposes of this book, I consciously use the term 'digital trade' in referring to the broader context of the digital economy, including trade in data itself. Since the book focuses on cross-border data flows, the most important component of digital trade that it looks at is trade in digital and data-driven services.

F. International Trade Law

International trade law comprises rules governing cross-border trade between countries, developed through negotiated agreements at the WTO and through a network of preferential trade agreements (PTAs) (referring to trade agreements consisting of two parties or more but not multilateral in nature). Some of the key areas covered under WTO agreements are trade in goods, trade in services, and intellectual property rights. This book refers to both relevant rules in both WTO treaties, particularly the General Agreement on Trade in Services (GATS)[65] and electronic commerce or digital trade chapters in PTAs. Further, the book contains references to provisions in digital-only agreements (referred to as digital economy agreements, or DEAs).[66] While the book highlights several examples of PTAs and DEAs, it does not aim to be an exhaustive comparative study of PTAs, but rather uses representative examples to highlight broader trends in international trade law.

For understanding how international trade law is relevant to cross-border data flows, the most important WTO disciplines are contained in GATS. For instance, data-restrictive measures restrict the transfer of data (or intangible components consisting of bits and bytes) across borders and thereby affect the supply of several digital services that rely on digital data flows to enable their efficient functioning. Based on the above discussion, most Internet-driven digital services will be covered by GATS. This is because data-restrictive measures are primarily aimed at blocking the intangible bits and bytes, which either form part of a service or are generated/processed during the supply of a digital service such as a website, subscription software or application.

However, other trade treaties can also be relevant in examining measures affecting cross-border data flows. For example, blocking an Internet platform

[64] AD Mitchell and N Mishra, 'Data at the Docks: Modernizing International Trade Law for the Digital Economy' (2020) 20(4) *Vanderbilt Journal of Entertainment and Technology Law* 1073, 1076.

[65] General Agreement on Trade in Services (Marrakesh, April 1994) (GATS).

[66] See, eg Digital Economy Partnership Agreement (12 June 2020) (DEPA); Singapore–Australia Digital Economy Agreement (Adelaide and Singapore, 06 August 2020) (SADEA); UK–Singapore Digital Economy Agreement (Singapore, 25 February 2022) (UKSDEA); Korea–Singapore Digital Partnership Agreement (Singapore, 21 November 2022) (KSDPA); etc.

selling physical goods affects not only the platform (a service), but also the goods traded using the service (eg shoes or watches). The sale of goods on an Internet platform could be examined, for instance, under the General Agreement on Tariff and Trade (GATT),[67] while the distribution services provided by the Internet platform would be examined under GATS.[68] Similarly, measures related to source code disclosure can also implicate rules on trade secrets contained in the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).[69] While the book makes occasional references to different types of disciplines in trade treaties, the predominant focus remains on rules applying to trade in digital services and digital trade contained in GATS and several PTAs respectively.

More recently, scholars have started referring to rules dedicated to digital trade or electronic commerce as 'digital trade law'.[70] As discussed earlier, such rules are typically contained in PTAs with chapters dedicated specifically to electronic commerce-related trade (or sometimes as a part of the chapter on trade in services). Further, DEAs contain rules specifically dedicated to trade and related issues of the digital economy. Particularly in the context of DEAs, the term 'digital trade law' is arguably more apt than international trade law, given that these agreements are specifically designed to avoid the trade-offs between negotiating different areas of cross-border trade. However, this book uses the term 'international trade law' more frequently than 'digital trade law' because the majority of countries still rely upon the traditional multilateral and plurilateral framework of international trade agreements to conduct digital trade. However, with rapid policy developments, including the negotiation of digital-only agreements, 'digital trade law' may become a more suitable characterisation of this specific field in the future.

At first sight, the worlds of international trade law and data governance may seem disconnected and divergent from each other. Yet, as the brief discussion above indicates, with the widespread digitalisation of the economy, the regulation of data flows is central to international trade law. This is despite regulatory frameworks for trade and data governance being quite distinct from each other. Expectedly, most ongoing trade policy discussions and negotiations focus on critical aspects of global data governance, thus creating the need to understand

[67] General Agreement on Tariffs and Trade (Marrakesh, April 1994) (GATT).

[68] It is outside the scope of this book to delve into the larger debate on the distinction between goods and services. See I Willemyns, *Digital Services in International Trade Law* (Cambridge, Cambridge University Press, 2021) 117–178.

[69] Agreement on Trade-Related Aspects of Intellectual Property Rights, Annex 1C of Marrakesh Agreement Establishing the World Trade Organization (Marrakesh, 15 April 1994) (TRIPS); See generally K Irion, 'Algorithms Off-limits?: If Digital Trade Law Restricts Access to Source Code of Software then Accountability Will Suffer' in *FAccT' 22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (New York, Association for Computing Machinery, 2022) 1561; N Mishra, 'International Trade Law Meets Data Ethics: A Brave New World' (2021) 53(2) *International Law and Politics* 303, 345–65.

[70] See, eg Burri and Chander (n 59).

the divergences and synergies between the two areas of regulation. At the same time, global data governance is fast evolving into a complex area of both domestic and transnational regulation. Thus, it is both timely and relevant to explore these different interfaces of international trade law and global data governance.

III. FREE FLOW OF DATA VERSUS DATA SOVEREIGNTY

The imbalance of economic and political power among countries (and stakeholder groups within those countries) in the global data governance framework leads to a deep regulatory divide as to how cross-border data flows must be regulated.[71] This section first presents two competing visions for the governance of cross-border data flows – data sovereignty versus free flow of data – and then presents the DFFT framework, which can be arguably viewed as a negotiated compromise between these competing visions.

A. Data Sovereignty versus Free Flow of Data

The tussle between the ability of governments to regulate data flows and the need for an interconnected and open Internet lies at the heart of tensions in global data governance and, consequently, influences how different countries perceive the role of international trade law in the regulation of cross-border data flows. The subsequent chapters provide more detail, through various examples, as to how governments operationalise data sovereignty in practice through different kinds of data-restrictive measures. The main aim of this section is to highlight the high-level, philosophical conflict between the idea of a free and open Internet (characterised by the free flow of data) and a regulated Internet (characterised by state-driven ideas of data sovereignty). This tension can shape how governments design and implement laws, as well as how they cooperate among themselves to develop regional or global frameworks on digital trade.

Data sovereignty is a vague term.[72] As Chander and Sun argue, data sovereignty can be a 'double-edged sword': while it can be used safeguard important public interests such as privacy and data security, it can equally be used to repress and control citizens.[73] In the context of regulating data flows,[74] data sovereignty broadly refers to the ability of governments to control how data is collected,

[71] J Mwangi, 'Contesting Digital Colonialism Narratives in Africa and Their Framing Effects' in PG Sampath and F Tregenna (eds), *Digital Sovereignty: African Perspectives* (Capetown, Zenodo, 2022) 75.

[72] Porciuncula and La Chapelle (n 4) 3; P Hummel et al, 'Data Sovereignty: A Review' (2021) 8(1) *Big Data & Society* 1.

[73] A Chander and H Sun, 'Sovereignty 2.0' (2023) 55(2) *Vanderbilt Journal of International Law* 283, 311.

[74] Data sovereignty also applies in other contexts; for instance, it can relate to management and development of data infrastructure and controlling the quality and accuracy of domestic data.

stored, processed and transferred in and out of borders of the country. Christakis and Aaronson specifically relate data sovereignty to the application of domestic laws, regulations and procedures to data originating within a country.[75]

Several developing countries have equated data sovereignty to the ability of governments to decide who derives economic value from domestic data.[76] These countries thus focus on implementing laws to allow hoarding and controlling of data within the borders of the country, thereby gaining some form of competitive advantage.[77] While some countries frame data sovereignty as a response to the ruthless extraction of economic benefits of data by Western powers,[78] others focus on shifting power from huge digital platforms to governments to facilitate stronger governmental control over data.[79] Data sovereignty is also often seen as an urgent necessity because of the weaponisation of digital networks and data infrastructure (thus linking data to national security)[80] resulting from the excessive dependence on a few foreign digital powers such as the USA and China.[81]

The widespread implementation of data sovereignty increases the possibility of regulatory fragmentation across countries. For instance, if countries adopt conflicting legal standards in their domestic laws to regulate data processing, storage or cross-border transfers, this increases the scope for regulatory fragmentation.[82] Similarly, as I argue later in the book, meaningful international regulatory cooperation on global data governance becomes harder to achieve when countries adopt stringent data sovereignty models. O'Hara and Hall argue that wide variations in Internet regulatory models could lead to 'four internets' (referring to the EU, USA, China and Russia).[83] Others, however, argue that

[75] T Christakis, 'European Digital Sovereignty: Successfully Navigating between the "Brussels Effect" and Europe's Quest for Strategic Autonomy' (2020); SA Aaronson, 'The Difficult Past and Troubled Future of Digital Protectionism' in I Borchert and LA Winters (eds), *Addressing Impediments to Digital Trade* (London, CEPR, 2021) 141.

[76] See generally PG Sampath and F Tregenna, 'Digital Sovereignty in Africa: An Introduction' in Sampath and Tregenna, *Digital Sovereignty* (n 71) 7.

[77] A Basu, 'Sovereignty in a "Datafied' World" (ORF, 18 October 2021) www.staging.orfonline.org/research/sovereignty-in-a-datafied-world/; Aaronson, 'Data is Disruptive' (n 51); See also P Hebbar, 'The One Who Controls Data, Will Be the World Leader, Says PM Modi at World Economic Forum' (AIM, 24 January 2018) www.analyticsindiamag.com/modi-wef-davos-data-control-real-wealth/. In this narrative, however, data sovereignty can also be seen as a rights narrative, ie developing countries have a right to manage their own data. See Hummel et al (n 72) 1–2. Similar ideas are reflected in the narrative of indigenous data sovereignty.

[78] Aaronson, 'Data is Disruptive' (n 51); Mwangi (n 71) 72.

[79] Aaronson, 'Data is Disruptive' (n 51) 20.

[80] See generally Y Nugraha et al, 'Towards Data Sovereignty in Cyberspace' (3rd International Conference on Information and Communication Technology, Nusa Dua, Bali, Indonesia, 2015) 465–71.

[81] H Farrell and AL Newman, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion' (2019) 44(1) *International Security* 42.

[82] See generally R Matthan, 'A World Fragmented by Divergences in Data Regulation' (*Mint*, 1 March 2022) www.livemint.com/opinion/columns/a-world-fragmented-by-divergences-in-data-regulation-11646153126442.html; WEF (n 3) 3–6.

[83] K O'Hara and W Hall, *Four Internets: Data, Geopolitics and the Governance of Cyberspace* (New York, Oxford University Press, 2021).

regulatory fragmentation does not automatically lead to the technical fragmentation of the Internet.[84]

Several countries have also used the terms 'digital sovereignty' and 'cyber-sovereignty' as a part of their broader policy vision. The meaning assigned to each of these terms can overlap with the idea of data sovereignty, although there are some differences as well.[85] The term 'digital sovereignty' usually refers to the ability of governments to control the infrastructure where data is stored and make independent choices regarding their digital systems and infrastructure.[86] For instance, in Australia, digital sovereignty is equated to a 'legitimate form of strategic autonomy'.[87] Similarly, in the EU, digital sovereignty is seen as being fundamental to protecting core values, making free choices and ensuring that all the data of Europeans is treated consistently with European laws and regulations.[88] However, as Yakovleva argues, the idea of digital sovereignty within the EU also entails mobilising industrial data to create a strong regional economic market.[89] Cory argues that the EU has strengthened its digital sovereignty standards by deliberately excluding technical experts from foreign countries, especially the USA, from its standard-setting bodies.[90] Therefore, the distinction between digital sovereignty and protectionism can be murky in practice.[91]

The term 'cyber-sovereignty' refers to the ability/vision of governments to control the cyberspace within the borders of the country, with regard to, for example, the kind of content available, access to that content, and what information can flow in and out of the borders.[92] Perhaps, the most famous articulation of this concept is Chinese President Xi's speech in 2015, in which he asserted that cyber-sovereignty is essential for each country to choose how to develop and regulate the Internet.[93] The idea of cyber-sovereignty is often strongly

[84] 'IGF 2022 – Day 0 – Caucus Room 11 – Understanding Internet Fragmentation Concepts' (*YouTube*, 29 November 2022) www.youtube.com/watch?v=cdU7s8i1Okg&t=263s (reference to comments of Bill Drake).

[85] In this context, Chander and Sun (n 73) argue that demarcating the digital from data is practically impossible.

[86] Federal Ministry of Economic Affairs and Energy, 'Project GAIA-X: A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem' (2019) 3; J Pohle and T Thiel, 'Digital Sovereignty' (2020) 9(4) *Internet Policy Review* 2.

[87] AD Mitchell and T Samlidis, 'Cloud Services and Government Digital Sovereignty in Australia and Beyond' (2021) 29(4) *International Journal of Law and Information Technology* 364, 376.

[88] S Yakovleva, 'On Digital Sovereignty, New European Data Rules, and the Future of Free Data Flows' (2022) 49(4) *Legal Issues of Economic Integration* 339, 339–40; Hummel et al (n 72) 6.

[89] Yakovleva (n 88) 339, 341.

[90] Cory (n 38).

[91] As Aaronson argues, there is no consensus on what constitutes digital protectionism. However, the USTR has taken the position that laws and regulations that impede the flow of data across borders and restrict the ability of firms to offer their services globally constitute digital protectionism. See generally Aaronson, 'The Difficult Past' (n 75).

[92] M Palaniappan, 'Cyber Sovereignty: In Search of Definitions, Exploring Implications' (Observer Research Foundation, 28 December 2022) www.orfonline.org/research/cyber-sovereignty/.

[93] See also Xinhua, 'International Strategy of Cooperation on Cyberspace' (2017) www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm.

interlinked with national security.[94] Ultimately, irrespective of how different governments frame dialogues on sovereignty in the digital world (and whether this term is used pejoratively or not),[95] the usual outcome has been guarded and stringent regulation of cross-border data flows.

In contrast to the above narrative, free flow of data has often been portrayed as a value aligned with the vision of a globally interconnected world.[96] Experts offer several reasons for facilitating the free flow of data: reducing digital trade barriers, promoting economic freedom and efficiency, and checking illegal government surveillance.[97] The idea of free flow of data is particularly associated with the liberalisation of the economy. Farrell and Newman argue that the digital domain is undergoing a perceptible shift, wherein the free flow of data and an open and interoperable Internet are no longer seen as useful economic and political devices.[98] However, several initiatives from both within and outside trade bodies seem to indicate otherwise.

To date, the most consolidated efforts to develop international norms on data transfers have been through international trade law.[99] For instance, several recent PTAs, especially following the example of the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP),[100] have incorporated provisions requiring parties to allow cross-border data flows for digital trade and prohibiting data localisation.[101] A dataset developed by researchers at the University of Lucerne[102] indicates that at least 22 PTAs contain binding provisions on cross-border data flows, while 45 contain at least some kind of provisions on cross-border data flows; similarly, 25 PTAs contain binding provisions prohibiting data localisation.

[94] Palaniappan (n 91).

[95] See generally Mitchell and Samlidis (n 87) 366.

[96] 'Secretary Hillary Clinton's Internet Freedom Speech at GW' (*YouTube*, 16 February 2011) www.youtube.com/watch?v=acDcUQoeFxY.

[97] L Chen et al, 'The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies' (T20 Japan, 29 March 2019) www.t20japan.org/policy-brief-digital-economy-economic-development/.

[98] H Farrell and AL Newman, 'The Janus Face of the Liberal International Information Order: When Global Institutions Are Self–Undermining (2021) 75(2) *International Organisation* 333, 334; See also D Ciuriak, 'Unfree Flow with No Trust: The Implications of Geoeconomics and Geopolitics for Data and Digital Trade' (CIGI, 14 February 2022) www.cigionline.org/articles/unfree-flow-with-no-trust-the-implications-of-geoeconomics-and-geopolitics-for-data-and-digital-trade/ (arguing that data flows are informed by the geoeconomics and geopolitics of the modern digital age).

[99] See, eg S Azmeh et al, 'The International Trade Regime and the Quest for Free Digital Trade' (2019) 22(3) *International Studies Review* 671.

[100] Comprehensive and Progressive Agreement for Trans-Pacific Partnership (Santiago, 2018).

[101] Contrary to popular perception, the first PTA to contain binding disciplines on data flows and data localisation was the 2014 Mexico–Panama FTA (not the CPTPP). See M Burri, 'Creating Data Flow Rules through Preferential Trade Agreements' in A Chander and H Sun (eds), *Data Sovereignty along the Digital Silk Road* (Oxford University Press, forthcoming) (copy on file with the author).

[102] University of Lucerne, 'TAPED – A New Dataset on Data-related Trade Provisions', www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-director-internationalisation/research/taped/.

The narrative on the free flow of data is, however, also premised on other human rights concerns and the concomitant public benefits from the free movement of data. Several international instruments, for instance, recognise the importance of the free flow of data in protecting various human rights, such as freedom of expression and access to information.[103] The value of an open Internet has been recognised in several international/regional declarations.[104] A declaration initiated by the USA and several of its allies in 2022 called the 'A Declaration of the Future of the Internet' stated the importance of an 'open, free, global and interoperable' Internet to protect various human rights online and enable meaningful innovation.[105]

While the free flow of data still enjoys a high degree of support, especially among liberal democracies, there are various reasons why several governments fear the idea of the free flow of data. First, several governments are concerned about how the data of their citizens may be treated outside the country, where they exercise no control. Second, governments are concerned about fiscal revenue losses arising due to loss of control over data flows. Third, governments are increasingly worried about national security implications of cross-border data flows (whether real or perceived). Additionally, there is a fear that without appropriate data-restrictive measures, foreign digital giants will dominate the local economy.[106] Further, scholars have pointed out that removing trade barriers to data flows without addressing other problems, such as the data divide, may lead to social conflict within certain countries.[107]

B. DFFT as a Middle Path

The idea of DFFT was proposed by Japan in the G20 meeting in 2019. The underlying premise was that although cross-border data flows had obvious social and economic benefits, they could only be facilitated if there was sufficient 'trust' among countries. For instance, data protection, cross-jurisdictional data access,

[103] See Tunis Agenda for The Information Society (Tunis, ITU, 18 November 2005) WSIS-05/TUNIS/DOC/6(Rev. 1)-E; ITU, 'Declaration of Principles – Building the Information Society: A Global Challenge in the New Millennium' (12 December 2003) WSIS03/GENEVA/DOC/4-E. Free flow of information is recognised as a human right in many treaties. See UNGA Res 2200A(XXI) 'International Covenant on Civil and Political Rights' (16 December 1966), Art 19 (ICCPR); UNGA Res 217A(III) 'Universal Declaration of Human Rights' (10 December 1948), Art 19 (UDHR) (although not binding, some scholars recognise it as customary international law).

[104] See Mishra, 'Building Bridges' (n 20) 478–83.

[105] The White House, 'A Declaration for the Future of the Internet' (2022).

[106] These ideas are borrowed from the speech by Minister CC Sing: 'Can Digital Trade Agreements Spur the Next Round of Growth?' (PIIE, 16 September 2020) www.piie.com/events/can-digital-trade-agreements-spur-next-round-growth.

[107] See, eg ED Mansfield and N Rudra, 'Embedded Liberalism in the Digital Era' (2021) 75(2) *International Organization* 558 (focusing on the impact on labour and social welfare due to widespread digitalisation); Shaffer (n 3) 259.

intellectual property and data security were seen as being central to generating such trust for cross-border data flows.[108] Therefore, the Japanese government proposed that G20 members explore concrete mechanisms to develop such trust. The DFFT framework was seen as midway between the idea of data sovereignty and the free flow of data, thereby trying to set a balanced discourse for the regulation of cross-border data flows.[109]

While this framework appears vague at first sight, its flexibility provides an inherent advantage in dealing with several of the existing legal and policy uncertainties in global data governance and digital trade. As per the proposal put forth by the Japanese government, the DFFT initiative is aimed at combining the trade track (eg provisions on cross-border data flows and data localisation enshrined in PTAs) with a regulatory track, focusing on frameworks necessary to build trust mechanisms for digital trade.[110] The Japanese government has also proposed the institution of a multistakeholder body called the Institutional Arrangement for Partnership to operationalise this framework, although the specific details are yet to be decided.[111]

The multidimensional nature of the DFFT framework is evident in the ongoing policy discussions. For example, the Japanese government and certain bodies such as the G7 have indicated that the OECD initiative on government access to data (discussed in chapter four) and existing mutual recognition mechanisms for personal data transfer (discussed in chapter two) could be important for implementing the DFFT framework.[112] The development of the DFFT is unlikely to occur through a single forum. For instance, in addition to treaties, parties may also need to look at other non-binding policy fora to develop mechanisms for data transfers, such as certification mechanisms or codes of conduct. One such example is the initiation of the Global Cross-Border Privacy Rules Forum by seven economies of the Asia-Pacific Economic Cooperation (APEC): USA, Canada, Japan, Korea, Philippines, Singapore and China.[113] This initiative is aimed at building upon and updating the data certification system developed in APEC and extending it beyond countries in the Asia-Pacific (discussed further in chapter two).

[108] Expert Group on Data Free Flow with Trust (n 33) 3.

[109] As regards the importance of discourse in the regulation of data, see S Yakovleva, 'Governing Cross-border Data Flows: Reconciling EU Data Protection and International Trade Law' (PhD thesis, University of Amsterdam 2021) 74.

[110] A Arasasingham and M Goodman, 'Operationalizing Data Free Flow with Trust (DFFT)' (CSIS, April 2023) 3.

[111] G7 Digital and Tech Ministers' Meeting, 'G7 Digital and Tech Track Annex – 1: Annex on G7 Vision for Operationalising DFFT and Its Priorities' (Takasaki, 30 April 2023).

[112] ibid; Expert Group on Data Free Flow with Trust (n 33) 4–5.

[113] Global Cross-Border Privacy Rules Declaration (21 April 2022).

IV. THE DIGITAL TRADE–GLOBAL DATA GOVERNANCE INTERFACE

Cross-border data flows drive the modern-day digital economy, and certain estimates indicate that such flows grew 45 times between 2005 and 2016.[114] Data flows occur even in the most routine Internet transactions, such as accessing websites, using applications on smart devices and surfing the Internet.[115] Cross-border data flows facilitate various processes and business activities in the global supply chain and are intrinsic to the supply of all digital services. For example, using a digital platform involves complex flows between servers of different services (eg e-payment services, the e-commerce portal) and the customer's device.

While cross-border data flows have various economic benefits and facilitate global trade, governments nevertheless have reasons to still regulate them. The following subsection identifies five important policy objectives driving cross-border data regulation and how such regulations impact digital trade. It also briefly explains why the book focuses on these five areas of data regulation. The subsection concludes by highlighting why the book proposes a dynamic and multilayered approach to achieve stronger alignment between international trade rules and global data governance.

A. Why Governments Regulate Cross-Border Data Flows

As previously noted, governments regulate cross-border data flows for various reasons. This book covers five aspects of global data governance that also affect digital trade: privacy and data protection; cybersecurity; governmental access to data; bridging the data divide; and competition law. This subsection explains the rationale behind focusing on each of these areas and also outlines the key structure of the book in the next six chapters.

The impact of the majority of domestic data-related laws, regulations and policies is often transnational or even global.[116] This extra-territorial impact could be intentional or unintentional. For instance, even if a particular data-restrictive measure may be contained in a domestic data protection law, eg obtaining prior approval of the regulator to transfer certain categories of sensitive personal data, it can have a detrimental impact on service providers (both domestic and foreign) transferring such data for routine business purposes. A different example is the influence of the adequacy framework under the EU's General Data Protection Regulation on various jurisdictions outside of the EU (chapter two). Another example is governmental access to cross-border data,

[114] J Manyika et al, 'Digital Globalization: The New Era of Global Flows' (McKinsey Global Institute, March 2016) 30.
[115] Sen (n 15) 324.
[116] See definition of global data governance in s IIC.

which often raises questions of extra-territorial jurisdiction over cloud computing services and service providers, especially for companies with global business models (see chapter four).

A key reason why governments regulate cross-border data flows is privacy and data protection. With the increase in the ability of both governments and the private sector to conduct surveillance simply by collecting and analysing personal data, privacy has become a central issue in global data governance. It is not only recognised as a fundamental human right in several international instruments, but also embedded in the constitutions of several countries.[117] As per the United Nations Conference on Trade and Development (UNCTAD), about 71 per cent of countries in the world have adopted data protection laws.[118]

Chapter two explores the complex interface of international trade law and privacy. Although they seem to be conflicting regulatory agendas at first sight, this chapter argues that there are several ways in which international trade law and privacy/data protection law can go together. After examining why certain data-restrictive measures contained in data protection laws violate international trade law, the chapter explores avenues for aligning the two fields of regulation. For instance, the chapter proposes how trade tribunals can interpret and apply existing exceptions contained in trade treaties more meaningfully in assessing such measures; increasing flexibilities in trade treaties for incorporating transnational/multistakeholder norms, standards and best practices on data protection by reference; and providing more scope to companies engaging in digital trade to use evolving transnational mechanisms for enabling personal data transfers.

Another important reason why governments regulate cross-border data flows is cybersecurity. However, the meaning of cybersecurity is evolving in both domestic and global data governance to cover multiple dimensions of technical, economic and political security. Chapter three covers the interface of international trade law and the ever-expanding concept of cybersecurity as contained in various domestic laws and regulations that have the effect of restricting cross-border data flows. At the same time, robust cybersecurity regulation and standard setting have become extremely important from a transnational perspective, especially in the context of digital trade. The chapter explores this interface between the two worlds by examining how rules contained in international trade agreements apply to cybersecurity-related data-restrictive measures.

While several domestic cybersecurity measures are likely to violate obligations contained in trade agreements, most countries are likely to justify these measures under existing exceptions contained in those treaties. In particular, as cybersecurity is increasingly linked to national security concerns, the security exception contained in trade agreements has become relevant. The widespread use of security exceptions, however, raises many sensitive concerns around data sovereignty

[117] Mishra, 'Building Bridges' (n 20) 489–93.

[118] UNCTAD, 'Data Protection and Privacy Legislation Worldwide', www.unctad.org/page/data-protection-and-privacy-legislation-worldwide.

and geopolitical dynamics between countries. Further, new-generation PTAs provide little scope to develop international consensus on cybersecurity issues. Chapter three thus provides new ideas for aligning international trade law and domestic cybersecurity regulation, including better processes for notification and discussion of cybersecurity measures in WTO committees and other trade bodies, and an expanded scope for considering multistakeholder cybersecurity norms in implementing digital trade rules. It also argues for the development of a clear mechanism for technical standard setting in the context of digital and data-driven services, including referring to relevant private, multistakeholder and transnational cybersecurity standards.

As our lives have become digital, access to data has become an important tool for governments to regulate/audit companies as well as to conduct law enforcement activities. Chapter four examines various tools deployed by governments to facilitate access to data through different laws and regulations for the purposes of both regulatory supervision/audit and law enforcement (termed 'data access measures'). It examines why data access measures may prejudice cross-border data flows and then examines better ways of addressing the interface between digital trade and governmental access to data. International trade law has so far largely remained silent on the relationship between trade rules and governmental access to data. This is unsurprising, given that the majority of countries seek solutions to these problems through bilateral treaties or other political mechanisms. Nonetheless, the rapid increase in data access measures, particularly data localisation, can hamper digital trade and compromise digital trust.

Chapter four, therefore, proposes certain reforms in international trade law to address the growing rise of data access measures and its detrimental impact on digital trade. First, it argues that countries negotiating digital trade agreements may consider signing up to high-level normative frameworks on data access developed at various non-trade bodies, such as the OECD and the Global Privacy Assembly, and other international treaties, such as the Budapest Convention, as a parallel initiative. Second, relevant provisions in trade treaties must explicitly acknowledge that regulators have legitimate grounds for requesting access to certain data. Finally, where data access measures result in trade disputes, trade tribunals must be able to consider evolving norms on data access in relevant international treaties and possibly even multistakeholder policy frameworks.

While there are several economic and social benefits of cross-border data flows, the benefits of such flows are not equitably distributed across all countries. As a response, various developing countries have adopted data-restrictive measures to enable the development of their domestic data capabilities and digital industries. These measures (often framed as tools of digital industrial policy) are seen as being necessary to bridge the data divide. Chapter five investigates whether data-restrictive measures aimed at bridging the data divide can violate international trade law and whether such law can offer any meaningful avenues

to bridge the global data divide. It argues that existing trade agreements are mostly ineffective in addressing concerns pertaining to the global data divide.

Chapter five thus proposes the development of a new framework for streamlined special and differential treatment, based on a fair and equitable relationship between developed and developing countries. For instance, developing countries could be provided with tailored technical assistance and capacity-building support to develop their domestic data regulatory frameworks by developed countries, on the condition that they gradually liberalise cross-border data flows across various digital sectors. The chapter also advocates for special concessions for least developed countries. It emphasises the need to develop a more inclusive model of regulatory cooperation to ensure that developing countries are given meaningful opportunity to express their regulatory preferences and participate in relevant policy and technical discussions in different trade as well as non-trade bodies in relation to global data governance.

Chapter six examines competition laws and policies aimed at reducing the concentration of data in a few technology companies and creating more equitable opportunities in data markets.[119] While cross-border data flows have enabled the rapid growth across several industries, certain Big Tech companies (typically headquartered in digitally advanced countries) control massive volumes of data and data-processing capabilities, potentially resulting in reduced competition in digital markets and causing consumer harm. The chapter thus investigates whether competition disciplines can enable more robust and equitable digital and data flows, and if trade law can play a supportive role in that regard. It argues that competition law must be a foundation for enabling equitable data flows and identifies various ways in which international trade law can play a modest but meaningful role in aligning digital trade rules with relevant principles on digital competition.

In addition to the above examples, there are other policy objectives behind the regulation of cross-border data flows that implicate international trade law. For instance, governments may regulate how platforms manage data and digital content to control the dissemination of fake news. Similarly, certain governments have strict technical controls on the kind/content of data that flows into the country and regulate the censoring of content through an array of data-restrictive measures. Governments may also restrict or control data flows to impose certain digital taxes. However, this book sets aside these issues to focus on the above aspects of data regulation.

While most countries agree on the need for good data governance, including in relation to cross-border data flows, there is little consensus on this to date.[120] For instance, across all the five policy areas investigated in this book,

[119] See, eg PRS, 'Anti-Competitive Practices by Big Tech Companies', www.prsindia.org/policy/report-summaries/anti-competitive-practices-by-big-tech-companies.

[120] Aaronson, 'The Difficult Past' (n 75) 145.

countries have taken varied approaches in their domestic regulation. Studies also indicate that developing countries lack both the regulatory expertise and the infrastructure/resources to foster trust in global data markets or to participate meaningfully in those markets.[121] Thus, the 'data divide' between the developed and developing world exists not only in terms of access to economic opportunities, but also in the capacity to engage in global data governance.[122]

B. A Multilayered Approach to Regulating Cross-Border Data Flows

This introductory chapter highlights that international trade law and global data governance share a complex relationship that cannot be resolved solely through domestic legal and policy interventions. Further, as the subsequent chapters argue, although international trade law, especially new-generation PTAs, are increasingly being used to develop binding rules on data flows and data localisation, they also have limitations. For instance, applying international trade law to certain data-restrictive measures may raise complicated questions regarding the technical feasibility of those measures and require dispute settlement bodies to investigate their underlying policy rationales. In particular, in a world where the narrative on the free flow of data is under immense attack, trade bodies are likely to be cautious in dealing with matters that implicate sovereignty-related concerns.

This book, therefore, takes a flexible and pragmatic approach to exploring mechanisms and avenues to align international trade law with global data governance. Despite the tensions between countries on different aspects of data regulation, it remains amply clear that the majority of countries have strong incentives to develop common solutions to address the trust deficit underlying cross-border data flows today. This is because most countries aspire to be participants in the global digital economy and desire to bring about digital transformation in their countries that can lead to more economic growth and prosperity.[123] Cross-border data flows are central to this digital growth trajectory. Further, not all data-restrictive measures benefit every economy. For instance, several small-sized economies (developed or developing) are much better off enabling data flows than imposing data-restrictive measures.[124] Even for large developing countries, the beneficial impact of data-restrictive measures

[121] See generally A Chander et al, 'World Development Report 2021 – Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation' (2021) World Bank Policy Research Working Paper 9594.

[122] N Mishra and B Agrawal, 'Addressing the Global Data Divide through Digital Trade Law' (2022) 14(2) *Trade, Law & Development* 238, 282–83.

[123] JL González and J Ferencz, 'Digital Trade and Market Openness' (2018) OECD Trade Policy Papers No 217, 34.

[124] See generally D Medine, 'Data Localization – a Hidden Tax on the Poor' (CGD, 27 March 2023) www.cgdev.org/blog/data-localization-hidden-tax-poor; M Bauer et al, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery' (2014) ECIPE Occasional Paper No 3.

remains debatable.[125] In addition, countries across the world are struggling with common problems of the data divide and the concentration of data in a few big companies.[126] Therefore, the problems presented across these different areas of data regulation are transnational policy challenges.

In chapter seven, after examining each of these areas, the book proposes combining traditional trade law disciplines with other soft law norms, best practices and institutional innovations to enable a more decentralised and multi-layered framework for digital trade. This response is necessary and timely for international trade rules to keep abreast of emerging areas of global data governance. New-generation DEAs are often more effective at dealing with evolving areas of data and artificial intelligence regulation than traditional trade treaties. Further, soft law norms and best practices are an important complement to binding trade disciplines on data flows, to ensure that high-level principles enabling co-regulation in digital sectors and transnational regulatory cooperation remain possible.

Chapter seven also highlights the importance of multistakeholder and private norms and standards in the regulatory framework for cross-border data flows and recommends various ways in which international trade law can incorporate these standards and best practices by reference. It recommends various institutional innovations for trade bodies to align better with Internet policy-making and data regulatory bodies at various levels of governance. In making several of these proposals, the chapter also considers ongoing negotiations at the WTO to develop a plurilateral agreement on electronic commerce and contextualises the findings of those chapters for the ongoing dialogues at the WTO.

V. CONCLUSION

Ultimately, I hope to leave my readers with two key messages through this book. First, data-related laws and regulations often implicate provisions in international trade law and can create legal uncertainty for governments, businesses and consumers. For instance, restrictions on cross-border data flows may breach various legal obligations contained in trade treaties, even though they may be justifiable under the different policy exceptions contained in such treaties. There are elaborate legal tests in international trade treaties to examine these issues. Applying these tests often entails complex legal and policy questions, several of which are highlighted in the subsequent chapters. However, the existing framework of trade rules, including dedicated disciplines on digital trade or electronic commerce in PTAs, do not always provide clear answers, thus this interface of international trade law and domestic laws can lead to significant uncertainty for governments,

[125] Bauer (n 124).
[126] See ch 5.

businesses and, ultimately, consumers. Therefore, finding alignment between existing trade rules and global data governance is an important but difficult endeavour.

Second, in response to the existing challenges, and especially given that global data governance is dispersed across various entities at different levels of governance, trade rules applicable to digital trade need to evolve to address the policy challenges arising from cross-border data flows underlying digital transactions. This would require a clear shift in the policy approach and require trade rules that are flexible and pragmatic, and focused on digital trust, international cooperation and regulatory alignment. The book offers various proposals for a multilayered legal and policy approach, combining binding trade disciplines with relevant soft law instruments, principles-based approaches and institutional innovations, with greater consideration of multistakeholder and transnational norms and standards. Although this proposed approach may appear vague due to the presence of numerous soft, flexible and non-binding elements, the book argues why it is ultimately more robust and sustainable to achieve regulatory synergies in the data-driven world.

2

The Tussle and Harmony of Trade and Privacy

I. INTRODUCTION

International trade law and privacy share a difficult relationship. For instance, Irion et al have characterised this relationship as that of 'strange bedfellows'.[1] Chander and Schwartz encapsulate the confusing trade-off between the two in the title of one of their journal articles: 'Privacy and/or Trade'.[2] Given that international trade and privacy law have evolved as two distinct areas of regulation, the complexity of their relationship is unsurprising. As this chapter further explains, this relationship is important for two reasons: (i) personal data flows are a strong driver of the current-day global digital economy; and (ii) the regulation of personal data and the related concerns of privacy protection have become critical to global data governance.[3]

Several countries across the world have now implemented comprehensive laws relating to privacy and data protection. As per the UNCTAD Cyberlaw tracker, 137 out of 194 countries in the world have now adopted a legal framework relating to privacy and/or data protection.[4] While these statistics do not necessarily indicate the quality of the legal framework, they aver to the growing importance of privacy and data protection. In certain countries, the right to privacy protection is embedded in the domestic constitutional or human rights law framework. This is unsurprising, given that the right to privacy is recognised in various international human rights treaties.[5] Data protection laws

[1] K Irion et al, 'Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements' (Bureau Européen des Unions de Consommateurs et al, 2016).

[2] A Chander and PM Schwartz, 'Privacy and/or Trade' (2023) 90(1) *University of Chicago Law Review* 49.

[3] This chapter uses the terms 'privacy' and 'data protection' loosely and sometimes interchangeably; however, they are conceptually different. Privacy represents the value signifying the protection of the right to a private life, while data protection is the rules and compliance requirements for personal data to remain protected when entities process it for various reasons. See M Oostveen, 'Why Privacy ≠ Data Protection (and How They Overlap)' (HIIG, 4 May 2016), https://www.hiig.de/en/why-privacy-%E2%89%A0-data-protection-and-how-they-overlap/.

[4] UNCTAD, 'Data Protection and Privacy Legislation Worldwide', www.unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[5] UNGA Res 217A(III) 'Universal Declaration of Human Rights' (10 December 1948), Art 12 (UDHR); UNGA Res 2200A(XXI) 'International Covenant on Civil and Political Rights'

contain extensive checks, balances and compliance requirements pertaining to the collection, processing and transfer of personal data.

This chapter mostly focuses on requirements for cross-border transfer and processing of personal data in data protection laws. We can view the restrictiveness of these requirements along a spectrum. On the one end of the spectrum, some countries (typically seen as being business-friendly) adopt an accountability-based approach, wherein the company making the international data transfer is accountable for ensuring compliance with data protection law outside the borders but with no further restrictions on the movement of personal data.[6] In the middle of the spectrum lies the adequacy-based approach. Inspired by the mechanism developed by the EU, this approach entails a conditional mechanism, wherein personal data can be transferred only to specific countries whose data protection frameworks offer a level of protection at least equivalent to that of the country of origin of the data subject.[7] Simply put, this requires maintaining a whitelist of foreign jurisdictions to which companies can freely transfer personal data without facing any further restrictions. A stricter conditional mechanism is the need to obtain the prior approval of a regulator on a case-by-case basis for transfer of personal data abroad instead of maintaining a whitelist of safe jurisdictions.[8] At the other end of the spectrum, certain countries impose strict data localisation requirements for personal data. This might relate to specific categories of data, such as sectoral data,[9] or may apply across the board.[10]

(16 December 1966), Art 17 (ICCPR); Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 4 November 1950), Art 8 (ECHR).

[6] DJB Svantesson, 'The Regulation of Cross-Border Data Flows' (2011) 1(3) *International Data Privacy Law* 180, 194. Some examples of jurisdictions using an accountability-based approach include Australia, Mexico, Singapore and Hong Kong.

[7] See generally European Commission, 'Adequacy Decisions', www.commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[8] One of the most-cited examples is China. See Q Tong and W Xintong, 'China Tightens Controls on Cross-Border Data Transfers' (Nikkei Asia, 16 June 2023) www.asia.nikkei.com/Spotlight/Caixin/China-tightens-controls-on-cross-border-data-transfers. See also R Creemers and G Webster, 'Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov 1, 2021' (DigiChina, 7 September 2021) https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (PIPL).

[9] See, eg Law of the People's Republic of China on Basic Medical and Health Care and the Promotion of Health (28 December 2019), Art 10; for Federal Law No 2 of 2019 Concerning the Use of Information and Communication Technology (ICT) in Health Fields (UAE), see Baker McKenzie, 'UAE Issues Law to Protect Health Data and Restrict its Transfer Outside the Country' (March 2019) www.bakermckenzie.com/-/media/files/insight/publications/2019/03/bmham-client-alert--uae-issues-law-to-protect-health-data-and-restrict-its-transfer-outside-the-country--march-2019updatedpdfs.pdf?la=en; Act on the Establishment, Management etc of Spatial Data (3 June 2014) Act No 12738 (Republic of Korea), Art 16; Regulatory Framework for Stored Values and Electronic Payment Systems (UAE) C6/2020, Art 34; RBI Notification on Storage of Payment Systems Data (India, 06 April 2018) RBI/2017-18/153, DPSS.CO.OD No2785/06.08.005/2017-2018.

[10] See, eg Federal Law No 152-FZ on Personal Data as amended in July 2014 by Federal Law No 242 FZ on Amendments to Certain Legislative Acts of the Russian Federation for Clarification of Personal Data Processing in Information and Telecommunications Networks, Art 18(5) (Russian Personal Data Law); Law of the Republic of Kazakhstan No 94-V on Personal Data and its Protection (21 May 2013), Art 12(2).

The latter two categories of measures pertaining to cross-border transfer/processing of personal data often implicate international trade law. This is because both conditional transfer mechanisms and data localisation measures restrict cross-border data flows, either directly or indirectly. As briefly indicated in chapter one, restrictions on transferring data across borders can violate existing obligations in international trade law because, for instance, they might discriminate against foreign providers of digital services or restrict their market access in sectors where countries have committed to opening their markets. Thus, this chapter investigates how international trade law applies to privacy-related data-restrictive measures, and if international trade law and privacy can be meaningfully aligned.

Section II first examines the interface between privacy and digital trade flows. With the rapid digitalisation across several sectors, transfer of personal data has become central to conducting cross-border digital trade. At the same time, data-restrictive elements have increased in data protection laws, including explicit restrictions on personal data transfers. While most governments see these restrictions as being important for protecting the privacy rights of their citizens, they adversely impact digital trade. Additionally, different frameworks on data protection across countries create a fragmented global regulatory framework for data protection. This fragmentation is harmful for digital trade as a safe and secure digital environment is only possible if there is a coherent global framework on privacy and data protection. Thus, this section argues that a two-way relationship exists between trade and privacy; viewing privacy laws simply as a trade barrier is an incomplete characterisation of the relationship of trade and privacy. Privacy laws can also act as an enabler of digital trade and instil trust in the global digital economy.

Section III then examines how international trade law applies to data-restrictive measures contained in domestic privacy and data protection laws. In doing so, this chapter looks at both the General Agreement on Trade in Services (GATS) of the World Trade Organization (WTO), as well as preferential trade agreements (PTAs) and digital economy agreement (DEAs). The key difference between GATS and many PTAs/DEAs is that while GATS provides flexibility to countries to adopt privacy/data protection laws through the exceptions, e-commerce chapters in PTAs and DEAs usually contain an explicit obligation on countries to adopt a basic framework for personal data protection. However, certain data-restrictive measures aimed at privacy/data protection may violate requirements contained in both GATS and PTAs, especially when they take the form of highly restrictive data localisation or conditional transfer mechanisms. While these measures may be justified under the exceptions contained in trade agreements, the application of exceptions is complicated in practice, given the lack of international consensus on the benchmarks for privacy protection, the variable regulatory capacity across different countries and the political sensitivity of the issues involved.

Section IV outlines a new framework for stronger alignment of international trade law and privacy by viewing privacy protection as not only an important domestic but also transnational policy goal. To implement such a framework, trade policy-makers must look beyond the existing vocabulary of obligations and exceptions in international trade law and instead focus on the interplay of international trade law and various global responses to privacy and data protection concerns, including in relation to the cross-border transfer of personal data. The chapter proposes specific reforms, such as incorporating transnational/multistakeholder privacy norms, best practices and standards by reference in trade treaties, and experimenting with new forms of institutional engagement in trade bodies, including transnational bodies such as the Global Privacy Assembly and technical standard-setting bodies. It also proposes that trade tribunals must rely more strongly on technological evidence and expert advice in assessing trade disputes pertaining to privacy-related data-restrictive measures. This measured approach will reduce political friction while providing sufficient tools for meaningful scrutiny of such measures. This caution is also necessary as trade bodies lack the expertise to function as privacy regulatory bodies.

II. PRIVACY, DIGITAL TRADE AND CROSS-BORDER DATA FLOWS

This section uncovers the complex relationship of privacy regulation and digital trade. Privacy protection is a core component of global data governance. With the digitalisation of our lives, personal data protection has become an uphill challenge for regulators around the world. Consequently, domestic data protection laws have mushroomed, often containing highly prescriptive requirement for entities dealing with personal data. This is further complicated because different countries and political cultures ascribe different values to the role of privacy in society and economy.[11] Therefore, although some high-level consensus on principles of data protection exists, the framework for personal data transfers is highly fragmented across countries. This fragmentation signifies not only regulatory culture differences, but also the lack of digital trust among countries. After an assessment of these tensions, the section argues that privacy protection laws should not be seen merely as a barrier to digital trade. Rather, it is equally important to consider how a global culture of privacy and data protection is an enabler of digital trade.

[11] See, eg P Boshe et al, 'African Data Protection Laws: Current Regulatory Approaches, Policy Initiatives, and the Way Forward' (2022) 3(2) *Global Privacy Law Review* 56; PM Schwartz and DJ Solove, 'Reconciling Personal Information in the United States and European Union' (2014) 102(4) *California Law Review* 877; O Manzar, 'Privacy and the Indian Culture' (Mint, 21 September 2017) www.livemint.com/Opinion/rM3vgXErD5oWiv12IEaKcK/Privacy-and-the-Indian-culture.html.

A. Data-Restrictive Measures in Data Protection Laws: Regulatory and Economic Implications

A significant volume of data flowing across borders through digital services, applications and websites consists of personal data.[12] While the definition of personal data can vary across jurisdictions, it typically refers to data related to an identified or identifiable natural person.[13] Therefore, anonymised and aggregated datasets can also fall within the scope of personal data, ie if the individuals in the dataset can be reverse identified using existing technologies.[14] In particular, the EU's framework for data protection, the General Data Protection Regulation (GDPR),[15] imposes a very high standard, whereby if individuals are likely to be identified in a dataset, then such data falls within the scope of personal data. With the rapid development of Big Data technologies, several datasets now contain identifiable data, even if they are stored and processed as anonymised datasets. Thus, the intersection of digital trade and privacy relates to a broad cross-section of Internet transactions of different kinds of businesses.

The role of data protection law has become increasingly significant in the modern-day digital world. First, the rapid development of data-driven technologies and especially the growth of digital platforms has raised concerns regarding protecting individuals from being subject to illegal surveillance and losing control over how technology companies decide about their lives.[16] Thus, data protection law is critical to regulating the behaviour of such technology companies to protect basic privacy rights. Second, personal data can be used for illegal surveillance by foreign governments; thus, data protection law is seen as an important tool to prevent companies from skirting local laws by processing and transferring data abroad, where foreign governments may be able to access such data.[17] Third, data protection laws can generate societal trust, especially when regulators regulate unethical commercial surveillance and protect rights of individuals such as through robust requirements on user consent for collecting and processing personal data, providing remedies for data breaches and even protecting citizens from illegal government surveillance.[18]

[12] Distinguishing personal from non-personal data can be difficult in practice. Further, some of the data that is transferred for digital trade purposes is industrial data. Nonetheless, personal data remains a big driver of the digital economy. See OECD, 'Mapping Approaches to Data and Data Flows – Report for the G20 Digital Economy Task Force' (2020) 12–15.

[13] European Commission, 'What Is Personal Data?', www.commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en.

[14] C Kuner et al (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford, Oxford University Press, 2020) 110–11.

[15] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, recital 26 (GDPR).

[16] See generally S Zuboff, *The Age of Surveillance Capitalism* (New York, Public Affairs, 2019).

[17] UNDP, 'Drafting Data Protection Legislation: A Study of Regional Frameworks' (2023) 10.

[18] LA Bygrave, *Data Privacy Law* (Oxford, Oxford University Press, 2014) 8.

As briefly set out in section I, several countries now impose highly restrictive or compliance-heavy mechanisms to ensure that personal data is not illegally processed in foreign countries. For instance, most regulatory frameworks based on a GDPR-like framework have adopted adequacy mechanisms requiring the regulator to assess the extent to which a foreign jurisdiction offers a robust framework for data protection and thus can offer the same protections as the domestic legal framework. Under the GDPR, the European Commission determines whether a non-EU country has an adequate level of data protection, ie if its data protection framework is 'essentially equivalent' to that of the EU.[19] Adequacy negotiations are usually long and arduous, and involve not only legal but also political and economic considerations.[20] Further, where countries have strong political or ideological differences, adequacy negotiations are likely to fail, even when domestic regulatory frameworks may be similar to each other.[21] Previously, the EU and the USA had twice negotiated bilateral arrangements for the cross-border transfer of personal data (both of which were invalidated by the European Court of Justice for failing to meet the data protection law requirements of the EU).[22] In 2023, these two parties concluded a new agreement for data transfer.[23]

Data protection laws may also provide for contractual safeguards allowing for the transfer of personal data across borders both for intra-company and inter-company transactions. The former mechanism is termed Binding Corporate Rules (BCRs) and the latter is called standard contractual clauses (SCCs) in the GDPR. Following a 2020 judgment of the European Court of Justice,[24] the European Commission updated the standards for SCCs in 2021, requiring companies to assess if the transferee jurisdiction provides a standard of data protection essentially equivalent to the EU.[25] This requirement essentially means that an adequacy-like assessment must also be made for SCCs. Additionally,

[19] GDPR, Preamble (104), Art 45(1). See also Case C 362/14 *Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650, 73–74.

[20] C Kuner, 'International Data Transfers after Five Years of the GDPR: Postmodern Anxieties' (*EU Law Live*, 5 May 2023) www.eulawlive.com/op-ed-international-data-transfers-after-five-years-of-the-gdpr-postmodern-anxieties-by-christopher-kuner/.

[21] L Cerulus, 'Europe Eyes Privacy Clampdown on China' (*Politico*, 4 February 2019) www.politico.eu/article/european-union-eyes-privacy-clampdown-on-china-surveillance-huawei/.

[22] See FTC, 'US–EU Safe Harbor Framework', www.ftc.gov/business-guidance/privacy-security/us-eu-safe-harbor-framework; 'Privacy Shield Overview' (Privacy Shield Framework) www.privacyshield.gov/program-overview.

[23] 'Commission Implementing Decision of 10 July 2023 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU–US Data Privacy Framework' (EU–US Privacy Framework) https://commission.europa.eu/system/files/2023–07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.

[24] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ECLI:EU:C:2020:559.

[25] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council [2021] OJ L199/32.

some countries permit personal data transfers on a case-by-case basis, requiring the data controller/processor to apply to a regulator for approval.[26] This enables the regulator to exercise tighter control over data flows and address issues such as data security in a foreign jurisdiction. Where such approval mechanisms are complex or onerous, they can amount to a de facto localisation requirement for companies collecting and processing data within that country.

The most obvious restrictive form is an explicit data localisation requirement contained in data protection laws.[27] For instance, Russia,[28] Saudi Arabia[29] and Rwanda[30] have adopted domestic laws requiring localisation of personal data. In some other jurisdictions, certain specific categories of personal data must be stored or processed locally. This restriction could apply to some specific sectoral data such as health,[31] telecommunications metadata[32] or (often vaguely) defined subcategories of personal data, such as critical or sensitive data.[33]

Data localisation or other extensive compliance requirements contained in data protection laws are often viewed generally as protectionist measures or instruments of control for the domestic government. However, other rationales may also inform such measures, including the practical challenges of cross-border enforcement of data protection laws, especially when the companies have no commercial presence within the jurisdiction.[34] To date, however, no study has conclusively confirmed that the presence of data localisation or similar restrictive mechanisms can improve the quality of privacy enforcement of the country.

The existence of conflicting and restrictive frameworks on cross-border transfers of personal data can lead to economic inefficiency. For instance, foreign companies may need to bear huge costs to comply with data localisation or other compliance requirements contained in data protection laws, especially if they use servers across different countries. These costs, including business processing outsourcing and other IT services based in developing countries, are especially burdensome for smaller companies.[35] Domestic companies in

[26] See, eg PIPL, Art 38.

[27] Some scholars argue that the mechanism under the GDPR is a soft data localisation requirement. See A Chander, 'Is Data Localization a Solution for *Schrems II*?' (2020) 23(3) *Journal of International Economic Law* 771.

[28] Russian Personal Data Law, Art 18(5).

[29] Personal Data Protection Law (Saudi Arabia) Royal Decree M/19 of 17 September 2021, Art 29.

[30] Law No 058/2021 Relating to the Protection of Personal Data and Privacy (Rwanda, 15 October 2021), Art 50.

[31] See, eg Personally Controlled Electronic Health Records Act (Australia) No 63 of 2012, s. 77.

[32] M Hohnmann, 'German Bundestag Passes New Data Retention Law' (GPPI, 16 October 2015) www.gppi.net/2015/10/16/german-bundestag-passes-new-data-retention-law.

[33] This trend is quite common in South Asia. See the discussion of Pakistan and Sri Lanka in G Greenleaf, 'Pakistan and Sri Lanka's Data Privacy Bills Move Forward' (2021) 173 *Privacy Laws & Business International Report* 24.

[34] See generally OECD, 'Report on the Cross-Border Enforcement of Privacy Laws' (2006).

[35] UNCTAD, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' (2016) UNCTAD/DTL/STICT/2016/1, 4.

the jurisdiction imposing the measure may also be impacted as they could lose access to competitively priced foreign cloud services and other digital services.[36] Some studies have shown that even business-friendly mechanisms such as the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR; a data certification mechanism introduced by APEC, as discussed in more detail in section IVA) have a low uptake among small and medium enterprises due to compliance costs.[37] Ultimately, high costs of digital services and applications will be passed on to end consumers, creating inefficiency along the entire digital value chain.

In addition to economic inefficiency, data-restrictive requirements in domestic laws can lead to regulatory inefficiency. First, extensive regulatory approval or data localisation requirements necessitate governments to monitor the implementation of these laws on an ongoing basis. Especially for governments with regulatory capacity deficit, the enforcement costs may outweigh potential benefits. Chander et al, in their study for the World Bank, had indicated the various difficulties faced by embryonic data protection authorities with a limited budget and expertise in undertaking regulatory monitoring and enforcement.[38] Second, certain data-restrictive measures concentrate extensive power in the government to monitor processing and flows of personal data; this control has potential risks for human rights.[39]

Extensive data restrictions also entail costs from a transnational regulatory perspective. For instance, several governments may expend their resources in negotiating adequacy arrangements with their key trading partners. As noted earlier, these negotiations often entail political in addition to legal considerations, and may be especially burdensome for developing countries. Further, certain countries (particularly developing ones) may be forced to adopt specific data protection frameworks aligned with digital powers such as the EU or the USA to get better access to those markets. However, this may lead to counterproductive outcomes, especially if the regulatory culture of the country necessitates a different approach to privacy protection or where there could be premature load bearing in adopting an extensive regulatory framework.[40] In conclusion,

[36] On the contrary, certain companies, especially local telecommunications service providers, may enjoy benefits of such localisation measures, especially if they are bigger in size and can benefit from being protected from foreign competition, at least in the short run.

[37] APEC, 'Trade Policy Dialogue on Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses' (23 August 2019) APEC Project CTI 08 2018T, 6, 9.

[38] See generally A Chander et al, 'World Development Report 2021 – Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation' (March 2021) World Bank Policy Research Working Paper 9594.

[39] A Plaum, 'The Impact of Forced Data Localisation on Fundamental Rights' (Access Now, 4 June 2014) www.accessnow.org/the-impact-of-forced-data-localisation-on-fundamental-rights/; D Medine, 'Data Localization – a Hidden Tax on the Poor' (*CGDev Blog*, 27 March 2023) www.cgdev.org/blog/data-localization-hidden-tax-poor.

[40] Regulatory fragmentation can also lead to jurisdictional conflicts over access to personal data, as illustrated later in ch 4.

while data protection laws are an important part of digital regulation today, certain aspects of these laws, particularly compliance requirements or restrictions on cross-border processing and transfer of personal data, can lead to economic and regulatory inefficiencies and pose as barriers to digital trade.

B. The Digital Trade – Privacy Dilemma

While certain aspects of data protection law are emerging as barriers to digital trade, many governments impose these requirements for sound policy reasons, such as protecting the privacy rights of their citizens, facilitating stronger enforcement and holding the private sector accountable for their data processing activities. Further, several data protection laws explicitly acknowledge the importance of facilitating personal data flows.[41] This creates an obvious dilemma between trade and privacy objectives.

A large reason for the fragmentation of the regulatory frameworks on privacy and data protection stems from the lack of trust between countries. For instance, governments are suspicious of the data operations of foreign technology companies, especially if they are data monopolies with worldwide presence. As chapter six argues, the ability of some of the biggest technology companies in the world today to access and monitor gigantic volumes of personal data of their users gives them unqualified economic and even political power. This power can easily be misused by these companies to illegally monitor and exploit their users and trap them in their digital ecosystems for an indefinite period, thereby reducing opportunities for emerging market players.

Similarly, governments may be concerned about the protection of the data of their citizens when it moves abroad to foreign jurisdictions without a robust data protection framework, especially in authoritarian countries. In such scenarios, the personal data of their citizens stored in the foreign jurisdiction is not subject to the same data protection principles as the home jurisdiction. Further, the value accorded to privacy and data protection can vary across countries; for instance, in certain countries, data protection laws may be seen as being critical to information security or consumer protection rather than protecting individual privacy rights.[42] Increasingly, protection of personal data such as location and personal identity details have also become critical from the perspective of protecting national security.[43] Also, in some countries, governments enjoy

[41] See, eg GDPR, Recital 3.

[42] K Irion, 'Government Cloud Computing and National Data Sovereignty' (2012) 4(3–4) *Policy & Internet* 40, 50.

[43] SA Aaronson, 'Why Personal Data Is a National Security Issue' (*Barrons*, 12 August 2020) www.barrons.com/articles/why-personal-data-is-a-national-security-issue-51597244422; D Van Puyvelde et al, 'National Security Relies More and More on Big Data. Here's Why' (*Washington* Post, 27 September 2017) www.washingtonpost.com/news/monkey-cage/wp/2017/09/27/national-security-relies-more-and-more-on-big-data-heres-why/.

significant exemptions from complying with requirements set out in data protection laws for a large range of situations related to public interest and national security.[44]

Finally, countries are likely to struggle in pursuing legal action against foreign companies that breach their domestic data protection laws, especially in scenarios where these companies do not have a local commercial presence, especially data operations. In the absence of a truly global treaty on data protection and the lack of sufficient international norms, these concerns are further magnified. Developing countries that have limited regulatory resources are likely to find cross-border enforcement harder than seasoned data protection authorities in richer countries.

The above discussions indicate that the absence of robust and coherent privacy and data protection norms also create roadblocks to trust in global digital trade. Without a global framework for data privacy, it is impossible to create an open and secure Internet and generate the interconnectivity of networks necessary to boost digital trade.[45] Expectedly, several bodies have created initiatives and instruments to deal with various aspects of personal data flows. Some of the most significant initiatives are discussed in section IVA below. Therefore, in creating a global framework for cross-border data flows, including understanding how international trade law can play a contributory role, policymakers (in both domestic and international bodies) must also devote attention to the potential trade-enabling function of data protection law and its importance from a transnational/global perspective.

III. INTERFACE OF PRIVACY MEASURES WITH INTERNATIONAL TRADE LAW

This section examines whether international trade law contained in both WTO treaties and PTAs apply to data-restrictive measures related to privacy/data protection. As explained in chapter one, the most relevant WTO treaty applicable to measures relating to cross-border data flows is GATS. This section first provides a brief overview of GATS to contextualise the discussions for the rest of the section. It then examines how GATS applies to data-restrictive measures contained in domestic data protection and/or privacy laws.

GATS does not contain any specific benchmarks or requirements for members to adopt a data privacy framework. Instead, the key question is whether a specific measure may be inconsistent with the broader obligations under GATS and, if

[44] See, eg discussion of exemptions in Indonesia's data protection law in IGNP Widiatedja and N Mishra, 'Establishing an Independent Data Protection Authority in Indonesia: A Future-Forward Perspective' [2022] *International Review of Law, Computers & Technology* 1.

[45] N Mishra, 'Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows' (2021) 52(2) *Vanderbilt Journal of Transnational Law* 463; UNCTAD (n 35) 2.

so, whether it can be justified under the exceptions contained in the treaty. While this legal test may seem straightforward in theory, it is far more complex in practice due to the various difficulties in applying a pre-Internet era to modern digital services, particularly as the application of international trade law to domestic data protection measures may be seen as a direct confrontation to the digital/data sovereignty of a country.

The last part of this section examines how existing provisions in PTAs (focusing on the e-commerce chapters) and DEAs are relevant to privacy. This section argues that several PTAs and DEAs address the relationship between digital trade and privacy more directly. First, several recent PTAs incorporate provisions on cross-border data flows and data localisation, preventing parties from adopting data-restrictive measures. However, such measures are subject to a vaguely worded legitimate public policy exception, which arguably creates at least some degree of legal uncertainty for cross-border flows of personal data. Second, unlike GATS, several PTAs incorporate requirements for parties to adopt basic frameworks on data protection and privacy consistent with international standards, although the benchmarks for these standards are often vague and vary significantly across treaties. EU PTAs contain an express carve-out for data protection rules, thereby enabling parties to implement data protection laws without violating any trade obligations. While the variation across PTAs reflects the diversity of domestic privacy and data protection regulations, it can create a 'spaghetti bowl effect',[46] causing more uncertainty for digital trade.

A. An Overview of GATS

GATS has a unique and complex architecture. At the outset, a few details are necessary to understand how GATS applies to data-restrictive measures. This explanation will also be helpful for the subsequent chapters examining the application of GATS to other data-restrictive measures. GATS contains two sets of obligations: (i) general obligations applicable to all measures of members affecting trade in services; and (ii) specific obligations that only apply in service sectors where members have offered relevant commitments in their GATS Schedule of Commitments (explained in more detail below). The provisions on most favoured nation treatment (MFN) and transparency are examples of general obligations, whereas the provisions on market access and national treatment are examples of specific obligations. The provision on domestic regulation contains both general and specific obligations.

The GATS Schedule of Commitments is a list of commitments agreed upon by each WTO member in different service sectors and modes of delivery, as explained below. It contains specific information such as: (i) 'terms, limitations

[46] J Bhagwati, 'US Trade Policy: The Infatuation with FTAs' (Columbia University, 1995) Discussion Paper Series No 726, 4.

and conditions on market access'; (ii) 'conditions and qualifications on national treatment'; (iii) any additional commitments 'not subject to scheduling under Articles XVI or XVII, including those regarding qualifications, standards';[47] and (iv) a time frame for implementation of commitments and date of entry, where required.[48] Effectively, the Schedule indicates the extent to which a WTO member is willing to expose their domestic players to foreign competition in specific service sectors.

In identifying commitments across different service sectors in their GATS Schedule, most WTO members have used two documents: Doc W/120 and Provisional Central Product Classification (CPC Prov). Doc W/120 contains a classification of the services economy (dividing the whole economy into 12 service sectors) and was prepared by the GATT Secretariat on the request of the members in 1993.[49] This document cross-refers each sector to a corresponding sector heading in the CPC Prov, which was developed by the UN in 1991.

In their GATS Schedule, WTO members must prescribe not only commitments in a specific sector, but also the specific mode of delivery. Four modes of delivery are listed in GATS: 'from the territory of one Member into the territory of another Member' (Mode 1); 'from the territory of one Member to the service consumer of another Member' (Mode 2); 'by a service supplier of one Member, through commercial presence in the territory of any another Member' (Mode 3); and 'by a service supplier of one Member, through the presence of natural persons of a Member in the territory of any other Member' (Mode 4).[50]

B. Assessing Privacy-Related Data-Restrictive Measures under GATS

Under GATS, a data-restrictive measure that impacts supply of any digital services could qualify as a measure affecting trade in services. The word 'measure' has been defined very broadly in GATS and includes not only domestic laws and regulations, but also administrative practices and decisions,[51] as well as acts or omissions attributable to a specific member,[52] even if they are unwritten[53] or discretionary.[54] Similarly, the phrase 'trade in services' has a broad meaning and

[47] General Agreement on Trade in Services (Marrakesh, April 1994), Art XVIII (GATS).

[48] GATS, Art XX:1.

[49] WTO, 'Services Sectoral Classification List – Note by the Secretariat' (10 July 1991) WTO Doc MTN.GNS/W/120 (Doc W/120).

[50] GATS, Art I: 2.

[51] GATS, Art XXVIII(a). See also *Argentina – Measures Relating to Trade in Goods and Services*, Appellate Body Report (adopted 9 May 2016) WT/DS453/12, para 6.259 (Argentina – Financial Services).

[52] *United States – Sunset Review of Anti-Dumping Duties on Corrosion-Resistant Carbon Steel Flat Products from Japan*, Appellate Body Report (adopted 9 January 2004) WT/DS244/10, para 81.

[53] *United States – Laws, Regulations and Methodology for Calculating Dumping Margins (Zeroing)*, Appellate Body Report (adopted 9 May 2006) WT/DS294/46, para 198.

[54] See, eg *United States – Tariff Measures on Certain Goods from China*, Panel Report (circulated 15 September 2020) WT/DS543/10, paras 7.53–7.54; *China – Measures Affecting the Protection and*

includes 'production, distribution, marketing, sale and delivery of a service'.[55] I will now examine how a data-restrictive measure related to privacy/data protection can breach GATS.

(i) Breach of Specific Obligations Contained in GATS

A data-restrictive measure can violate the MFN requirement if it fails to 'accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favourable than that it accords to like services and service suppliers of any other country'.[56] Thus, for a data-restrictive measure to violate Article II, two conditions must be met: (i) the measure affects like digital services and service suppliers of different WTO members; and (ii) it provides less favourable treatment to 'like' services and service suppliers of different WTO members, by creating different competitive conditions for like services or service suppliers of different WTO members.

The likeness of services and service suppliers can be de jure (ie based on the country of origin of the service or service provider) or de facto (ie based on the application of an economic test determining the competitiveness between different services and service suppliers from different countries).[57] Most adequacy mechanisms constitute a de jure discrimination under Article II, as they entail differential treatment between different services or service providers, based on where the data processing services are conducted.[58] For the purposes of this test, the regulatory rationale behind the differential treatment is irrelevant.[59]

A clear example of MFN violation would be a ban on a specific digital service from a member (eg WeChat, offered by a Chinese company) while permitting the supply of a like digital service from another member (eg WhatsApp, offered by a US company) on the grounds that the former does not offer end-to-end encryption (this may, however, be justifiable under the exceptions, as discussed below). In certain cases, however, privacy preferences of end users can create two distinct markets of encrypted and unencrypted messaging services, thus not meeting the likeness requirement in Article II.[60]

Enforcement of Intellectual Property Rights, Panel Report (adopted 20 March 2009) WT/DS362/15, paras 7.359–7.367, 7.393–7.394.

[55] GATS, Art XXVIII(b).

[56] GATS, Art II:1. However, members may list specific exemptions in the Art II Annex.

[57] The pertinent factors in examining competition between different services are the intrinsic character or nature/property (including quality) of the services; their end use; consumer perceptions; and classification under Doc W/120. See Argentina – Financial Services (n 51) para 6.61.

[58] This is based on the finding in ibid para 6.44–6.45, wherein the AB held that likeness can be presumed if a discrimination is purely based on the origin of a service or service supplier.

[59] ibid paras 6.151, 6.124–6.126.

[60] M Burri, 'Understanding the Implications of Big Data and Big Data Analytics for Competition Law: An Attempt for a Primer' in K Mathis and A Tor (eds), *New Developments in Competition Behavioural Law and Economics* (Cham, Springer, 2018) 241, 255.

Several data protection laws contain specific requirements for data localisation. Such measures often favour domestic companies (especially large telecommunications service providers) and discriminate against foreign companies/services as the measures require them to build new data operations domestically or lease them from domestic companies. In doing so, the data localisation requirement skews the competition in favour of domestic companies operating in like sectors. This kind of discrimination against foreign services and service providers is covered by the national treatment obligation in Article XVII. As explained earlier, this obligation only applies if a WTO member has made relevant GATS Schedule commitments in the affected sector and mode of delivery.

The assessment of relevant commitments in a WTO member's GATS Schedule often requires answering complex questions, especially given that the classification used by most members is based on a two-decades-old classification system. While several scholars have argued for a technologically neutral interpretation of commitments (consistent with past WTO decisions),[61] it is not clear what this means in practice. For instance, certain countries have argued that the category of 'computer and related services' should not cover recent innovations such as cloud computing and social media services.[62] Further, as digital services have evolved rapidly with the convergence of various digital services under single platforms, legal uncertainty exists regarding the relevance of the old CPC Prov classification. The most recent iteration (CPC v2.1) does not even contain 'computer and related services', as the existing subsectors under this sector have been reclassified into different categories such as 'business services' and 'online content services'.[63] Further, developing countries are expectedly cautious about giving up their ability to implement digital industrial policies in fast-emerging digital sectors.[64]

A strict data localisation measure contained in a data protection law can also violate the obligation on market access, contained in GATS, Article XVI:2. This provision has two requirements: (i) a member must have made commitments on market access in sectors/modes affected by a measure (thus similar to the

[61] LL Tuthill, 'Cross-Border Data Flows: What Role for Trade Rules?' in P Sauvé and M Roy (eds), *Research Handbook on Trade in Services* (Cheltenham, Edward Elgar, 2016) 357, 360–61. See generally I Willemyns, 'GATS Classification of Digital Services – Does "The Cloud" Have a Silver Lining?' (2019) 53(1) *Journal of World Trade* 59. See also *China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, Appellate Body Report (adopted 19 January 2010) WT/DS363/19, para 396 (China – Publications and Audiovisual Products).

[62] See, eg WTO Committee on Specific Commitments, 'Report of the Meeting Held on 18 September 2014 – Note by the Secretariat' (15 October 2014) WTO Doc S/CSC/M/71; WTO Committee on Specific Commitments, 'Report of the Meeting Held on 15 March 2017' (1 May 2017) WTO Doc S/CSC/M/78.

[63] CPC 843 for online content services and Division 83 for professional, technical and business services, including various IT and web-hosting-related services (CPC 8313, 8314, 8315, 8316). See UN DESA, 'Central Product Classification (CPC)' (2015) Statistical Paper Series M No 77, Ver 2.1.

[64] R Zhang, 'Covered or Not Covered: That Is the Question' (November 2015) WTO Working Paper ERSD-2015-11, 30. See also ch 5.

national treatment obligation); and (ii) the measure results in one or more of the following: limiting the 'number of service suppliers'; 'total value of service transactions or assets'; 'total number of service operations or on the total quantity of service output'; 'total number of persons that may be employed in a particular service sector or that a service supplier may employ'; 'the participation of foreign capital'; and 'restrict or require specific types of legal entity or joint venture through which a service supplier may supply a service'.[65]

If a WTO member inscribes full market access commitments for a specific service sector, any privacy-related measure banning cross-border data flows in that sector (under Mode 1 or Mode 3, depending on the wording of the measure) will effectively restrict the number of foreign service suppliers and/or foreign service transactions or operations to zero in the member's territory, unless the foreign companies localised its server operations. In a previous dispute, the WTO Appellate Body (AB) held that a complete restriction on market access constitutes a 'zero quota' and is a violation of GATS, Article XVI.[66] Thus, a measure banning cross-border data flows in a sector and mode of delivery in which a member has inscribed market access commitments breaches GATS, Article XVI(b) and (c).

GATS also imposes various obligations regarding implementation of domestic regulations in Article VI. Thus, various aspects of the implementation of a data-restrictive measure in a data protection law could be subject to assessment under Article VI. For instance, this provision would apply if a particular data localisation measure is implemented in an arbitrary manner to target specific foreign companies. It may also apply if a particular regulatory approval system or certification mechanism for cross-border transfer of personal data is not conducted in a transparent manner or deliberately targets foreign digital services or service providers. GATS, Article VI can thus be effective as it prevents the abuse of administrative discretion and ensures minimum due process in the implementation of measures on cross-border data flows.[67]

If WTO members have offered relevant commitments in their Schedule, GATS, Article VI:5 prohibits them from imposing licensing requirements or technical standards that can 'nullify and impair' those commitments, including when they are not based on objective and transparent criteria or are more burdensome than necessary,[68] or 'could not reasonably have been expected of that Member at the time the specific commitments in those sectors were made'.[69]

[65] GATS, Art XVI: 2.

[66] See *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, Appellate Body Report (adopted 20 April 2005) WT/DS285/26, paras 238, 251, 373. (US – Gambling).

[67] S Peng, 'The Rule of Law in Times of Technological Uncertainty: Is International Economic Law Ready for Emerging Supervisory Trends?' (2019) 22(1) *Journal of International Economic Law* 1, 9, 16–18.

[68] GATS, Art VI:5(a)(i), read with GATS, Art VI:4.

[69] GATS, Art VI:5(a)(ii).

In assessing whether the licensing and qualification requirements and technical standards are reasonable and based on objective criteria, governments must consider the international standards of 'relevant international organizations'.[70]

The definition of international organisations in GATS, Article VI is limited to international bodies 'whose membership is open to the relevant bodies of at least all WTO members'. As discussed later in section IVA, several relevant discussions on data protection are occurring outside traditional state-driven bodies, thus the ability of WTO panels to consider a broader range of instruments in assessing reasonableness of technical standards is constrained. In other words, WTO members currently have a wide discretion in choosing the applicable technical standards in implementing their domestic privacy laws.[71] On the one hand, this flexibility may be seen favourably as protecting domestic policy space; on the other hand, it could lead to protectionist measures that, in turn, create a fragmented framework for digital trade.

(ii) Justifying Privacy-Related Data-Restrictive Measures under General Exceptions

As more countries adopt data protection laws containing data-restrictive elements, the exceptions contained in trade treaties have become extremely important. They provide an escape mechanism for countries to defend their domestic regulations. GATS contains a list of public policy exceptions under Article XIV (also known as general exceptions) that a member can invoke to justify its domestic measures. As described below, the test under the exceptions is quite rigorous and difficult to satisfy in practice. Therefore, certain scholars are concerned that trade law will interfere with domestic regulatory prerogatives and will be especially harmful for developing countries seeking to build an indigenous model of digital regulation.[72] Further, as the interface between privacy and trade law can be broached in WTO law primarily through strictly worded exceptions, certain scholars argue that trade liberalisation trumps privacy in the GATS framework.[73]

The first relevant exception in the context of privacy measures is GATS, Article XIV(a), which permits measures 'necessary to protect public morals or maintain public order'. To date, this provision has been interpreted liberally in WTO disputes.[74] In *US – Gambling*, the WTO panel held that 'public morals

[70] GATS, VI.5(b).

[71] RH Weber, 'Regulatory Autonomy and Privacy Standards under the GATS' (2012) 7 *Asian Journal of WTO and International Health Law & Policy* 25, 37.

[72] See generally J Kelsey, 'How a TPP-Style E-commerce Outcome in the WTO Would Endanger the Development Dimension of the GATS Acquis (and Potentially the WTO)' (2018) 21(2) *Journal of International Economic Law* 273.

[73] K Irion et al, 'Privacy Peg Trade Hole: Why We (Still) Shouldn't Put Data Privacy in Trade Law' (*University of Chicago Law Review Online*, 27 March 2023) www.lawreviewblog.uchicago.edu/2023/03/27/irion-kaminski-yakovleva/.

[74] M Du, 'How to Define "Public Morals" in WTO Law? A Critique of Brazil – Taxation and Charges Panel Report' (2018) 13(2) *Global Trade and Customs Journal* 69.

denotes standards of right and wrong conduct maintained by or on behalf of a community or nation'.[75] Further, public morality was considered context-specific and thus could vary across countries, depending on their 'prevailing social, cultural, ethical and religious values'.[76] The term 'public order' is often used interchangeably with 'public morals', although the GATS specifically provides that the public order exception can only be invoked when there is a 'a genuine and sufficiently serious threat … to one of the fundamental interests of society'.[77]

As protection of data privacy is intrinsically tied to cultural, political and social values in many societies,[78] WTO members can argue that their privacy-related data-restrictive measures fall within the scope of GATS, Article XIV(a). Further, in countries where data protection laws are seen as being fundamental to data security,[79] the public order exception may be specifically relevant, especially as personal data breaches can prejudice the safety of critical information infrastructure within the country in the health, financial and other key sectors.

The second relevant exception is GATS, Article XIV(c)(ii), which states that a measure violating GATS obligations can be justified if: (i) it is implemented to secure compliance with domestic 'laws and regulations',[80] including those 'relat[ing] to … the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts'; (ii) the above 'laws and regulations' are consistent with WTO law; and (iii) the measure is necessary to secure compliance with these laws and regulations.[81]

GATS, Article XIV(c)(ii) can be interpreted in an evolutionary manner to cover different aspects of data privacy and protection.[82] The term 'relating to'

[75] US – Gambling (n 66) para 6.465.

[76] ibid para 6.465. See also *European Communities – Measures Prohibiting the Importation and Marketing of Seal Products*, Appellate Body Report (adopted 18 June 2014) WT/DS400/16/Add.7 and WT/DS401/17/Add.7, para 5.199 (EC – Seal Products).

[77] GATS, Art XIV(a), fn 5.

[78] See, eg JQ Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2014) 113(6) *Yale Law Journal* 1151.

[79] See generally J Lee, 'Hacking into China's Cybersecurity Law' (2017) 53(1) *Wake Forest Law Review* 57.

[80] See *Mexico – Tax Measures on Soft Drinks and Other Beverages*, Appellate Body Report (adopted 24 March 2006) WT/DS308/16, para 79 (Mexico – Taxes on Soft Drinks) (where the AB held that 'laws and regulations' refer to domestic laws and regulation, and not international law, unless it is incorporated into domestic law).

[81] *Colombia – Indicative Prices and Restrictions on Ports of Entry*, Panel Report (adopted 20 May 2009) WT/DS366/15, para 7.514; *United States – Import Prohibition of Certain Shrimp and Shrimp Products*, Appellate Body Report (adopted 6 November 1998) WT/DS58/23, para 7.174 (US – Shrimp). See also *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, Appellate Body Report (adopted 10 January 2001) WT/DS161/12 and WT/DS169/12, para 157 (Korea – Various Measures on Beef); *Thailand – Customs and Fiscal Measures on Cigarettes from the Philippines*, Appellate Body Report (adopted 15 July 2011) WT/DS371/46, para 177; US – Gambling (n 66) paras 6.536–6.537. See also M Du, 'The Necessity Test in World Trade Law: What Now?' (2016) 15(4) *Chinese Journal of International Law* 817, 835.

[82] In the context of evolutionary interpretation, see US – Shrimp (n 81) para 129.

requires a substantial relationship of the measure to the stated policy objective.[83] For instance, 'protection of privacy of individuals' in GATS, Article XIV(c)(ii) can be interpreted to cover policy objectives of preventing unauthorised online surveillance of individuals by governments and indiscriminate use of personal data by companies without express user content. Further, the term 'secures compliance' implies that domestic laws and regulations should 'enforce "obligations" contained in [those] laws and regulations',[84] and does not imply that the results of the measure can be guaranteed with 'absolute certainty'.[85]

Under GATS, Article XIV, the necessity of a measure is examined through two steps: (i) assessing the relative importance of the interests and values underlying the measure; and (ii) conducting a 'weighing and balancing' test considering the importance of those interests/values. The more critical the policy objective behind a measure, the easier it is to defend the necessity of the measure.[86]

Protection of individual privacy is explicitly covered under GATS, Article XIV(c)(ii). Furthermore, privacy is a central concern in the regulation of digital technologies and networks today.[87] Therefore, privacy considerations clearly fall under GATS, Article XIV. Even in scenarios where a country disguises specific protectionist or other ulterior motives as a data protection or privacy-related measure, a WTO panel is likely to defer to the stated policy objective without questioning the subjective intention of the specific WTO member (though it can scrutinise it under the weighing and balancing test, explained below). This is a more judicious approach, given that the perception of privacy and data protection varies across countries.[88]

The more vital and difficult element under the general exceptions is assessing the necessity of the measure using the weighing and balancing test, which requires consideration of various factors, such as the contribution of the measure to the policy objective, the restrictive impact of the measure on international commerce, and the availability of reasonable and less trade-restrictive alternatives.[89] Under this test, the WTO panel must first examine whether a

[83] *United States – Standards for Reformulated and Conventional Gasoline*, Appellate Body Report (adopted 20 May 1996) WT/DS2/AB/R, p 19 (US – Gasoline); US – Shrimp (n 81) para 141.

[84] US – Gambling (n 66) para 6.538. See also *United States – Standards for Reformulated and Conventional Gasoline*, Panel Report (adopted 20 May 1996) WT/DS2/R (US – Gasoline) para 6.33.

[85] Mexico – Taxes on Soft Drinks (n 80) paras 72–74; See also *China – Measures Affecting Imports of Automobile Parts*, Panel Report (adopted 12 January 2009) WT/DS342/15, para 7.337.

[86] Korea – Various Measures on Beef (n 81) para 162.

[87] A Rachovitsa, 'Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue' (2016) 24(4) *International Journal of Law and Information Technology* 374, 375, 390.

[88] CL Mann, 'International Internet Governance: Oh What a Tangled Web We Weave' (2001) 2(2) *Georgetown Journal of International Affairs* 79, 81; C Kuner, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law' (2011) OECD Digital Economy Papers No 187, 7.

[89] *Brazil – Measures Affecting Imports of Retreaded Tyres*, Appellate Body Report (adopted 17 December 2007) WT/DS332/19/Add.6, para 146, 178 (Brazil – Retreaded Tyres); US – Gambling (n 66) para 307; Korea – Various Measures on Beef (n 81) para 164. See also Du, 'The Necessity Test in World Trade Law' (n 81) 817.

'genuine relationship of means and ends' exists between the measure and the policy objective of privacy protection, ie whether the measure actually contributes to privacy protection.[90] In conducting this examination, both legal and technological questions can be relevant.[91] For example, a panel may consider whether local data storage benefits or is potentially counterproductive to privacy protection, ie whether it increases the vulnerability of data to both cyberattacks and illegal government surveillance.[92] It may also consider whether data localisation or other conditions imposed for personal data transfer facilitate robust enforcement of domestic data protection laws. Such an evidence-oriented approach is less interfering and more respectful of a country's policy preferences as it is primarily focused on the measure rather than the proffered policy objective.

The second factor examined under the weighing and balancing test is the trade-restrictive impact of the measure and its impact on international commerce. Data-restrictive measures are generally disruptive,[93] affecting commercial arrangements across different industries due to the widespread adoption of digital services in various business operations.[94] Therefore, such measures are likely to have an adverse impact on international commerce. However, the direct economic impact of cross-border data flows is not easily measurable.[95] This could inhibit complainants from providing robust quantitative evidence of the restrictive impact of data localisation.[96] However, complainants could provide other evidence showing the impact of the measure, such as surveys showing less open or competitive markets for foreign digital services, low trust levels in indigenous digital services or local cloud computing facilities, and lack of sufficient digitally driven services in the domestic market. All these factors indicate reduced opportunities of import and export of digital services into the market.[97]

[90] Brazil – Retreaded Tyres (n 89) para 210. See also EC – Seal Products (n 76) para 5.210.

[91] See the discussion of a similar approach in U Gasser, 'Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy' (2016) 130 (2) *Harvard Law Review Forum* 61.

[92] T Maurer et al, 'Technological Sovereignty: Missing the Point?' in M Maybaum et al (eds), *Architectures in Cyberspace* (Tallinn, NATO CCD COE Publications, 2015) 53, 61–62; N Cory, 'Cross-Border Data Flows: Where Are the Barriers and What Do They Cost?' (ITIF, May 2017) 3–4; K Komaitis, 'The "Wicked Problem" of Data Localization' (2017) 3(2) *Journal of Cyber Policy* 355, 361–62.

[93] See, eg M Bauer et al, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery' (2014) ECIPE Occasional Paper 3/2014; JP Meltzer, 'The Internet, Cross-Border Data Flows and International Trade' (2014) 2 *Asia & the Pacific Policy Studies* 90, 92; United States International Trade Commission, *Digital Trade in the US and Global Economies, Part 2* (August 2014) Publication No 4485, 65.

[94] WK Hon et al, 'Policy, Legal and Regulatory Implications of a Europe-only Cloud' (2016) 24(3) *International Journal of Law and Information Technology* 251, 253–54.

[95] US Department of Commerce, 'Measuring the Value of Cross-Border Data Flows' (September 2016) 1.

[96] Both quantitative and qualitative evidence can be put forth to assess the restrictive impact of a measure. See Brazil – Retreaded Tyres (n 89) para 146.

[97] See generally T Voon, 'Exploring the Meaning of Trade Restrictiveness in the WTO' (2015) 14(3) *World Trade Review* 451, 456.

Finally, the test requires consideration of alternative less trade-restrictive measures proposed by the complainant that are reasonably available to the defendant[98] and achieve an equivalent level of privacy protection.[99] Several technological and policy solutions can be proposed as potential alternatives. For example, a complainant might propose robust encryption,[100] privacy trustmarks or self-certification mechanisms as less trade-restrictive alternatives to banning cross-border data flows. For instance, if a successful mechanism is developed under the ongoing global CBPR dialogues (entailing revised discussions on expanding the CBPR framework originally designed under APEC to a global level),[101] certain countries may argue that conducting data transfers using those mechanisms are a less trade-restrictive alternative than data localisation or similar restrictions. Similarly, the successful negotiation of a global treaty on cross-border privacy enforcement[102] could negate the requirements for data localisation. It can also be argued that implementing a privacy-by-design approach, wherein companies are obliged to incorporate fundamental data protection principles in their design,[103] would invalidate the need for excessive restrictions on data transfers.

Given the sensitivity of personal data regulation, the diverging privacy preferences across countries and the geopolitical divide between leading digital powers, a more judicious approach would be to treat the above evolving legal, policy and technological solutions as complementary rather than alternative measures.[104] For example, many developing countries have inadequate expertise and resources to enforce or monitor many of these mechanisms. Further, certain governments suspect the reliability of privacy trustmarks, and thus could argue that these mechanisms do not achieve the desired level of privacy protection.[105] Certain initiatives aimed at enabling cross-border data flows, such as the ongoing Global CBPR Forum, deliberately exclude specific countries for political reasons[106] and are thus unlikely to qualify as a credible alternative. Finally, due to the absence of international benchmarks or standards[107] and the uncertainties

[98] US – Gambling (n 66) para 308; China – Publications and Audiovisual Products (n 61) paras 326–27; EC – Seal Products (n 76) para 5.279.

[99] See, eg Brazil – Retreaded Tyres (n 89) para 156; China – Publications and Audiovisual Products (n 61) 246.

[100] WK Hon, *Data Localization Laws and Policy* (Cheltenham, Edward Elgar, 2017) 8.

[101] US Department of Commerce, 'Global Cross-Border Privacy Rules Declaration', www.commerce.gov/global-cross-border-privacy-rules-declaration. See also s IVA.

[102] As proposed by Chander and Schwartz. See Chander and Schwartz (n 2) 115–16.

[103] See, eg GDPR, Preamble (78); see also Art 25(1).

[104] See Brazil – Retreaded Tyres (n 89) 172.

[105] C Connolly et al, 'Privacy Self-Regulation in Crisis? TRUSTe's "Deceptive" Practices' (2014) UNSW Law Research Paper No 2015-08, 2, 3.

[106] 'GT Voice: China, Other Nations Must Break US' Self-Serving Data Rules System' (*Global Times*, 17 May 2022) www.globaltimes.cn/page/202205/1265902.shtml.

[107] C Kuner et al, 'The Language of Data Privacy Law (and How It Differs from Reality)' (2016) 6(4) *International Data Privacy Law* 259. See also LA Bygrave, 'Hardwiring Privacy' in R Brownsford

in the development of data-driven technologies,[108] the assessment of compliance with technological mechanisms would be a guesswork rather than a foolproof process.[109] Therefore, in most cases barring naked protectionism, data-restrictive measures contained in data protection laws are likely to be provisionally justified under GATS, Article XIV(a) or Article XIV(c)(ii).

Even if a measure provisionally satisfies the necessity test in GATS, Article XIV, it must be further examined for consistency with the chapeau of GATS, Article XIV:

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

In conducting this assessment, a WTO panel would examine the implementation and operationalisation of the measure[110] to ensure that it is implemented in 'good faith'.[111] The assessment under the chapeau requires an enquiry into the 'design, architecture, and revealing structure of a measure'[112] to assess if the measure violates GATS, Article XIV chapeau in 'its actual or expected application'.[113] Panels often also use factual evidence in assessing a measure under the chapeau where the design of the measure is not revealing.[114]

In applying the GATS, Article XIV chapeau to a privacy-related data-restrictive measure, it must be first assessed whether 'like conditions' prevail either (i) between the WTO member imposing the privacy measure and other exporting WTO members or, in case a privacy measure favours or disfavours specific members, (ii) between those countries and other exporting WTO members. In assessing 'like conditions' under the chapeau, a WTO panel can compare regulatory conditions in different countries. For example, countries with strong data protection laws can be considered 'unlike' countries with a weak privacy regime. In practice, making these comparisons entails sensitive political and cultural questions, even if it is theoretically possible.

et al (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford, Oxford University Press, 2017) 755, 759, 772.

[108] See generally A Chander, 'Future-Proofing Law' (2017) 51(1) *UC Davis Law Review* 1, 3; C Xavier et al, 'The Internet of Things and Its Impact on Individual Privacy: An Australian Perspective' (2016) 32(1) *Computer Law & Security Review* 4, 9.

[109] Kuner et al, 'The Language of Data Privacy Law' (n 107) 269.

[110] US – Gasoline (n 83) para 22.

[111] US – Shrimp (n 81) para 158.

[112] EC – Seal Products (n 76) para 5.302.

[113] ibid para 5.302.

[114] *China – Measures Related to the Exportation of Rare Earths, Tungsten and Molybdenum*, Appellate Body Report (adopted 29 August 2014) WT/DS431/17, para 5.113.

In examining whether the privacy measure constitutes 'arbitrary or unjustifiable discrimination' or 'disguised restriction on trade', different aspects of the design, structure and implementation of the privacy measure could be informative.[115] For example, if a domestic law prevents commercial surveillance by foreign suppliers, including assembling and manipulating data for estimating market trends, but imposes no such requirement on domestic suppliers, then it qualifies as 'arbitrary or unjustifiable discrimination'. Similarly, allowing domestic suppliers to conduct extensive data analysis across their entire customer network while depriving foreign suppliers of similar benefits constitutes a 'disguised restriction on trade in services'.[116] Thus, WTO members can defend data restrictions in their privacy and data protection laws. Nonetheless, given the strictness of the above tests, they are unlikely to provide sufficient policy comfort to most countries. This is especially because of growing data sovereignty concerns, discussed in chapter one.

In conclusion, privacy-related data-restrictive measures can be theoretically scrutinised under WTO law. However, the questions raised in the legal analysis are difficult and sensitive. First, a technologically neutral interpretation of commitments contained in GATS Schedules may be unpopular with several countries, especially in the developing world. Second, in identifying the extent to which privacy compliance is relevant for and impacts competition in markets, the available evidence is neither robust nor conclusive. Third, while privacy-related measures that violate GATS can be justified under exceptions, the legal justification would require trade tribunals to scrutinise sensitive and controversial areas of domestic data regulation.

Nonetheless, WTO panels may adopt a more apolitical approach by looking at evidence specifically relating to the design and implementation of the measure, rather than the meaning and value attributed to privacy and data protection as a policy objective within a particular country. Such an approach is less threatening to countries concerned about sensitive data sovereignty concerns. But it does not provide sufficient legal certainty to all the stakeholders involved, nor does it resolve all aspects of the tension between cross-border data flows and privacy protection. As the next subsection discusses, certain PTAs and DEAs advance on WTO law to include more substantial provisions relevant to data flows and data protection.

C. Privacy and Data Protection in PTAs and DEAs

This subsection highlights key trends in provisions on cross-border data flows, data localisation and data protection in the Electronic Commerce chapters of

[115] A similar test was applied in US – Shrimp (n 81) para 156; EC – Seal Products (n 76) para 5.302.
[116] DA MacDonald and CM Streatfield, 'Personal Data Privacy and the WTO' (2014) 36(3) *Houston Journal of International Law* 629, 648 (referring to US – Gambling (n 66) para 369).

PTAs and DEAs. The Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP)[117] is often touted as a modern benchmark for digital trade rules and has informed provisions on digital trade in several PTAs. However, there are alternative models, such as the EU model (contained in EU PTAs such as the EU–New Zealand Free Trade Agreement (EU–NZ FTA)[118] and the EU–UK Trade and Cooperation Agreement (EU–UK TCA))[119] and the Chinese/Asian model (contained in the Regional Comprehensive Economic Partnership Agreement (RCEP)).[120] Most DEAs contain more extensive provisions on data protection than PTAs, as explained below.

(i) Cross-Border Data Flows and Data Localisation

Although GATS does not contain any explicit disciplines on data flows and data localisation, this trend has been changing in several recent PTAs. A dataset developed by researchers at the University of Lucerne (the TAPED (Trade Agreement Provisions on Electronic-commerce and Data) survey)[121] indicates that at least 45 PTAs contain language on cross-border data flows with 22 PTAs containing hard obligations. Further, 25 PTAs contain a separate provision prohibiting countries from imposing data localisation measures.[122]

Several PTAs borrow the language from CPTPP, Articles 14.11 and 14.13 relating to cross-border data flows and data localisation respectively.[123] CPTPP, Article 14.11.2 requires all 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 of a covered person', but the definition of 'covered person' excludes financial[124] and government services.[125] In a similar way, CPTPP, Article 14.13.2 prohibits parties from requiring a 'covered person to use or locate computing facilities in that Party's territory as a condition for

[117] Comprehensive and Progressive Agreement for Trans-Pacific Partnership (Santiago, 2018) (CPTPP).

[118] EU–New Zealand Trade Agreement (Brussels, 30 June 2022) (EU–NZ FTA).

[119] Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part (Brussels and London, 30 December 2020), (EU–UK TCA).

[120] Regional Comprehensive Economic Partnership (Hanoi, 15 November 2020) (RCEP).

[121] University of Lucerne, 'TAPED – A New Dataset on Data-related Trade Provisions', www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-director-internationalisation/research/taped/.

[122] These commitments have been undertaken by developing countries who are part of regional FTAs like the CPTPP, RCEP, USMCA and Mercosur, and select developed countries like the UK, Australia, Japan, Singapore and New Zealand.

[123] See, eg ASEAN–Hong Kong, China Free Trade Agreement (The Philippines, 12 November 2017), Art 11.7.2 (AHKFTA); Indonesia–Australia Comprehensive Economic Partnership Agreement (Jakarta, March 2019), Art 13.11.2 (IACEPA); Peru–Australia Free Trade Agreement (Canberra, 12 February 2018), Art 13.11.2 (PAFTA); SADEA, Art 23.

[124] CPTPP, Art 14.1.

[125] CPTPP, Art 14.2.3.

conducting business in that territory'. Both these obligations are subject to the non-conforming measures adopted by the parties in their GATS Schedule, ie parties can exclude these obligations to apply in certain sectors by expressly listing them.[126] Given the broad formulation of the above provisions, they cover a broad number of data transactions necessary for conducting digital trade.

The above two provisions contain a similarly worded exception enshrined in CPTPP, Articles 14.11.3 and 14.13.3 respectively, allowing parties to 'adop[t] or maintain[n]' inconsistent measures in order to achieve a 'legitimate public policy objective' (which is undefined and thus subject to open interpretation), provided that the measure: (i) is not applied in a manner that constitutes arbitrary or unjustifiable discrimination or disguised restriction on trade; and (ii) does not restrict information transfers or the location of computing facilities 'greater than required to achieve the objective'.[127] In the case of the Agreement between the United States of America, the United Mexican States, and Canada (USMCA), however, the provision on data localisation does not contain the above legitimate public policy exception.[128] Further, certain PTAs do not contain a specific carve-out for data flows in the financial sector.[129] PTAs with similarly worded provisions are seen as reflecting the US-centric approach to digital trade, although they are also common in PTAs of Latin American countries.[130]

The RCEP, which is often seen as an alternative Asian/Chinese vision of digital trade rules,[131] still follows the basic elements of the provisions on data flows and data localisation as the CPTPP. However unlike the CPTPP, the exception contains a clear self-judging element, wherein any party implementing a data-restrictive measure enjoys the sole prerogative to decide the necessity behind the legitimate public policy objective.[132] Further, the RCEP allows parties to restrict data flows or impose data localisation when the party 'considers it necessary for the protection of its essential security interests'; such a measure cannot be disputed by the other parties.[133] Another key difference is that the electronic commerce chapter of the RCEP is not subject to binding dispute settlement mechanism.

[126] CPTPP, Art 14.2.6.

[127] CPTPP, Arts 14.11.3, 14.13.3. In the USMCA, the prohibition on data localisation is not qualified with a specific exception. See USMCA, Art 19.12.

[128] USMCA, Art 19.12.

[129] See, eg AHKFTA, Arts 11.15.1–2; SADEA, Art 25.2; KSDPA, Art 14.16.

[130] For instance, the Mexico–Panama FTA was the first treaty to incorporate a binding provision on cross-border data flows. The first agreement banning data localisation was a treaty between Japan and Mongolia. See M Burri, 'Creating Data Flow Rules through Preferential Trade Agreements' in A Chander and H Sun (eds), *Data Sovereignty along the Digital Silk Road* (Oxford University Press, Forthcoming) (Copy on file with author).

[131] PL Hsieh, *New Asian Regionalism in International Economic Law* (Cambridge, Cambridge University Press, 2021) 67–100.

[132] RCEP, Arts 12.15.3(a), 12.14.3(a).

[133] RCEP, Arts 12.15.3(b), 12.14.3(b). See also IACEPA, which includes a provision wherein parties have agreed that they are not prohibited from adopting or maintaining any measures 'necessary for the protection of its essential security interests'. See IACEPA, Arts 13.11.3(b), 13.12.3(b).

In recent years, the EU has shown willingness to commit to provisions on data localisation and cross-border data flows, subject to a broad carve-out for data protection, as discussed below. For instance, the EU–UK TCA and EU–NZ FTA both prohibit parties from restricting cross-border flows by: (i) requiring the use of local computing facilities or network elements, including those that are domestically approved or certified; (ii) imposing local storage or processing requirements for data; and (iii) subjecting cross-border transfer of data to local storage requirements or use of local computing facilities or network elements.[134]

While the above developments in PTAs provide more clarity regarding data flows necessary for digital trade, certain uncertainties remain. For instance, the CPTPP exception refers to an undefined list of legitimate public policy objectives (unlike GATS, which contains a closed list) as well as explicitly borrowing the language of the chapeau and elements of the necessity test from WTO treaties (which are themselves difficult to interpret, as argued earlier in section IIIB).

(ii) Personal Information Protection

Several PTAs contain provisions on data protection, requiring parties to implement a basic regulatory framework on data protection or at least explicitly acknowledging their right to do so. As per the TAPED survey, at least 120 PTAs have commitments on data protection, with 26 of these PTAs containing hard commitments.

Both the CPTPP and the RCEP incorporate a provision requiring parties to adopt laws and regulations for the protection of personal data of users of electronic commerce.[135] However, the CPTPP encourages its parties to consider the standards and guidance of relevant international bodies in framing such laws, while the RCEP obligates the same.[136] In later treaties such as the Singapore Australia Digital Economy Agreement (SADEA) and the USMCA, the parties have agreed on examples of relevant guidelines of international bodies, namely the APEC Privacy Framework and the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines.[137]

Both the CPTPP and the RCEP provide a clarification of what is considered an adequate framework for personal information protection, providing considerable flexibility to parties to adopt different privacy laws of different quality and depth:

> For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal

[134] EU–UK TCA, Art 201; EU–NZ FTA, Art 12.4.2.
[135] CPTPP, Art 14.8.2; RCEP, Art 12.8.1.
[136] CPTPP, Art 14.8.2; RCEP, Art 12.8.2.
[137] USMCA, Art 19.8.2, SADEA, Art 17.2.

> information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.[138]

The provision on personal information protection in the CPTPP and the RCEP and similarly worded provisions in other PTAs are problematic for various reasons. First, parties could argue that the boundaries of 'legitimate public policy objective' in CPTPP, Articles 14.11.3 and 14.13.3 is circumscribed by CPTPP, Article 14.8.2. In other words, the policy space to restrict data flows on grounds of privacy will be determined by the interpretation of what constitutes a 'legal framework' for the 'protection of personal information'. Second, the provision does not provide sufficient clarity on the importance of international standards in determining the scope and applicability of CPTPP, Article 14.8.2, resulting in a low threshold for what constitutes an adequate framework for protection of personal information. For instance, 'voluntary undertakings' such as self-regulatory standards do not necessarily conform to fundamental principles in data processing.[139] Similarly, domestic laws providing ad hoc or sector-specific mechanisms may be inadequate for holistically protecting privacy of individuals. Therefore, some countries have now omitted this specific footnote,[140] or at least omitted the reference to 'voluntary undertakings', given the criticism of self-regulatory frameworks on privacy protection.[141]

However, there are certain positive developments in PTAs and DEAs as regards promoting a global framework for data protection. For instance, certain recent PTAs contain provisions that relate to the interaction of different domestic data protection frameworks when companies engage in digital trade. This includes encouraging parties to develop mutual recognition mechanisms,[142] adopting non-discriminatory practices in protecting e-commerce users from privacy violations[143] and publishing information regarding their personal information protection laws, including remedies and compliance requirements for businesses handling personal data.[144] Further, the Digital Economy Partnership Agreement (DEPA) and the USMCA are more effective in promoting a consensus on the high-level principles of data protection (collection limitation, data quality, purpose specification, use limitation, security safeguards, transparency, individual participation and accountability) that must underpin the legal framework protecting personal information.[145]

Some PTAs have also directly addressed how personal data can flow freely between countries under the existing mechanisms, such as APEC CBPR. For

[138] CPTPP, Art 14.8.2; RCEP, Art 12.8.1.
[139] G Greenleaf, 'APEC's Privacy Framework: A New Low Standard' (2005) 11(5) *Privacy Law and Policy Reporter* 121.
[140] See, eg AHKFTA, Art 11.9.2; IACEPA, Art 13.7.2; PAFTA, Art 13.8.2.
[141] See, eg UKSDEA, Art 8.61.E(2).
[142] See, eg AHKFTA, Art 11.9.5; IACEPA, Art 13.7.4; PAFTA, Art 13.8.5; CPTPP, Art 14.8.5.
[143] See, eg AHKFTA, Art 11.9.3; IACEPA, Art 13.7.3; PAFTA, Art 13.8.4; CPTPP, Art 14.8.4.
[144] See, eg AHKFTA, Art 11.9.4; IACEPA, Art 13.10.2.
[145] DEPA, Art 4.2.3: USMCA Art 19.8.3.

instance, in SADEA, parties have recognised that the APEC CBPR is a 'valid mechanism to facilitate cross-border information transfers while protecting personal information'.[146] The DEPA also obligates parties to 'pursue the development of mechanisms to promote compatibility and interoperability' between their respective regimes.[147] These are stronger requirements than the relevant provisions in the CPTPP and similarly worded PTAs, which recognise that parties should promote compatibility between their privacy regimes but do not have any mechanism to operationalise it.[148]

EU PTAs generally adopt the most defensive and cautious approach to data protection. For instance, the EU–UK TCA and the EU–NZ FTA state that parties enjoy an unqualified right to maintain measures for personal data protection and privacy, including during cross-border data transfers, provided that these measures are of 'general application'.[149] This essentially means that, irrespective of the nature of data restrictions contained in a data protection framework and its trade-restrictive impact, the domestic data protection law is immune from dispute settlement under the PTA. Effectively, this means that any provision in the GDPR cannot be challenged under the PTA. While this provision was introduced to preserve privacy,[150] it can help a party justify strong government controls over personal data or protectionist measures as long as it is disguised as a data protection law.

Conclusively, several PTAs advance on WTO disciplines by explicitly recognising the role of privacy and data protection disciplines for digital trade. However, they suffer from limitations. For instance, several PTAs do not identify clear international benchmarks on data protection. Further, the exceptions contained in many PTAs do not provide clear answers regarding the addressing of trade disputes on data-restrictive measures. Certain DEAs proactively bring together privacy and trade rules under one umbrella. For instance, they create more consensus between parties regarding high-level principles of data protection and foster agreement on common frameworks to enable cross-border transfer of personal data by incorporating OECD principles and APEC instruments by reference. While these DEAs are currently limited to smaller liberal economies, China[151] and the EU[152] have both shown

[146] SADEA, Art 17.8. See also KSDPA, Art 14.17.8.

[147] DEPA, Art 4.2.6.

[148] CPTPP, Art 14.8.5.

[149] EU–UK TCA, Art 202; EU–New Zealand Trade Agreement (Brussels, 30 June 2022), Art 12.5 (EU–NZ FTA).

[150] European Data Protection Supervisor, 'Data Protection is Non-negotiable in International Trade Agreements' (22 February 2021) www.edps.europa.eu/press-publications/press-news/press-releases/2021/data-protection-non-negotiable-international_en.

[151] 'China Keen to Join Digital Economy Partnership Agreement: Commerce Minister' (Xinhua, 27 May 2023) www.english.www.gov.cn/news/202305/27/content_WS6471c869c6d03ffcca6ed733.html.

[152] European Commission, 'Recommendation for a Council Decision Authorising the Opening of Negotiations for Digital Trade Disciplines with the Republic of Korea and with Singapore' COM(2023) 230 final, SWD(2023) 85 final.

interest in them. Greater engagement and participation in such DEAs could potentially help address some of the lingering tensions between trade law and data protection/privacy.

IV. ALIGNING INTERNATIONAL TRADE LAW WITH PRIVACY GOVERNANCE

The discussion in the previous section indicates that international trade law has evolved to some extent to address the interface between digital trade and privacy. Nonetheless, international trade agreements were not designed specifically to address privacy and data protection issues, and would thus be an inappropriate forum to determine the normative foundations or standards of data privacy. Further, international trade law currently provides few avenues to acknowledge and incorporate emerging multistakeholder standards, norms and best practices on data governance by reference. This section therefore examines the extent to which international trade agreements can and should be reformed to better align digital trade and privacy protection. It begins by setting out an overview of the various global responses to privacy and data protection concerns, particularly in the context of cross-border data flows.

The section then explores various ways in which international trade law can respond to and, to the extent feasible, co-opt the multilayered and multistakeholder nature of privacy and data protection in global data governance.[153] First, the section argues that even within the existing framework in WTO law and PTAs, the existing provisions can be read more meaningfully in disciplining unnecessarily restrictive measures and achieve at least some degree of consensus on the implementation of data protection laws. Second, the section envisages a more proactive role for international trade law in contributing to a transnational framework for cross-border data flows by incorporating relevant normative privacy and data protection frameworks by reference, particularly through bottom-up experimentation under DEAs. It also proposes a possible non-binding WTO declaration containing core aspects of data protection and privacy under the ongoing plurilateral initiative on e-commerce. Third, the section proposes institutional innovations to increase potential avenues for cooperation among various stakeholders to develop interoperable frameworks and mechanisms for personal data flows, and to facilitate regulatory coordination between the WTO and other relevant fora such as the Global Privacy Assembly, APEC and the OECD.

[153] L DeNardis, *The Internet in Everything: Freedom and Security in a World with No Off Switch* (New Haven, Yale University Press, 2020) 84, 88.

A. International and Transnational Frameworks for Personal Data Protection and Cross-Border Data Flows

So far, this chapter has focused on the interface between international trade law and data protection laws adopted at the domestic level. However, various other international instruments and regulatory frameworks also address data protection and privacy. As Peng argues, the public–private interface often lies at the heart of privacy regulation; however, these relationships are often not contextualised in international trade law.[154] One of the key motivations behind these instruments is achieving some kind of high-level consensus to foster a stronger global framework for regional or international data protection.

The most significant treaty on personal data protection is the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,[155] consisting of all members of the Council of Europe and a few other countries. This treaty was modernised in 2018 to address new regulatory concerns pertaining to artificial intelligence. While it is outside the scope of this chapter to discuss all the details of the treaty, its Preamble recognises the role of personal data flowing across borders. Further, Article 14(2) provides that parties should not prohibit or restrict transborder personal data flows 'for the sole purpose of the protection of privacy'. It does, though, allow derogations if automated data processing in a foreign country would prohibit an equivalent level of protection of personal data or where the transfer is made from a non-contracting state through the intermediary of a party as a means of circumventing requirements for transborder personal data flows contained in the domestic law.[156] This treaty, however, does not specify any mechanisms for facilitating personal data flows and is also less relevant outside Europe.

Regional organisations such as the OECD and APEC provide more specific solutions for personal data transfers. The OECD, which is an intergovernmental organisation working on stimulating economic progress and trade, recognises the importance of 'consistency and effectiveness in privacy protection' at a 'global level' as 'good practice' in Internet governance.[157] The OECD has adopted the OECD Privacy Guidelines, which contains implementation guidelines for its members, including the development of national privacy strategies alongside the adoption of privacy laws and enforcement mechanisms.[158] One of the key

[154] See generally S Peng, 'Public–Private Interactions in Privacy Governance' (2022) 11(6) *Laws* 80.

[155] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108, Strasbourg, 28 January 1981) (Convention on Personal Data).

[156] Convention on Personal Data, Art 14(3).

[157] OECD, 'Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data' (2013) C(80)58/FINAL, as amended by C(2013)79, 2013) (OECD Privacy Guidelines).

[158] OECD Privacy Guidelines, Art 19.

objectives of this framework is to ensure that privacy laws do not become a tool for protectionism.[159] The OECD has also published recommendations on cross-border cooperation for the enforcement of privacy laws.[160] One of them is to constitute an informal network of privacy regulators to facilitate cross-border enforcement of privacy laws.[161] Similar initiatives and proposals are currently also being discussed within the Global Privacy Assembly, as explained below.

Similar to the OECD framework, APEC countries have adopted a voluntary 'privacy framework', the APEC Privacy Framework, which 'recogniz[es] the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and economic growth in the APEC region'.[162] One of the most notable contributions of APEC in the context of digital trade was the development of the CBPR framework and the Privacy Recognition for Processors (PRP), with the aim of navigating the 'fluidity of interactions across public and private governance realms' in privacy regulation.[163] The CBPR is essentially a certification system provided to companies that comply with certain basic standards of data protection set out in the APEC Privacy Framework.[164] These certifications are awarded by government-approved accountability agents. The PRP is a certification system designed especially for data processors (ie companies acting on behalf of data controllers) with the ability to implement the standards required of data controllers.[165]

Regional bodies such as the Association of Southeast Asian Nations (ASEAN)[166] and the African Union[167] have also been working towards developing a common framework for data protection and personal data flows. The Ibero-American Data Protection Network is in the process of developing contractual clauses for personal data flows.[168]

[159] Bygrave, *Data Privacy Law* (n 18) 44.

[160] OECD, 'Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy' (2007).

[161] GPEN, 'Action Plan for the Global Privacy Enforcement Network' () www.privacyenforcement.net/content/action-plan-global-privacy-enforcement-network-gpen.

[162] APEC, 'APEC Privacy Framework' (November 2004) (APEC Privacy Framework). See also Bygrave (n 18) 77.

[163] See generally Peng, 'Public–Private Interactions in Privacy Governance' (n 155) 2.

[164] APEC, 'What is the Cross-Border Privacy Rules System', www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System.

[165] Infocomm Media Development Authority, 'About the APEC Privacy Recognition for Processors (PRP) System', www.imda.gov.sg/how-we-can-help/privacy-recognition-for-processors-certification.

[166] ASEAN, 'ASEAN Model Contractual Clauses for Cross Border Data Flows' (2nd ASEAN Digital Senior Officials' Meeting, January 2021).

[167] M King'ori, 'The African Union's Data Policy Framework: Context, Key Takeaways, and Implications for Data Protection on the Continent' (Future Privacy Forum, 29 March 2023) www.fpf.org/blog/the-african-unions-data-policy-framework-context-key-takeaways-and-implications-for-data-protection-on-the-continent/.

[168] G Cervio et al, 'Multijurisdiction: Ibero-American Network for the Protection of Personal Data – Standard Contractual Clauses for the International Transfer of Personal Data' (*Global Compliance News*, 23 October 2022) www.globalcompliancenews.com/2022/10/23/multijurisdiction-ibero-american-network-for-the-protection-of-personal-data-standard-contractual-clauses-for-the-internal_10232022/.

The most important transnational regulatory network working towards developing a global framework for data protection and privacy is the Global Privacy Assembly (GPA). It consists of more than 130 data protection and privacy authorities from across the globe, working on various initiatives on the convergence of principles on many issues, including open and secure flows of personal data.[169] The GPA issues various recommendations, resolutions and guidelines on data protection, several of which also deal with complex data protection issues arising with the emergence of modern digital technologies. It is evolving as one of the most important sites for developing transnational consensus on data protection issues.

The above developments present a contrasting picture for the global regulatory framework on data protection. While, on the one hand, we see more regulatory fragmentation resulting from the implementation of varied domestic laws, we also see a degree of consolidated effort to develop a transnational consensus on certain high-level principles of data protection and personal data flows. This diversity of frameworks suggests that a potential solution to address privacy concerns on a global scale is possible by working towards a multilayered framework, involving different stakeholders at different levels of governance and co-opting different norms, best practices and standards emerging in relevant multistakeholder and transnational fora.

B. Relevance of WTO Rules for Privacy Protection

As argued earlier, the multilateral WTO framework does not per se contain rules that boost global privacy and data protection. In particular, the application of WTO law to privacy-related measures requires panels to balance trade obligations with a country's domestic values on data privacy, irrespective of whether those values align with international standards and best practices. Recent PTAs adopt a different approach by including more elaborate provisions relating to privacy protection (see the discussion in the next section). Nonetheless, the existing WTO rules can still be relevant in addressing certain frictions between cross-border data flows and data privacy.

For instance, GATS, Article VII can potentially encourage countries to develop interoperability between their domestic regulatory frameworks. I will take as an example an agreement between two countries that provides a certification mechanism to enable cross-border transfer of personal data. Under GATS, Article VII:2, if a member recognises licences or certifications granted to service suppliers of another member either through a process of harmonisation or a mutual agreement, it must provide 'adequate opportunity' to all other members to negotiate similar/comparable recognition agreements. For instance, the newly

[169] Global Privacy Assembly, 'Mission and Vision', www.globalprivacyassembly.org/.

negotiated EU–US Privacy Framework provides a mechanism to all US digital service suppliers to self-certify that their data operations are GDPR-compliant, thereby enabling them to transfer personal data of EU residents to their US servers. Another country with a data protection regulatory framework similar to or more robust than that of the USA can potentially argue under Article VII that the EU must provide them with an adequate opportunity (ie similar to that of the USA) to negotiate an arrangement for personal data transfer.

Further, an instrument such as the EU–US Privacy Framework (or its predecessor, the now-invalidated EU–US Privacy Shield) could violate GATS, Article VII:3:

> A Member shall not accord recognition in a manner which would constitute a means of discrimination between countries in the application of its standards or criteria for the authorization, licensing or certification of services suppliers, or a disguised restriction on trade in services.

This is because several countries have regulatory frameworks comparable to that of the USA (for example, most APEC members follow the APEC Privacy Framework, like the USA). Thus, the aggrieved country could argue how its regulatory framework is similar to or stronger than that of the USA and that its digital service suppliers have sufficient resources to self-certify that their data processing practices are GDPR-compliant (similar to what used to happen under the Privacy Shield).

The disciplines on domestic regulation contained in GATS, Article VI can also be relevant in addressing certain burdensome technical standards or licensing requirements contained in domestic data protection laws. For example, where WTO members require digital service suppliers to obtain licences or authorisation for cross-border data transfers (assuming the members have committed to keep these services open to foreign services or service members suppliers in their GATS Schedule), such applications should be assessed in a fair and objective manner.[170] WTO panels can also examine if specific privacy standards imposed by members in such sectors are consistent with relevant international standards.[171] However, such panels are unlikely to consider private or multistakeholder standards developed in Internet technical bodies as they do not qualify as 'relevant international standards of international organizations' under GATS, Article VI.

Finally, as discussed previously in section IIIB, the various exceptions in international trade treaties allow members to adopt measures necessary to achieve domestic privacy-related policy objectives, even if those measures violate certain obligations. These exceptions can be helpful in distinguishing privacy measures genuinely aimed at protecting the privacy of individuals or achieving higher

[170] GATS, Art VI:1.
[171] GATS, Art VI:5 read with Art VI:4.

standards of data protection than those protecting domestic digital service suppliers. For a holistic application of the necessity test under the exceptions, trade tribunals can and should adopt a multidimensional approach in assessing the necessity of privacy-related data-restrictive measures. For example, experts from the Internet technical community could help understand the logic and the technical impact of a privacy-related measure.[172] Several experts have argued that data-restrictive measures generally interfere with the open architecture of the Internet and fail to protect Internet privacy transnationally.[173] Experts also typically support market-driven privacy technologies and standards over prescriptive domestic standards as the former are more robust and effective in dealing with cyber-risks.[174] Such technical inputs can be helpful in examining the necessity of privacy-related data-restrictive measures.

C. Developing a Transnational Framework for Personal Data Flows in International Trade Law

The multilateral framework of the WTO currently makes a limited contribution to enabling a transnational framework for data privacy. However, some PTAs mark a clear move in a different direction as countries are increasingly showing openness towards undertaking substantive obligations on developing frameworks on data protection consistent with international benchmarks and standards. This section identifies how international trade agreements can both normatively and institutionally create a culture of transnational data protection.

The first aspect in developing a transnational framework is identifying the relevant normative framework necessary to enable cross-border flows of personal data. Rather than aiming for harmonisation (eg all countries adopt the GDPR framework), a more robust and sustainable approach would be to formulate high-level principles for data protection. These principles need not be determined by trade bodies but can evolve in appropriate regional or global fora (APEC, the OECD, ASEAN and the African Union are potential examples). Dialogues between regional fora may also lead to more long-term interoperability.[175] International trade law can acknowledge and incorporate these principles by

[172] Gasser (n 91) 68.

[173] D Broeders, 'Aligning the International Protection of "the Public Core of the Internet" with State Sovereignty and National Security' (2017) 2(3) *Journal of Cyber Policy* 366, 367–69; L DeNardis et al, 'The Rising Geopolitics of Internet Governance: Cyber Sovereignty v Distributed Governance' (paper presented at Columbia SIPS Tech & Policy Initiative, Columbia SIPA, November 2016) 14–15.

[174] See, eg S Baird, 'The Government at the Standards Bazaar' in L DeNardis (ed), *Opening Standards: The Global Politics of Interoperability* (Cambridge MA, MIT Press, 2011) 13, 18, 19; R Ghosh, 'An Economic Basis for Open Standards' in DeNardis, *Opening Standards* (idem) 75, 76; DeNardis et al (n 173) 17.

[175] A proposal was made in 2017 to find greater alignment between BCRs and the APEC CBPR mechanism, both of which enable intra-company transfers of personal data. See European

reference, as in the cases of the DEPA and the USMCA. In other words, trade treaties do not specifically determine how countries implement or enforce data protection laws, but instead set out high-level principles that must guide them in developing their domestic framework. Further, as discussed earlier, DEAs contain requirements for developing interoperability of different regulatory frameworks on data protection, including privacy trustmarks.

In terms of finding a long-term solution to some of the problems entailing global data transfers, the multilateral framework of the WTO could also be relevant. Some scholars have proposed that WTO members can develop a non-binding framework setting out high-level principles of data regulation that must guide those members in developing their domestic data laws and regulations. These guidelines could take the form of a declaration under the ongoing plurilateral joint initiative discussions on e-commerce. The other alternative could be a Reference Paper specific to data flows, modelled on similar lines as the Reference Paper on Telecommunications Services, which could be voluntarily adopted by countries in developing GATS commitments on telecommunications services. This Reference Paper could incorporate the prevailing international and multistakeholder best practices and norms on cross-border data flows, but would leave it to each country to implement this in practice. Such a framework could provide a foundation necessary for implementing provisions on data flows and data localisation in a balanced manner, and could help countries navigate the trade-off between protecting regulatory autonomy and promoting interoperable data protection laws.

In developing these common frameworks or guidelines, trade bodies must adopt an approach that is different from negotiating binding provisions.[176] For instance, as discussed earlier, recent DEAs contain several provisions taking the form of digital cooperation agreements and instruments of digital diplomacy rather than binding provisions based on difficult trade-offs and concessions. This is more supportive of a robust framework for global data governance that, in turn, can facilitate digital trade flows.

The second element of the transnational framework is finding the appropriate institutional response to several of the cross-border data governance challenges. As the discussion in section IVA indicates, several global bodies exist that bring different perspectives and regulatory styles to global privacy governance. This indicates that the institutional response to data protection and privacy issues must be multilayered. This is quite an unusual model for the WTO and trade bodies, but is increasingly necessary for global data governance. Therefore, it is important for trade bodies to develop new forms of cooperation with global multistakeholder bodies and transnational regulatory frameworks working on relevant aspects of data protection and privacy.

Commission, 'Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World' COM/2017/07 final, 11.

[176] For further discussion on the necessary instrumentalities, see ch 7.

As a hypothetical example, in the development of the Reference Paper for Data Flows, it may be helpful to engage in repeated consultations with the OECD, GPA and certain relevant UN agencies in identifying the principles. Similarly, especially under the PTAs, parties can better engage in the relevant committees constituted under the treaty to explore co-regulatory approaches, such as an approved code of conduct for personal data transfer or developing practical pre-approved standard contractual clauses. Another potentially critical area of co-regulation is standard-setting for implementing privacy-compliant technologies. In that regard, the role of private and multistakeholder standard-setting bodies is critical, and compliance with internationally recognised privacy standards is essential to create an optimal environment for digital trade.[177] In the next chapter, I discuss how international trade law can accommodate developments in relevant private and multistakeholder standard-setting bodies.

V. CONCLUSION

International trade law and privacy protection appear opposed to each other at first sight. However, this chapter has argued that this conflict is neither necessary nor meaningful for either digital trade or global data governance. After examining the various ways in which existing data restrictions contained in data protection laws conflict with international trade law, this chapter proposed various means to increase alignment between these two fields of regulation. In particular, by increasing flexibilities in trade treaties for incorporating transnational and multistakeholder norms and standards on data protection as well as acknowledging the relevance of evolving transnational mechanisms for personal data transfers, the trade–privacy dilemma can be resolved to a considerable extent. While the proposed solutions are not perfect, they provide a pragmatic response in addressing the typical restraints faced by different entities engaging in global digital trade.

In developing a common framework for personal data flows across borders, the chapter has cautioned against following a one-size-fits-all approach. It has also identified the limitations of attributing a privacy regulation role to trade bodies. It has argued that, as an alternative, a multilayered approach that incentivises trade bodies to develop institutional engagement with relevant multilateral, multistakeholder and transnational regulatory frameworks dealing with different aspects of privacy protection would be more feasible. This approach is more sustainable and can gradually help develop more interoperable solutions to enable personal data transfers necessary for digital trade, while continuing to respect the differences in privacy culture across countries.

[177] For instance, countries may require all cloud service providers to follow ISO/IEC 27018, an internationally recognised standard for cloud privacy. This may be more effective at protecting privacy and far less trade restrictive than imposing a domestic standard that may be incompatible with international standards.

3

The Emerging Dimensions of Digital Trade and Cybersecurity

I. INTRODUCTION

Cybersecurity is possibly the fastest expanding policy area in global data governance today. Several governments now consider cybersecurity to extend well beyond the technical aspects of network and data security to include national security, economic security and even social order/stability. Cybersecurity is critical for all digital transactions. For instance, data breaches and cybercrimes are common roadblocks to digital trade and lead to systemic trust deficit across the entire digital ecosystem.[1] Further, cybersecurity is increasingly important from the perspective of cyber-physical infrastructure, including the defence mechanisms necessary to protect data infrastructure, network cables and other physical components underlying the digital economy such as smart devices.[2]

Not unexpectedly, to address the multifaceted nature of cybersecurity, the measures implemented by governments vary significantly, ranging from exercising tight control over foreign investments in data-driven sectors[3] to strict requirements regarding how data is stored and encrypted,[4] and even to imposing

[1] See, eg S Simpson, '2019 CIGI–Ipsos Global Survey on Internet Security and Trust' (Ipsos, 12 June 2019) www.ipsos.com/en/2019-cigi-ipsos-global-survey-internet-security-and-trust; K Huang et al, 'The Devastating Business Impacts of a Cyber Breach' (HBR, 4 May 2023) www.hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach; H Heyburn et al, 'Analysis of the Full Costs of Cyber Security Breaches' (Ipsos MORI, 2020).

[2] See generally L DeNardis and M Raymond, 'The Internet of Things as a Global Policy Frontier' (2017) 51(2) *UC Davis Law Review* 475.

[3] See, eg The White House, 'Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States' (15 September 2022) EO 14083. See also L Knight and T Voon, 'The Evolution of National Security at the Interface Between Domestic and International Investment Law and Policy: The Role of China' (2020) 21(1) *Journal of World Investment & Trade* 104.

[4] See, eg B Goodwin, 'Online Safety Bill Could Pose Risk to Encryption Technology Used by Ukraine' (*Computer Weekly*, 20 April 2023) www.computerweekly.com/news/365535563/Online-Safety-Bill-could-pose-risk-to-encryption-technology-used-by-Ukraine; National People's Congress, 'Cybersecurity Law of the People's Republic of China [中华人民共和国网络安全法]' (7 November 2016) (Chinese Cybersecurity Law); Law No 24/2018/QH14 on Cybsersecurity' (12 June 2018) (Vietnamese Cybersecurity Law).

cyber-sanctions in the face of an imminent threat.[5] Further, at least for certain governments, cybersecurity now entails not only cyber-defence, but also cyber-offence mechanisms to safeguard vital security and strategic interests of the country.[6]

A unique feature of cybersecurity governance is the critical role of the private sector in different aspects, such as developing and implementing cybersecurity standards,[7] executing requirements of security-by-design,[8] collaborating with governments in the development of best practices on cybersecurity[9] and detection of cyber-threats,[10] and contributing to the development of norms in cybersecurity.[11] While some governments have been open to involving the private sector in developing norms and standards for cybersecurity,[12] others have taken a more defensive role in accommodating the private sector.[13]

Given the expanding scope and depth of cybersecurity and the involvement of both states and the private sector, the interface between digital trade and cybersecurity entails many complex legal and policy concerns. This chapter specifically focuses on the interface between international trade agreements and cybersecurity from the perspective of cross-border data flows. Like in the previous chapter, I focus on two questions in this chapter: (i) does international trade

[5] See various examples discussed in MV Callo-Müller and I Bogdanova, 'Unilateral Cyber Sanctions and Global Cybersecurity Law-Making' (OpinioJuris, 24 January 2022) www.opiniojuris.org/2022/01/24/unilateral-cyber-sanctions-and-global-cybersecurity-law-making/.

[6] M Willett, 'Offensive Cyber and the Responsible Use of Cyber Power' (IISS, 02 March 2023) www.iiss.org/en/online-analysis/online-analysis/2023/03/offensive-cyber-and-the-responsible-use-of-cyber-power/.

[7] P Kirvan and J Granneman, 'Top 10 IT Security Frameworks and Standards Explained' (TechTarget, Decmber 2021) www.TechTarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one; see generally K Karachalios and K McCabe, 'Standards, Innovation, and Their Role in the Context of the World Trade Organization' (E15 Initiative, December 2013) www.e15initiative.org/wp-content/uploads/2015/09/E15-Innovation-KarachaliosMcCabe-FINAL.pdf.

[8] See generally, Cybersecurity and Infrastructure Security Agency, 'Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default' (13 April 2023).

[9] See, eg National Institute of Standards and Technology, 'Framework for Improving Critical Infrastructure Cybersecurity' (v 1.1, 16 April 2018).

[10] See, eg J Krenz, 'Boosting Microsoft's Response to Cybersecurity Attacks with Microsoft Sentinel' (Microsoft, 30 May 2023) www.microsoft.com/insidetrack/blog/boosting-microsofts-response-to-cybersecurity-attacks-with-microsoft-azure-sentinel/; '5 Ways to Detect a Cyber Attack' (*HuffPost*, 30 January 2017) www.huffpost.com/archive/ca/entry/5-ways-to-detect-a-cyber-attack_n_13880814.

[11] See generally C Glen, 'Norm Entrepreneurship in Global Cybersecurity' (2021) 49(5) *Politics & Policy* 1121.

[12] P Gallagher, 'The Partnership between NIST and the Private Sector: Improving Cybersecurity' (NIST, 25 July 2013) www.nist.gov/speech-testimony/partnership-between-nist-and-private-sector-improving-cybersecurity; S Peng, '"Private" Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime' (2018) 51(2) *Cornell International Law Journal* 445, 451.

[13] See, eg A Qi et al, 'Assessing China's Cybersecurity Law' (2018) 34(6) *Computer Law & Security Review* 1342; A Kiet, 'Vietnam Tightens National Sovereignty Protection in Cyberspace' (Hanoi Times, 9 December 2021) www.hanoitimes.vn/vietnam-tightens-national-sovereignty-protection-in-cyberspace-319495.html; M Soliman, 'In the Middle East, Cyber Sovereignty Hampers Economic Diversification' (Middle East Institute, 6 January 2021) www.mei.edu/publications/middle-east-cyber-sovereignty-hampers-economic-diversification.

law apply to data-restrictive measures imposed on the grounds of cybersecurity protection?; and (ii) can international trade law play a more contributory role in creating a global framework for cybersecurity protection necessary to enable global digital trade flows?

In addressing the above questions, the chapter focuses specifically on data-restrictive measures pertaining to cybersecurity, such as data localisation,[14] security reviews and regulatory approvals for cross-border data transfers,[15] and outright bans on certain digital services.[16] This chapter looks at relevant rules contained in the General Agreement on Trade in Services (GATS) and digital trade chapters in preferential trade agreements (PTAs) and digital economy agreements (DEAs). Cybersecurity regulation also interfaces with treaties relevant to trade in goods, such as the General Agreement on Tariffs and Trade (GATT) and the Agreement on Technical Barriers to Trade (TBT Agreement),[17] which is outside the scope of this chapter.

Section II begins by highlighting how the meaning of cybersecurity is evolving in global data governance and its impact on digital trade. With the rapid digitalisation of the economy, cybersecurity concerns (covering both digital data and the networks/infrastructure carrying it) have increased at a dramatic rate. Several studies indicate the massive losses to the digital economy occurring from various kinds of cybercrimes and cyberattacks. Thus, cybersecurity protection is central to enabling digital trade flows. However, as cybersecurity is increasingly associated with several national/economic security concerns, governments are more actively regulating cyber-risks, including by imposing data-restrictive measures in domestic laws and regulations. These measures can restrict digital trade, so a dilemma now exists between addressing digital trade barriers and safeguarding the domestic policy space for cybersecurity regulation.

Considering this digital trade–cybersecurity dilemma, section III evaluates how existing rules contained in World Trade Organization (WTO) law (specifically, GATS) and PTAs apply to cybersecurity measures. Like in the previous chapter, I find that measures restricting cross-border data flows on the grounds of cybersecurity can violate obligations in GATS and PTAs. However, most governments are likely to justify such measures in the exceptions contained in trade treaties. Both the general and security exceptions can be relevant in this regard. The application of the legal tests contained in these exceptions, especially under

[14] See, eg Chinese Cybersecurity Law 2016, Art 37; Vietnamese Cybersecurity Law 2018, Art 43.1.

[15] See, eg Central Cyberspace Affairs Commission, 'Measures for Data Export Security Assessment [数据出境安全评估办法]' (7 July 2022); A Huld, 'Cross-Border Data Transfer – New Measures Clarify Security Review Requirements' (*China Briefing*, 11 July 2022) www.china-briefing.com/news/cross-border-data-transfer-new-measures-offer-clarification-on-security-review/.

[16] See, eg US Department of Homeland Security, 'DHS Statement on the Issuance of Binding Operational Directive 17-01' (13 September 2017), www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17–01; The White House, 'Executive Order on Securing the Information and Communications Technology and Services Supply Chain' (15 May 2019) EO 13873.

[17] Agreement on Technical Barriers to Trade (Uruguay, April 1994) (TBT Agreement).

WTO law, raise several difficult questions regarding technical efficacy of specific data-restrictive measures and objectively evaluating the cyber-risk preferences of individual governments. Further, the invocation of security exceptions for defending cybersecurity-related measures raises sensitive questions of data sovereignty and national security, and can thus lead to political tensions in trade bodies. This section also highlights cybersecurity-related disciplines in PTAs.

Given the potential conflict between international trade law and cybersecurity governance, section IV investigates the possibility of better alignment between digital trade rules and cybersecurity governance. Cybersecurity is not only a domestic policy concern, but also (more importantly) a transnational one. It is necessary to contextualise this perspective in international trade law. At first sight, trade rules can be relied upon to distinguish between protectionist and genuine cybersecurity-related data-restrictive measures. However, existing trade rules are insufficient, given that governments associate cybersecurity measures with a wide range of sensitive political concerns.

To fill these gaps, section IV proposes various ways in which international trade law can play a more facilitative role in promoting a global/transnational regulatory culture for cybersecurity governance. First, it proposes new mechanisms for transparent reporting and deliberations on cybersecurity-related measures in trade bodies. Second, it emphasises the possibility of developing a new framework in digital trade law that allows trade tribunals to consider a broader suite of relevant and high-quality multistakeholder and private standards on cybersecurity regulation. Third, it proposes that trade rules must provide avenues to incorporate global best practices and norms on cybersecurity regulation by reference. It is especially important to build this multilayered framework as trade bodies cannot and should not act as cybersecurity regulatory bodies.

II. CYBERSECURITY, DIGITAL TRADE AND DATA FLOWS

This section highlights the expansive meaning of cybersecurity in domestic and global data governance, then explores how that impacts cross-border data flows. Cybersecurity has traditionally referred to technical dimensions of data and network security, but governments increasingly associate cybersecurity with political and economic concerns and seek to regulate more aggressively on cybersecurity-related matters. While, on the one hand, cybersecurity is critical for digital trade flows, stringent domestic regulation of cybersecurity can curtail digital trade. This leads to what this section terms a 'digital trade–cybersecurity dilemma'.[18]

[18] A similar expression was used by the author in a previous article. See N Mishra, 'The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance' (2020) 54(4) *Journal of World Trade* 567.

A. The Expanding Contours of Cybersecurity

From a technical perspective, cybersecurity has been defined as the confidentiality, integrity and availability of data, as well as the networks and computer systems containing, communicating/carrying and processing that data.[19] Thus, cybersecurity considerations are relevant in designing both the protocols underlying the digital networks and the various digital services and applications that use data.[20] Cybersecurity standards can relate to a variety of objectives, from managing data and networks to protecting them from security failures.[21] Sometimes other terms such as 'digital security', 'data security' and 'information security' are used interchangeably with cybersecurity.[22]

The importance of cybersecurity is recognised in various international instruments and declarations. Currently, the most prominent treaty dealing with aspects of cybersecurity is the Budapest Convention, which was proposed by the Council of Europe in 2001 and has since been signed by 68 countries.[23] This treaty requires all parties to adopt laws and regulations to deal with various cyber-offences affecting the confidentiality, integrity and availability of data.[24] The treaty has two additional protocols: the first deals with the criminalisation of racist and xenophobic activities committed through computer systems,[25] the second with cooperation between countries in relation to electronic evidence.[26] However, several developing countries have refused to sign this treaty for both lack of representativeness and concerns about provisions that might interfere with domestic sovereignty.[27]

[19] This definition is developed by looking at the definition of 'cybersecurity' in Department of Foreign Affairs and Trade, Australia, 'Australia's International Cyber Engagement Strategy' (October 2017) 23; Convention on Cybercrime (ETS No 185, Budapest, 23 November 2001), Preamble (Budapest Convention). See also J Kosseff, 'Defining Cybersecurity Law' (2018) 103(3) *Iowa Law Review* 985, 1010.

[20] See generally M Finnemore and DB Hollis, 'Constructing Norms for Global Cybersecurity' (2016) 110(3) *American Journal of International Law* 425, 431; DB Hollis, 'An e-SOS for Cyberspace' (2011) 52(2) *Harvard International Law Journal* 373, 380; DeNardis and Raymond (n 2).

[21] Peng (n 12) 446.

[22] See, eg OECD, 'Economic and Social Benefits of Internet Openness' (2016) OECD Digital Economy Papers No 257, 28; OECD, 'Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document' (1 October 2015)19–20.

[23] Council of Europe, 'Chart of Signatures and Ratifications of Treaty 185', www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=exhG7iJ7.

[24] See, eg Budapest Convention, Arts 2–10.

[25] Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (Strasbourg, 28 January 2003) ETS No 189.

[26] Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (ETS No 224, Strasbourg, 12 May 2022).

[27] A Seger, 'India and the Budapest Convention: Why Not?' (ORF, 20 October 2016) www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/; M Fidler, 'South Africa Introduces Revised Cybercrime Legislation, Acknowledging Criticism' (*CFR Blog*, 07 March 2017) www.cfr.org/blog/south-africa-introduces-revised-cybercrime-legislation-acknowledging-criticism; A Peters, 'Russia and China Are Trying to Set the U.N.'s Rules on Cybercrime' (*FP*, 17 October 2016) https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/.

A new treaty on cybercrimes is currently being negotiated under the aegis of the United Nations.[28] Further, discussions on cybersecurity are ongoing at the UN Open Ended Working Group, in addition to the previous work done by the UN Governmental Group of Experts in discussing the role of international law in cybersecurity.[29] Other regional bodies, such as the African Union[30] and the Arab League,[31] have adopted treaties related to cybersecurity and cybercrimes. Declarations related to cybersecurity have been adopted by various international and regional bodies, such as the Organisation for Economic Co-operation and Development (OECD),[32] G20,[33] Asia-Pacific Economic Cooperation (APEC)[34] and G7.[35]

While there is consensus internationally on the need for a global framework for cybersecurity, there are diverging views regarding the role of states and other stakeholders in the regulation of cybersecurity. For instance, in several international fora, concerns have been raised regarding the preservation of sovereign control over digital space to address cybersecurity and other law enforcement concerns.[36] These differences are particularly magnified because the meaning of cybersecurity is understood very differently across countries. One such example is laws relating to protection of critical infrastructure from cyberattacks, where governments do not draw a clear distinction between technical and political security.[37]

Further, cybersecurity regulation can relate to the growth of the domestic digital economy.[38] This is reflected in a broad variety of inward-looking

[28] UNODC, 'Consolidated Negotiating Document on the General Provisions and the Provisions on Criminalization and on Procedural Measures and Law Enforcement of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes' (Vienna, 9–20 January 2023).

[29] UNGA, 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security – Note by the Secretary-General' (14 July 2021) UN Doc A/76/135.

[30] African Union Convention on Cyber Security and Personal Data Protection (Malabo, 27 June 2014).

[31] Arab Convention on Combating Information Technology Offences (Cairo, 21 December 2010).

[32] OECD, 'Digital Security Risk Management' (n 22); OECD, 'Recommendation of the Council on the Protection of Critical Information Infrastructures' (30 April 2008) C(2008)35; OECD, 'Recommendation of the Council Concerning Guidelines for Cryptography Policy' (27 March 1997) C(97)62/FINAL.

[33] G20, 'G20 Ministerial Statement on Trade and Digital Economy' (Tsukuba City, 8–9 June 2019), paras 25–27.

[34] APEC, 'APEC Cybersecurity Strategy' (2002) Doc No telwg26/BFSG/22.

[35] G7, 'Declaration on Responsible States Behaviour in Cyberspace' (Lucca, 11 April 2017).

[36] See, eg UNGA, 'Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General' (14 September 2011) UN Doc A/66/359.

[37] D Broeders, *The Public Core of the Internet: Towards an International Agenda for Internet Governance* (Amsterdam, Amsterdam University Press, 2016) 13; L DeNardis et al, 'The Rising Geopolitics of Internet Governance: Cyber Sovereignty v Distributed Governance', paper presented at the Columbia SIPS Tech & Policy Initiative (Columbia SIPA, November 2016) 14–15.

[38] See generally OECD, 'Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies' (November 2012) OECD Digital Economy Paper No 211.

regulations. For instance, some countries have excluded the participation of foreign digital companies from technical standard-setting discussions, thereby indirectly protecting their domestic digital sector.[39] Other countries mandate companies to use domestic technical standards.[40] While these measures are often linked to security, they can entail hidden protectionist interests. It is also now common for countries to ban or exclude the participation of certain foreign digital service providers in domestic markets on the grounds of security, although these bans can potentially also implicate protectionist interests.[41]

Certain countries also use cybersecurity or information security laws to preserve specific political or socio-cultural interests, including monitoring citizens or protecting local values.[42] Such countries tend to implement strict data localisation laws or extensive regulatory approval requirements for cross-border data transfers. While it may seem intuitive that authoritarian countries tend to implement such restrictive cybersecurity measures, these measures are also increasingly common in open, liberal democracies.

B. Cybersecurity, Digital Trade and Cross-Border Data Flows

Cybersecurity is fundamental for digital trade. It is fundamental to create trust for all Internet users and businesses. Consumers are also increasingly aware of the need for cybersecurity-compliant products and services. Private companies and Internet technical bodies and standard-setting institutions engage in various efforts to build robust cybersecurity standards. While concerns regarding the transparency and representativeness of such standards exist (as discussed later in section IVB), they play a vital role in promoting cybersecurity and thereby promoting digital trade flows. At the same time, as governments become more active in cybersecurity regulation, different stakeholders, particularly in the private sector, are concerned about how this may impact digital trade, especially when it entails data-restrictive measures.

[39] N Cory, 'How the EU Is Using Technology Standards as a Protectionist Tool in Its Quest for Cybersovereignty' (ITIF, 19 September 2022) www.ITIF.org/publications/2022/09/19/how-the-eu-is-using-technology-standards-as-a-protectionist-tool/.

[40] See, eg 'China: TC260 Announces 12 National Cybersecurity Standards' (OneTrust DataGuidance, 27 March 2023) www.dataguidance.com/news/china-tc260-announces-12-national-cybersecurity.

[41] See, eg S McCallum, 'European Commission Bans TikTok on Staff Devices' (BBC, 23 February 2023) www.bbc.com/news/technology-64743991; J Clayton and B Derico, 'TikTok Says US Threatens Ban if China Stake Not Sold' (BBC, 16 March 2023) www.bbc.com/news/technology-64973156; S Phartiyal, 'India Bans 200-Plus Chinese Mobile Apps in Boon for Paytm' (Bloomberg, 07 February 2023) www.bloomberg.com/news/articles/2023–02–07/ant-backed-paytm-soars-after-report-india-banned-chinese-rivals.

[42] A Segal, 'Chinese Cyber Diplomacy in a New Era of Uncertainty' (Hoover Institution, June 2017) Aegis Paper Series No 1703, 3–5, 16; J Kopstein, 'Washington's Cybersecurity Is about Surveillance, Not Security' (Al Jazeera, 10 March 2015) www.america.aljazeera.com/opinions/2015/3/washingtons-cybersecurity-is-about-surveillance-not-security.html.

Several examples illustrate how cybersecurity-related measures are barriers to cross-border data flows and digital trade. For instance, certain countries have banned specific digital services and apps for security factors such as the presence of malware or spyware, or concerns around unauthorised/illegal/excessive foreign government surveillance of their citizens.[43] While some of these bans may pertain to legitimate policy concerns, they can also be targeted towards specific countries for economic reasons (particularly to protect domestic players) or political reasons (if the foreign company is based in an unfriendly jurisdiction).

Further, domestic cybersecurity laws may contain data restrictions as well as impose burdensome authorisation, licensing, testing and registration requirements on foreign companies. These measures, however, harm digital companies. Data localisation, for instance, can limit the global data processing and cybersecurity operations of foreign companies, thereby reducing their competitiveness while increasing their compliance costs.[44] Further, by disrupting global data operations of companies, data localisation prohibits effective monitoring of cyber-threats across the global network.[45] Governmental requirements to provide technical information such as source code or algorithms as a condition of providing digital services in the domestic market may also disincentivise digital service suppliers (especially foreign suppliers) from entering certain markets because of risks of trade secret theft and illegal surveillance.[46]

The governments of certain states, such as China, require companies to adopt technical standards that the government considers 'secure and controllable', thus pressurising companies to adopt specific standards even if they are incompatible with internationally recognised standards.[47] These measures can adversely affect both the efficiency and the security of data flows.[48] For example, as per certain reports, China has issued 300 cybersecurity standards that are not only a significant barrier to market access,[49] but also affect the efficiency of

[43] A Hemrajani, 'CO22102 | The Indian Government Ban on Chinese Apps and the Singapore Connection' (RSIS, 19 October 2022) www.rsis.edu.sg/rsis-publication/cens/the-indian-government-ban-on-chinese-apps-and-the-singapore-connection/.

[44] JP Meltzer, 'Governing Digital Trade' (2018) 18(S1) *World Trade Review* s23, s24–s26; WJ Drake et al, 'Internet Fragmentation: An Overview' (World Economic Forum, 2016) Future of the Internet Initiative White Paper, 45. See also A Beattie, 'Data Protectionism: The Growing Menace to Digital Businesses' (*Financial Times*, 3 May 2018) www.ft.com/content/6f0f41e4-47de-11e8-8ee8-cae73aab7ccb.

[45] P Swire and D Kennedy-Mayo, 'The Effects of Data Localization on Cybersecurity – Organizational Effects' (15 June 2023) Georgia Tech Scheller College of Business Research Paper No 4030905, 8–10, 13, 16, 18–19.

[46] For concerns related to Chinese laws on this issue, see, eg The White House, 'How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World' (June 2018).

[47] S Sacks, 'Samm Sacks Testifies Before House Foreign Affairs Committee on "Smart Competition" With China' (New America, 10 May 2019) www.newamerica.org/cybersecurity-initiative/digichina/blog/samm-sacks-testifies-house-foreign-affairs-committee-smart-competition-china/.

[48] A Oddenino, 'Digital Standardization, Cybersecurity Issues and International Trade Law' (2018) 51 *Questions of International Law* 31, 35.

[49] S Sacks and MK Li, 'How Chinese Cybersecurity Standards Impact Doing Business in China' (CSIS Briefs, 2 August 2018) 10; see also N Ahrens, 'National Security and China's Information Security Standards' (CSIS Briefs, November 2012).

data flows out of the country, and could compromise the openness and interoperability of the Internet.[50] Therefore, the imposition of specific mandatory standards can also impede trade, especially if they are misaligned with industry best practices.[51]

C. The Digital Trade–Cybersecurity Dilemma

The increasing number of data-restrictive measures in cybersecurity laws and regulations can raise costs of digital trade. Further, the imposition of highly restrictive regulations may create a false sense of security, given that cybersecurity risks are transnational/global in nature. This leads to an obvious tension between cybersecurity and digital trade, wherein, on the one hand, digital trade is not possible without a robust cybersecurity framework, while, on the other, restrictions in domestic cybersecurity laws and regulations disrupt digital trade flows. This can be broadly referred to as the digital trade–cybersecurity dilemma. This dilemma arguably reflects the broader tension in the global economy between trade and security.[52] For instance, recent trade tensions reflect the changing nature of what governments perceive as security threats, including the actors who are behind it, as well as the sectors that are affected by such security risks.[53] The dual-use nature of data-driven technologies creates further challenges in making an objective assessment of cybersecurity challenges.[54]

The tension between digital trade rules and domestic cybersecurity laws and regulations has obvious costs. First, as explained earlier, they lead to more expensive and inefficient barriers for companies engaging in digital trade, particularly smaller companies. Second, this conflict leads to uncertainties in global cybersecurity governance as different forms of data restrictions and conflicting technical standards fragment the global framework for digital trade and create new risks. For instance, poor cybersecurity practices and weak standards mandated in domestic laws are likely to increase risks of data breaches and economic losses, and hamper efficient market competition. It also creates obstacles to creating a global regulatory framework for cybersecurity. Thus, it is increasingly important to resolve this tension between digital trade and cybersecurity. A prominent

[50] WTO (Council for Trade in Services), 'Report of the Meeting Held on 2 March 2018' (5 April 2018) WTO Doc S/C/M/138, 19–24; Sacks and Li, 'How Chinese Cybersecurity Standards Impact Doing Business in China' (n 49); Oddenino (n 48) 35.

[51] P Delimatsis, 'Global Standard-Setting 2.0: How the WTO Spotlights ISO and Impacts the Transnational Standard-Setting Process' (2018) 28(2) *Duke Journal of Comparative & International Law* 273, 275.

[52] B Heath, 'The New National Security Challenge to the Economic Order' (2020) 129(4) *Yale Law Journal* 924, 1026; JY Yoo and D Ahn, 'Security Exceptions in the WTO System: Bridge or Bottle-Neck for Trade and Security?' (2016) 19(2) *Journal of International Economic Law* 417.

[53] Heath (n 52) 1034.

[54] European Commission, 'Dual-use Technologies' (7 June 2019) www.knowledge4policy.ec.europa.eu/foresight/topic/changing-security-paradigm/artificial-intelligence-quantum-cryptography_en.

site where this tension is visible is international trade law. In the next section, I investigate how international trade law applies to cybersecurity-related data-restrictive measures.

III. INTERFACE OF CYBERSECURITY MEASURES AND INTERNATIONAL TRADE LAW

This section looks at the framework for international trade law to evaluate the extent to which data restrictions contained in domestic cybersecurity-related laws and regulations conflict with international trade law. The first part of the section deals specifically with WTO law, then the second part looks at the evolving framework of digital trade rules contained in PTAs.

The key argument of this section is that while existing trade disciplines can meaningfully address outright protectionist and arbitrary measures, several other aspects of domestic cybersecurity regulation are much more difficult to address in international trade law. The primary reason is because governments increasingly view cybersecurity as both a political and a technical risk, owing to the uncertain and dynamic nature of cyber-threats and geopolitical conflicts. Further, the new disciplines on cybersecurity cooperation in PTAs are weak and do not yet create sufficient incentives for countries to partner one another in developing interoperable frameworks for cybersecurity cooperation or adopting common standards/best practices in cybersecurity.

A. Assessing Cybersecurity-Related Data-Restrictive Measures under WTO Law

(i) Breach of Obligations Contained in GATS

Cybersecurity laws and regulations containing data-restrictive elements may violate different obligations in WTO law. For instance, if a WTO member bans digital services or apps from a specific jurisdiction for security reasons (while allowing similar services/apps to be supplied by companies based in other countries), then it may violate the most-favoured nation (MFN) requirement in GATS, Article II. As discussed in chapter two, the MFN requirement requires the examination of two factors: (i) if the services and service suppliers affected by the measure are 'like'; and (ii) if less favourable treatment is accorded to like services and service suppliers of different members. If an app/digital service originating in a specific country is banned, it an obvious case of origin-based discrimination (irrespective of the policy rationale) and thus would meet the criteria of 'likeness' of services and service suppliers.

In other cases of de facto discrimination (eg based on a neutrally worded law that in practice targets foreign companies from a specific WTO member), a legal test is conducted to examine the degree of competition and involves

assessment of various factors, including properties and nature of services; end users; consumer preferences; and the classification of services under Doc W/120. For instance, a regulation differentiating the security levels of services can be relevant for the likeness test in two ways: (i) if security itself is a defining factor in the final nature of the service, such as anti-virus software;[55] or (ii) if consumer preferences are affected by the security level of services or the security practices (or even reputation) of service suppliers.[56] In the latter case, panels may look at domestic surveys regarding consumer preferences,[57] although cybersecurity concerns are less likely to be relevant in developing countries with lower levels of digital development.[58]

If digital services and service suppliers of different WTO members are found to be 'like', a WTO panel would then evaluate if specific foreign services or service suppliers receive less favourable treatment than other WTO members. For example, in 2017, the US government banned Kaspersky, a Russian supplier of anti-virus software, because of the 'information security risks presented by the use of Kaspersky products on federal information systems' and 'the ties between certain Kaspersky officials and Russian intelligence and other government agencies'.[59] GATS, Article II was clearly violated in that situation as the measure specifically targeted a supplier originating from Russia. The regulatory rationale – ensuring the security of federal services – would be irrelevant in the assessment under GATS, Article II.[60] A similar test could be applied in the context of bans on TikTok and other Chinese apps in several other countries.

Cybersecurity-related data-restrictive measures may also discriminate against foreign services and service suppliers and provide preferential treatment to 'like' domestic services and service suppliers. Such measures may violate the national treatment obligation in GATS, Article XVII if the concerned members have offered relevant commitments in their GATS Schedule of Commitments. An example of such a violation is data localisation, which increases compliance costs for foreign suppliers and reduces their competitiveness. In contrast,

[55] See *European Communities – Measures Affecting Asbestos and Products Containing Asbestos*, Appellate Body Report (adopted 5 April 2001) WT/DS135/12, para 114 (where the Appellate Body held that toxicity of asbestos was a defining aspect of the physical nature of the good) (EC – Asbestos).

[56] See, eg *Argentina – Measures Relating to Trade in Goods and Services*, Appellate Body Report (adopted 9 May 2016) WT/DS453/12, paras 6.22 (in the case of Art XVII) and 6.24 (in the case of Art II); *China – Certain Measures Affecting Electronic Payment Services*, Panel Report (adopted 31 August 2012) WT/DS413/10, para 7.700.

[57] See, eg CIGI, 'CIGI–Ipsos Global Survey on Internet Security and Trust' (2019) www.cigionline.org/cigi-ipsos-global-survey-internet-security-and-trust/. See, eg T Knutson, 'Poll: Cybersecurity Big Source of Consumer Worry and Negligence' (Forbes, 3 April 2018) hwww.forbes.com/sites/tedknutson/2018/04/03/poll-cybersecurity-big-source-of-consumer-worry-and-negligence/#70664e3a5379.

[58] IM Ruiz, 'Cyber Security Challenges in Developing Countries' (*MS&E 238 Blog*, 6 July 2017) www.mse238blog.stanford.edu/2017/07/imunizr/cyber-security-challenges-in-developing-countries/.

[59] US Department of Homeland Security (n 16).

[60] *European Communities – Regime for the Importation, Sale and Distribution of Bananas*, Appellate Body Report (adopted 25 September 1997) WT/DS27/98, para 241.

domestic digital service suppliers (especially the bigger companies) are likely to own local servers and are therefore usually unaffected by this requirement. In fact, foreign companies may even be forced to rely on these local servers, further diverting competition in favour of local suppliers.[61] Thus, data localisation imposed on grounds of cybersecurity protection can result in less favourable treatment of foreign services and service suppliers and could violate GATS, Article XVII.

Similarly, if a country imposes a specific domestic cybersecurity standard, it can potentially raise the costs of compliance and reduce the market competitiveness of foreign companies. This measure can also jeopardise the security levels of their services if the mandated standards are weaker or incompatible with globally accepted standards and thus disrupt alignment between suppliers' local and global data operations. Domestic service suppliers (especially huge local companies) are less likely to be affected by this measure as they may be able to function competitively without synergising their domestic and foreign data operations. This measure will have a particularly discriminatory impact if those domestic companies contribute to the development of the mandated technical standards, thereby having an additional competitive advantage over foreign companies.

A ban on specific apps and digital services on grounds of cybersecurity can also conflict with the market access obligations contained in GATS, Article XVI, provided that the country imposing the ban has made relevant commitments in their GATS Schedule. For example, if a WTO member has undertaken full Mode 1 (cross-border delivery) market access commitments in a specific sector but imposes a restriction on digital services in that sector for security reasons (such as explicitly requiring local storage/processing of all data in that sector or even a complete ban on a service), it could amount to a 'zero quota' restricting the total number of service suppliers/service transactions/service transactions in violation of GATS, Article XVI(2)(a), (b) and (c) respectively.[62] However, if cybersecurity-related data-restrictive measures impose only additional compliance requirements for cross-border data transfers (eg obtaining approvals) but do not prohibit service suppliers from conducting their cross-border data operations, GATS, Article XVI is unlikely to be violated.[63]

Even if a cybersecurity measure is not explicitly discriminatory, it can still violate other obligations on domestic regulation contained in GATS, Article VI. For instance, a domestic cybersecurity standard may be imposed with the intent of achieving a higher level of security in the network or data-driven services. Similarly, security assessment of cross-border data transfers or requirement to

[61] AA Friedman, 'Cybersecurity and Trade: National Policies, Global and Local Consequences' (Centre for Technology Innovation at Brookings, September 2013) 10, 12.

[62] *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, Appellate Body Report (adopted 20 April 2005) WT/DS285/26, paras 238, 251, 373.

[63] ibid paras 25–26.

provide source code does not block market access for foreign companies. They are also likely to be equally expensive and cumbersome for domestic and foreign suppliers. Therefore, there is no outright discrimination or restriction on market access.

However, GATS, Article VI:1 requires members to implement all measures in a 'reasonable, objective and impartial manner'. For example, if the government imposing the mandatory requirement for disclosing source code or other technical information uses such information for unauthorised surveillance or sharing trade secrets with domestic competitors, then it can breach GATS, Article VI.[64] Further, requirements to undergo security assessment for cross-border data transfers may violate GATS, Article VI:3, for example where such approvals are not provided in a transparent manner (eg not providing the reasons for disallowing data transfers).[65]

If a WTO member imposes cybersecurity standards for digital service sectors where they have made relevant GATS commitments, GATS, Article VI:5 could also be relevant.[66] For example, if a domestic cybersecurity standard deviates significantly from internationally recognised standards, foreign suppliers are likely to face a higher burden to comply with these domestic standards. Further, if international standards already exist, such compliance requirements may be found unreasonable and unnecessary under GATS, Article VI:5.

Most global cybersecurity standards are created by multistakeholder or private organisations, such as the International Standards Organisation (ISO),[67] Internet Engineering Task Force (IETF),[68] Institute of Electrical and Electronics Engineers (IEEE)[69] and World Wide Web Consortium (W3C),[70] or by private industry groups.[71] The only major exception is the International Telecommunications Union (ITU), which is a multilateral institution involved in setting cybersecurity standards.[72] Multistakeholder/private bodies do not

[64] Such practices have been previously criticised by the WTO dispute settlement body. See *Argentina – Measures Affecting the Export of Bovine Hides and the Import of Finished Leather*, Panel Report (adopted 16 February 2001) WT/DS155/12, paras 11.90–11.94.

[65] WTO (Council for Trade in Services), 'Communication from the US Measures Adopted and Under Development by China Relating to Its Cybersecurity Law' (26 September 2017) WTO Doc S/C/W/374.

[66] At the time of the formulation of the GATS, WTO members had envisaged developing detailed domestic regulation guidelines for different service sectors. However, these disciplines were not developed for any sectors other than accountancy services. See WTO, 'WTO Adopts Disciplines on Domestic Regulation for the Accountancy Sector' (14 December 1998) WTO Press Release No 118.

[67] See, eg International Organization for Standardization, 'Cybersecurity – Guidelines for Internet Security' (2023) ISO/IEC 27032:2023.

[68] 'Leading Engineers Agree to Upgrade Standards to Improve Internet Privacy and Security' (*IETF Blog*, 7 November 2013) www.ietf.org/blog/leading-engineers-agree-upgrade-standards-improve-internet-privacy-and-security/.

[69] For cybersecurity standards formulated by the IEEE, see 'Design' (IEEE) www.cybersecurity.ieee.org/center-for-secure-design/.

[70] For standards designed by W3C, see 'Security at W3C' (W3C) www.w3.org/Security/.

[71] See generally Karachalios and McCabe (n 7).

[72] ITU, 'Study Group 17 at a Glance', www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx.

qualify as 'international organization[s]' under GATS, Article VI because they do not constitute 'international bodies whose membership is open to the relevant bodies of at least all Members of the WTO'.[73] For example, membership of the IETF[74] and IEEE[75] is open only to individuals.

The constraining definition of international standards in GATS, Article VI presents a challenge for assessing cybersecurity standards under GATS. This uncertainty is further exacerbated due to the unpredictable nature of cybersecurity threats[76] and the lack of sufficient consensus (even within the Internet technical community) on best policies or technological tools to achieve cybersecurity.

(ii) Justifying Cybersecurity Measures under GATS General Exceptions

Cybersecurity-related data-restrictive measures inconsistent with GATS obligations can be justified as being necessary to achieve the policy objectives listed in the general exceptions (GATS, Article XIV). This subsection looks at the two most relevant general exceptions for cybersecurity-related data-restrictive measures: GATS, Article XIV(a) (public order and public morals) and GATS, Article XIV(c) (compliance with domestic laws and regulations).[77]

As discussed in chapter two, GATS, Article XIV(a) covers all 'measures necessary to protect public morals or to maintain public order', with the term 'public order' being defined as 'genuine and sufficiently serious threat' to 'one of the fundamental interests of society'. Broadly speaking, this exception has been interpreted and applied in a flexible and evolutionary manner to cover a broad range of policy concerns. Cybersecurity risks are quite likely to qualify as risks to the public order as they can harm both virtual and physical infrastructure.[78] Further, cybersecurity failures can disrupt core government activities, for example by infecting government websites or erasing government databases.[79]

[73] GATS, Art VI:5(b). See also *United States – Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products*, Appellate Body Report (adopted 13 June 2012) WT/DS381/49/Rev.1, para 386 (US – Tuna II).

[74] IETF, 'About IETF', www.ietf.org/about/.

[75] IEEE, 'IEEE at a Glance', www.ieee.org/about/today/at-a-glance.html#membership.

[76] Peng (n 12) 450.

[77] GATS, Art XIV(b) (protecting human health). It could apply if a cyber-attack hurts or kills human beings or where a cyber-disruption (eg in the health services) leads to adverse consequences for human health. However, given the slim possibility of such events, this discussion is excluded here.

[78] For instance, security threats in the Internet of Things (IoT) can potentially cause physical harm to all homes connected by smart gadgets. See generally SJ Shackleford et al, 'When Toasters Attack: Enhancing the "Security of Things" Through Polycentric Governance' (2017) 2 *University of Illinois Law Review* 415.

[79] See, eg M Field, 'WannaCry Cyber Attack Cost the NHS £92m as 19,000 Appointments Cancelled' (*The Telegraph*, 11 October 2018) www.telegraph.co.uk/technology/2018/10/11/wannacry-cyer-attack-cost-nhs-92m-19000-appointments-cancelled/; K Dodson, 'Annual Cybersecurity Report: Impacts on Government' (*Cisco Blog*, 10 April 2018) www.blogs.cisco.com/government/annual-cybersecurity-report-impacts-on-government.

A WTO member could thus argue that such threats constitute a 'genuine' and 'serious' threat to 'fundamental interests of society', including public safety, under GATS, Article XIV(a). In certain cases, cybersecurity can also relate to public morality, such as protecting children from cybercrimes.[80]

GATS, Article XIV(c) covers measures necessary to secure compliance with different types of domestic laws or regulations, including laws relating to 'deceptive and fraudulent practices' in GATS, Article XIV(c)(i) and 'safety' in GATS, Article XIV(c)(iii). These laws can be broadly interpreted as covering domestic laws protecting consumers from cybercrimes, including unauthorised hacking by third parties and malware attacks.[81] Further, although GATS, Article XIV(c)(ii) is primarily about the protection of privacy of individuals, the term 'protection of confidentiality of individual records and accounts' could include data or network security. Finally, GATS, Article XIV(c) does not contain an exhaustive list. WTO members can, however, rely upon GATS, Article XIV(c) to argue that certain data-restrictive measures are necessary to address threats arising from poor cybersecurity practices (both potential and existing) or for preventing cybercrimes harming domestic consumers. To substantiate these claims, evidence on the nature and scale of cybersecurity threats could be relevant.

Given that cybersecurity risks arise from the weakest link in the global digital chain,[82] most panels would accord high priority to cybersecurity protection in conducting the weighing and balancing test under GATS, Article XIV. Three factors are weighed and balanced under this test, namely: the contribution of the measure to cybersecurity protection; its trade-restrictive impact; and the less trade-restrictive alternatives available to the defendant.

Regarding the first factor, ie establishing a causal relationship between a measure and the objective of cybersecurity, a case-by-case assessment using both technological and legal evidence is essential. For example, if a mandatory domestic cybersecurity standard deviates from international standards and best practices, it would be difficult to demonstrate that the mandated standard is robust and effective in achieving a high standard of cybersecurity protection.[83] In contrast, measures preventing cross-border data flows to countries with a poor track record of cybersecurity are likely to be considered effective as they avert cybersecurity threats. However, if the proffered policy objective of

[80] See, eg Z Doffman, 'Google Chrome Update – a Threat to Children, Cybersecurity and Government Snooping' (Forbes, 22 April 2019) www.forbes.com/sites/zakdoffman/2019/04/22/crisis-as-changes-to-google-chrome-threaten-child-safety-and-cybersecurity/#2340b9c75704.

[81] P Kastner and F Mégret, 'International Legal Dimensions of Cybercrime' in N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Cheltenham, Edward Elgar, 2015) 190, 205.

[82] M Smith, 'Supply Chain Cyber Security Is Only as Strong as the Weakest Link' (*Computer Weekly*, 27 August 2021) https://www.computerweekly.com/opinion/Supply-chain-cyber-security-is-only-as-strong-as-the-weakest-link.

[83] SJ Shackleford et al, 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors' (2016) 17(1) *Chicago Journal of International Law* 1, 21.

a data localisation measure is eliminating cybersecurity threats, then the causal link may be harder to establish, although this measure may facilitate stronger enforcement against cybercrimes/cybercriminals.[84] The same holds true for a ban on a specific foreign company, especially when cyber-threats are spread across the entire global value chain.

In assessing the contribution of the measure to cybersecurity protection, a WTO panel may consider various factors, including the design and operation of the measure and the technical impact of the measure on data/network security. However, its role must be limited to examining the sufficiency of the evidence regarding the contribution of the measure. In other words, a panel cannot act as an 'arbiter' of conflicting opinions, ie resolving conflicting evidence or expert reports regarding the efficacy of a cybersecurity standard.[85] For example, foreign companies are likely to be suspicious of domestic cybersecurity standards as being more risky and less secure and prefer standards developed by the ISO or IEEE.[86] Such bodies, however, do not enjoy the same legal status as state-driven standard-setting organisations under WTO law.[87] Further, certain experts argue that private/multistakeholder standards reflect the interests of leading technology companies in developed countries and thus do not constitute representative international standards.[88] While consultation with external experts can help in appreciating the evidence regarding the effectiveness, representativeness and transparency of mandated standards, the lack of international consensus on cybersecurity standards will likely limit a WTO panel's ability to comprehensively assess measures imposing domestic cybersecurity standards.

Similarly, a WTO panel cannot decide or evaluate the appropriate level of cyber-risk, which is the sole prerogative of the government.[89] For example, certain governments require forced disclosure of source code, algorithms or encryption keys as a condition of market access. Despite its highly restrictive impact, such information disclosure can help address vulnerabilities by allowing

[84] SJ Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations in Search of Cyber Peace* (Cambridge, Cambridge University Press, 2013) 89. See also *Brazil – Measures Affecting Imports of Retreaded Tyres*, Appellate Body Report (adopted 17 December 2007) WT/DS332/19/Add.6, para 228 (Brazil – Retreaded Tyres).

[85] EC – Asbestos (n 55) paras 8.181–8.182.

[86] See, eg H-W Liu, 'China Standard Time: The Boundaries of Techno-nationalism in Megaregionals' in S Peng et al (eds), *Governing Science and Technology under the International Economic Order* (Cheltenham, Edward Elgar, 2018) 114, 127–31.

[87] Peng (n 12) 462. In the context of TBT agreement, see also US – Tuna II (n 73) paras 359–401.

[88] V Thorstensen et al, 'Private Standards – Implications for Trade, Development, and Governance' (E15 Initiative, September 2015) 2–4. See generally CS Gibson, 'Globalization and the Technology Standards Game: Balancing Concerns of Protectionism and Intellectual Property in International Standards' (2007) 22(4) *Berkeley Technology Law Journal* 1407; E Wijkström and D McDaniels, 'International Standards and the WTO TBT Agreement: Improving Governance for Regulatory Alignment' (25 April 2013) WTO Staff Working Paper ERSD-2013-06, 11.

[89] *United States – Continued Suspension of Obligations in the EC – Hormones Dispute*, Panel Report (adopted 14 November 2008) WT/DS320/18, para 592. See also M Du, 'Re-conceptualizing the Role of Science in International Trade Disputes' (2018) 52(5) *Journal of World Trade* 697, 700. See also *EC – Seals*, Appellate Body Report, para 5.200 (where the Appellate Body said that different countries may have varying levels of protection for the same moral interests).

governments to detect existing backdoors for foreign surveillance or detecting local crimes/security threats.[90] As these policy concerns are relevant for the government to manage cyber-risks domestically, they are likely to contribute to better cybersecurity protection within the country.

As regards the second factor in the weighing and balancing test, data-restrictive measures are highly trade-restrictive, even where the measure is confined to specific sectors or digital services. Data restrictions usually have a cross-cutting impact and affect exports across all sectors due to the increased digitalisation of the majority of sectors in the economy. Further, foreign service suppliers and their consumers often bear the additional costs arising from data-restrictive measures. These costs are particularly burdensome for smaller companies, which are highly prevalent in digital sectors.[91]

The last step in conducting the weighing and balancing test is assessing whether any alternative measure(s) exist that are less trade-restrictive, reasonably available to the defendant and achieve the same desired level of protection as the implemented measure. Certain experts recommend market-based and technological solutions that can help address cybersecurity threats.[92] One such example is imposing a security-by-design requirement, requiring service suppliers to incorporate adequate security features at the time of designing the digital product or service.[93] This approach allows digital service suppliers to adopt internationally recognised standards and thus minimises the need for other kinds of restrictions, including mandatory standards.

While the above mechanisms can theoretically be proposed as alternatives by the complainant in a trade dispute, there are several reasons why WTO panels may not consider them, including: (i) inadequate regulatory capacity and expertise of several governments to evaluate compliance with security-by-design requirements; (ii) low viability of security-by-design laws or policies in the context of modern-day technologies;[94] (iii) lack of binding international consensus on cybersecurity standards and best practices; and (iii) the difficulty of second guessing the level or types of cyber-risks that a country must be willing to tolerate.[95] Therefore, technological solutions and marked-based standards

[90] See generally RS Neeraj, 'Trade Rules on Source Code – Deepening the Digital Inequities by Locking Up the Software Fortress' (28 April 2017) Centre for WTO Studies Working Paper CWS/WP/200/37, 17–19, 25–26.

[91] Kommerskollegium, 'No Transfer, No Production – the Importance of Cross-Border Data Transfers for Companies Based in Sweden' (2014:1).

[92] F Badiei et al, 'Markets versus Mandates: Solutions for Securing the Internet of Things' (R Street Institute, November 2017) 1.

[93] See, eg GDPR, Art 25.

[94] See generally Department of Digital, Media, Culture & Sport (UK), 'Secure by Design: Improving the Cybersecurity of Consumer Internet of Things Report' (2018); LA Bygrave, 'Security by Design: The Emperor's New Clothes in the Cybersecurity Space?' (Presentation at the University of Melbourne, Melbourne, 26 October 2018).

[95] See S Cho, 'Of the World Trade Court's Burden' (2009) 20(3) *European Journal of International Law* 675, 684; see also E Lydgate, 'Is It Rational and Consistent? The WTO's Surprising Role in Shaping Domestic Public Policy' (2017) 20(3) *Journal of International Economic Law* 561, 570.

can act as complements to prescriptive measures and form a part of the complex suite of measures intended to achieve a policy objective.[96]

The assessment of the cybersecurity measure under the GATS, Article XIV chapeau is the final step in the necessity assessment that ensures that the exception is not abused and that measures are implemented in good faith. Under this test, the level of cybersecurity protection of the country imposing the measure and other countries are first compared to assess if their regulatory conditions are 'like'. This assessment could be conducted by looking at specific indicators, such as the Global Cybersecurity Index.[97] Next, a panel will examine the design and implementation of the measure to assess if there is arbitrary or unjustifiable discrimination in like circumstances. For example, if foreign companies face higher burdens in domestic cybersecurity laws compared to their domestic counterparts, then it constitutes arbitrary or unjustifiable discrimination.[98]

Further, cybersecurity measures could constitute disguised restriction on trade in services, where the measure clearly protects domestic services or service suppliers or reduces opportunities for foreign suppliers. For example, certain mandatory technical standards provide domestic service suppliers with an advantage. Similarly, the mandatory disclosure of source code can be burdensome for foreign suppliers as it increases the chances of trade secret theft, prejudices the security of their data operations and can lead to global reputational damage.[99]

B. Justifying Cybersecurity-Related Measures under the GATS Security Exception

In addition to the general exception, the security exception in GATS, Article XIV can be relevant in justifying cybersecurity measures:

> Nothing in this Agreement shall be construed:
>
> (b) to prevent any Member from taking any action which *it considers necessary* for the *protection of its essential security interests*:
>
> (i) *relating to the supply of services* as carried out directly or indirectly *for the purpose of provisioning a military establishment;*
>
> (ii) *relating to fissionable and fusionable materials* or the materials from which they are derived;
>
> (iii) taken in time of *war or other emergency in international relations;* or

[96] Brazil – Retreaded Tyres (n 84) 172.

[97] ITU, 'Global Cybersecurity Index' www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

[98] Lydgate (n 95) 567.

[99] G Wildau, 'China Drafts Law to Ban Forced Tech Transfer from Foreign Partners' (*Financial Times*, 24 December 2018) www.ft.com/content/90cd02ba-0739–11e9-9fe8-acdb36967cfc.

(c) to prevent any Member from taking any *action in pursuance of its obligations under the United Nations Charter* for the maintenance of international peace and security.[100]

This exception has not yet been invoked in a GATS dispute. However, in recent years, WTO panel reports have looked at the security exception in other WTO treaties.[101] The discussion below draws upon this jurisprudence to draw conclusions regarding the scope and applicability of GATS, Article XIVbis in the cyber-context.

(i) Interpreting the Security Exception in WTO Law

For the longest time, the key question about the security exception was whether it allowed WTO members to unilaterally determine if the exception applied to their security measures (ie if it was self-judging in nature). This confusion arose because the chapeau of GATS, Article XIVbis 1(b) included the phrase 'it considers necessary', as stated above.[102] The WTO panels have now clarified that the security exception contained in GATT, Article XXI is not 'totally self-judging'[103] because the phrase 'it considers' is qualified by essential security interests limited to specific scenarios, namely, those related to military facilities or nuclear facilities and measures taken in time of 'war' or 'other emergency in international relations'.[104] All the above scenarios can be objectively assessed on a case-by-case basis and are thus subject to judicial reasoning.[105]

The first question is what constitutes essential security interests. The use of 'essential' implies that the level of security interests should be higher than usual security interests.[106] However, countries' opinions of which security interests are essential can vary, so individual WTO members determine their own essential security interests,[107] including relating their security interests to external events in other jurisdictions.[108] The panels have clearly stated that security exception

[100] Emphasis added.

[101] See *United States – Certain Measures on Steel and Aluminium Product*, Panel Report (circulated 9 December 2022) WT/DS544/14 (US – Steel and Aluminium Products (China)); *Russia – Measures Concerning Traffic in Transit*, Panel Report (adopted 26 April 2019) WT/DS512/7 (Russia – Traffic in Transit); *Saudi Arabia – Measures Concerning the Protection of Intellectual Property Rights*, Panel Report (circulated 16 June 2020) WT/DS567/11 (Saudi Arabia – IPRs); *United States – Origin Marking Requirement*, Panel Report (circulated 21 December 2022) WT/DS597/R (US – Origin Marking).

[102] Russia –Traffic in Transit (n 101) paras 7.28–7.30, 7.51–7.52 (summarising Russia's arguments). See also R Bhala, 'National Security and International Trade Law: What the GATT Says, and What the United States Does' (1998) 19 *University of Pennsylvania Journal of International Economic Law* 263, 268; HL Schloemann and S Ohlhoff, '"Constitutionalization" and Dispute Settlement in the WTO: National Security as an Issue of Competence' (1999) 93(2) *American Journal of International Law* 424, 427, 442.

[103] Russia –Traffic in Transit (n 101) para 7.72; US – Steel and Aluminium Products (China) (n 101) para 7.146.

[104] Russia –Traffic in Transit (n 101) para 7.65–7.68.

[105] ibid paras 7.82, 7.101; see also para 7.100.

[106] ibid para 7.130.

[107] ibid para 7.131.

[108] US – Origin Marking (n 101) para 7.359.

must be invoked in good faith,[109] implying that WTO members cannot use the exception to circumvent their obligations under WTO law.[110] Therefore, countries must clearly articulate their essential security interests to help determine the veracity of their claims.[111]

Further, a WTO member imposing an essential security measure should at least be able to demonstrate that the 'measur[e] at issue meet[s] a minimum requirement of plausibility in relation to the proffered essential security interests'.[112] The standard of 'plausibility' provides for a lower threshold than the necessity test under GATS, Article XIV, thus allowing panels to be somewhat deferential to the security objectives of WTO members. However, the good faith requirement can still be intrusive; for example, a government may be required to identify abusers of the exception in certain circumstances or investigate how the measure operates in practice.[113]

(ii) Applying the Security Exception to Cybersecurity Measures

The security exception in WTO law was written well before the current era of cyber-threats and cybercrimes. But an evolutionary interpretation of this exception would cover scenarios where a cybersecurity threat poses a national security risk. For example, certain cyberattacks may be of a sufficient scale/magnitude to debilitate the economy or infrastructure of a country. Any data-restrictive measures that contain such cyberattacks could be measures taken to protect essential security interests during a state of war. Another example is data-restrictive measures affecting the supply of digital services used in military or nuclear facilities.

GATS, Article XIVbis 1(b)(i) and (ii) applies when measures are 'related to' safeguarding the military or nuclear facilities of a WTO member from cybersecurity threats. Digital services are becoming integral to defence, and therefore requirements under GATS, Article XIVbis 1(b)(i) and (ii) can be satisfied in certain cases. For example, a cyberattack on a nuclear power plant or defence equipment can cause damage in one or several countries.[114] Similarly, digitalisation of military activities is not uncommon, making such systems vulnerable to cyberattacks.[115] However, the above provisions are unlikely to be very relevant as countries have shared interests in protecting their defence and nuclear systems.

[109] Russia –Traffic in Transit (n 101) para 7.132; see Peng (n 12) 468, 451, 477.
[110] Russia –Traffic in Transit (n 101) para 7.133.
[111] ibid para 7.134.
[112] ibid para 7.138.
[113] Heath (n 52) 1075.
[114] See, eg A Shalal, 'IAEA Chief: Nuclear Power Plant Was Disrupted by Cyber Attack' (Reuters, 11 October 2016) www.reuters.com/article/us-nuclear-cyber/iaea-chief-nuclear-power-plant-was-disrupted-by-cyber-attack-idUSKCN12A1OC.
[115] See, eg J Delcker, 'Digitizing Military will Cost Europe up to €41 Billion Per Year: Study' (*Politico*, 23 November 2017) www.politico.eu/article/digitizing-military-will-cost-europe-up-to-e41-billion-per-year-study; 'Digitalisation of Armed Forces Is One of the Top Priorities for Govt, Says Union Minister Subhash Bhamre' (*First Post*, 24 March 2017) https://www.firstpost.com/

The more relevant exception for cybersecurity measures is GATS, Article XIVbis 1(b)(iii), which permits WTO members to take measures to protect essential security interests during war or other emergency in international relations. WTO panels have specifically reflected on the meaning of 'war' and 'emergency in international relations'. The term 'war' generally refers to an armed attack or conflict,[116] while 'emergency in international relations' is a broader term that includes 'situation[s] of armed conflict, or latent armed conflict, or heightened tension or crisis, or of general instability engulfing or surrounding a state'.[117] Political and economic differences between countries do not constitute an emergency in international relations.[118] WTO panels have further held that whether a specific situation constitutes a war or emergency in international relations can be objectively assessed based on the evidence presented by the parties.[119]

In the cyber-context, this exception can thus apply when cybersecurity measures are imposed during times of war or emergency in international relations, such as a ban on foreign digital services imposed during an armed attack to minimise lateral risks of cyberattacks. In such a case, a panel can objectively determine whether a war or emergency in international relations exists and the plausible link between the imposed cybersecurity measure and the essential security interests. This exception can also apply when coordinated cyberattacks or systematic use of cyber-weapons result in a state of 'war' or 'emergency in international relations', although the latter question entails questions unresolved in public international law, as discussed below.

Assessing whether cyberattacks result in a state of war or emergency in international relations is difficult in practice. For example, cyberattacks on government websites,[120] banks,[121] electoral systems[122] and national health systems[123] are common. However, it is unclear whether such cyberattacks constitute an 'armed attack'.[124] Further, determining if GATS, Article XIV bis1b(iii) covers measures taken to restrict cyberattacks initiated by private parties is

tech/news-analysis/digitalisation-of-armed-forces-is-one-of-the-top-priorities-for-govt-says-union-minister-subhash-bhamre-3699863.html.

[116] Russia –Traffic in Transit (n 101) para 7.102.

[117] ibid para 7.76.

[118] ibid para 7.76. A similar approach was taken in US – Steel and Aluminium Products (China) (n 101) para 7.157.

[119] Russia –Traffic in Transit (n 101) para 7.71. See also Saudi Arabia – IPRs (n 101) para 7.257.

[120] See, eg BBC, 'Hackers Hijack Government Websites to Mine Crypto-Cash' (11 February 2018) www.bbc.com/news/technology-43025788.

[121] See, eg N Zinets, 'Ukraine Central Bank Warns of New Cyber-Attack Risk' (Reuters, 18 August 2017) https://www.reuters.com/article/us-cyber-ukraine-banking/ukraine-central-bank-warns-of-new-cyber-attack-risk-idUSKCN1AY0Y4.

[122] N Marachel, 'Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy' (2017) 5(1) *Media & Communication* 29, 35–37.

[123] See, eg S Neville, 'NHS Cyber Attack Far More Extensive Than Thought, Says Report' (*Financial Times*, 27 October 2017) www.ft.com/content/4110069a-ba3d-11e7-8c12-5661783e5589.

[124] R Buchan, 'Cyber Espionage and International Law' in Tsagourias and Buchan (n 81) 168, 187; E Boylan, 'Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners' (2017) 50(1) *Vanderbilt Journal of Transnational Law* 217, 229, 243.

difficult as 'war' typically refers to interstate actions while cyber-attacks are often conducted by non-state parties.[125] The origin of cyberattacks are much harder to trace than conventional armed attacks,[126] so attributing cyberattacks to a government is difficult.[127]

Since 'essential security interests' relates to the 'quintessential functions of the state',[128] cyber-attacks on fundamental government systems such as electoral, public health or financial systems can be seen as being important to 'maintaining internal law and order'.[129] In *Russia – Traffic in Transit*, the panel held that each country should determine its essential security interests in times of war or international emergency.[130] Thus, when a panel concludes that there is a state of war or international emergency, the affected WTO members have greater scope to adopt cybersecurity measures, provided they can clearly articulate their relationship to their essential security interests.

When states defend their cybersecurity measures under GATS, Article XIVbis, they must also demonstrate that they have exercised the exception in good faith and establish a 'plausible link' between their measure and essential security interests. This may be difficult because security vulnerabilities in digital services or systems are often not fully known (and hence are difficult to articulate). In any case, most data-restrictive measures are unlikely to contain cybersecurity threats as cyberattacks can be launched from anywhere, given the global connectivity of the Internet. Further, where measures disproportionately benefit the domestic technology industry and do not obviously address existing/known threats, panels are likely to adopt a cautious approach. Finally, given the highly critical nature of cybersecurity concerns, WTO members could use GATS, Article XIVbis 1(a) to argue that they are not required to provide substantive evidence regarding how they implement certain measures as it may prejudice their essential security interests, such as compromising the safety of their cyber-infrastructure.[131]

Finally, GATS, Article XIVbis 1(c) can apply to justify measures taken 'under the United Nations Charter for the maintenance of international peace and security'. Most cybersecurity measures do not fall within the purview of public

[125] P Marguiles, 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility' (2013) 14 *Melbourne Journal of International Law* 496, 503.

[126] See generally Office of the Director of National Intelligence (US), 'A Guide to Cyber Attribution' (14 September 2018).

[127] See J Goldsmith, 'How Cyber Changes the Laws of War' (2013) 24(1) *European Journal of International Law* 129, 131–2; Marguiles (n 125) 503, 507 (discussing the inadequacy of financial aid to make an attribution to a state).

[128] Russia –Traffic in Transit (n 101) para 7.130.

[129] ibid para 7.130.

[130] ibid para 7.131.

[131] T Voon and AD Mitchell, 'Australia's Huawei Ban Raises Difficult Questions for the WTO' (*East Asia Forum*, 22 April 2019) www.eastasiaforum.org/2019/04/22/australias-huawei-ban-raises-difficult-questions-for-the-wto/.

international law but rather operate in a grey zone.[132] In any case, there are no specific rules in international law or UN treaties governing cybersecurity. The UN Security Council could theoretically issue sanction(s) against a state that engages/acquiesces in cyberattacks disrupting international peace and security. If so, this sanction can inform a cybersecurity measure (for example, banning all digital services or data flows originating from or linked to the sanctioned state). Thus, the exception available in GATS, Article XIVbis(1)(c) is also unlikely to be useful in justifying most cybersecurity measures.

C. Evolving Cybersecurity Disciplines in PTAs and DEAs

Several PTAs contain cybersecurity-specific disciplines (in addition to the provisions on cross-border data flows, data localisation and data protection, discussed in chapter two). This subsection discusses such provisions in three important PTAs – the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Regional Comprehensive Economic Partnership (RCEP) and Agreement between the United States of America, the United Mexican States, and Canada (USMCA) – as well as certain DEAs as these treaties contain the most comprehensive provisions on cybersecurity and also reflect emerging global trends in the existing network of PTAs.

Although several PTAs have advanced beyond WTO law (in fact, GATS does not have any cybersecurity-specific disciplines), they are at best weak efforts at fostering a global regulatory framework for cybersecurity. What is important, however, is that the new-generation PTAs recognise various linkages between digital trade and cybersecurity, and can thus be a starting point to devising holistic trade rules on cross-border data flows. DEAs also reflect a more multidimensional view of cybersecurity cooperation and policy-making by considering roles of different stakeholders. Using the DEA frameworks, some trading partners are now also developing informal arrangements outside of these treaties to build regulatory cooperation on cybersecurity.[133]

(i) Cooperation on Cybersecurity

Global cybersecurity cooperation is essential for digital trade. While several PTAs recognise the importance of cybersecurity cooperation, they generally do not contain any comprehensive or binding provisions. For instance, in

[132] See A Shull, 'Governing Cyberspace During a Crisis of Trust' (CIGI, 26 March 2019) www.cigionline.org/multimedia/video-governing-cyberspace-during-crisis-trust?utm_source=cigi_newsletter&utm_medium=email&utm_campaign=beware-fake-news.

[133] See examples discussed in LY Chang and H Liu, 'Ensuring Cybersecurity for Digital Services Trade' in JW Kang et al (eds), *Unlocking the Potential of Digital Services Trade in Asia and the Pacific* (Manila, Asian Development Bank, 2022) 198–200.

Article 14.16 of the CPTPP, parties recognise the overall importance of cybersecurity, including the role of national computer security incident response teams and the collaboration mechanisms existing to deal with various kinds of cybercrimes, such as 'malicious intrusions' or 'dissemination of malicious code'. Similarly, USMCA, Article 19.15 contains a non-binding provision, although the scope is a bit broader. For instance, it states that parties 'shall endeavour' to 'strengthe[n] existing mechanisms' to collaborate against different kinds of cyber-intrusions.[134] Another unique addition in the USMCA is the recognition of a risk-based approach as a more effective method to regulate cybersecurity threats compared to prescriptive regulation.[135]

Although more recent than the other two treaties, the RCEP has a weak, high-level provision on cybersecurity (as expected, as it involves parties such as China and Vietnam with comprehensive cybersecurity laws and an inclination towards strong implementation of data sovereignty). Like the CPTPP, RCEP parties acknowledge the role of capacity-building in cybersecurity at the national level and using existing mechanisms for collaboration to deal with cybersecurity matters. None of the above provisions address the link between cybersecurity and a broader set of policy concerns, such as spam regulation.[136]

The language in DEAs tends to be broader in relation to cybersecurity cooperation in digital trade, although these provisions are still non-binding in nature. For instance, in the Digital Economy Partnership Agreement (DEPA) and the Korea–Singapore Digital Partnership Agreement (KSDPA),[137] in addition to recognising the importance of cybersecurity collaboration and building national capabilities to deal with cyber incidents, the provision also mentions the need for cooperation in workforce development in cybersecurity.[138] Additionally, a provision on online safety and security recognises the role of a multistakeholder approach in addressing online safety and security issues.[139]

The Singapore–Australia Digital Economy Agreement (SADEA) contains a similarly worded provision on cybersecurity cooperation.[140] The provision on creating a safe online environment is even broader in SADEA, and recognises the important role of various stakeholders, such as governments, technology service providers and users, in developing 'a safe, secure online environment [that] supports the digital economy'.[141] This treaty also states that 'parties shall

[134] USMCA, Art 19.15.1.
[135] ibid Art 19.15.2.
[136] SA Aaronson, 'What Does TPP Mean for the Open Internet?' (International Institute for Economic Policy Brief on Trade Agreements and Internet Governance, prepared for the Global Commission on Internet Governance, 16 November 2015); V Cerf et al, 'Internet Governance Is Our Shared Responsibility' (2014) 10(1) *I/S: A Journal of Law and Policy for the Information Society* 1, 24–25.
[137] Korea–Singapore Digital Partnership Agreement (Singapore, 21 November 2022) (KSDPA).
[138] KSDPA, Art 14.22; DEPA, Art 5.1.
[139] KSDPA, Art 14.23.2; DEPA, Art 5.2.
[140] Singapore–Australia Digital Economy Agreement (6 August 2020), Art 34 (SADEA).
[141] SADEA, Art 18.

endeavour to maintain an open, free and secure Internet in accordance with their respective laws and regulations'.[142]

Finally, the UK–Singapore Digital Economy Agreement (UKSDEA) identifies several additional factors as being critical to cybersecurity cooperation in digital trade: maintaining dialogues on cybersecurity, establishing mutual recognition of a baseline security standard for IoT technologies and collaborating on cybersecurity research and development projects.[143] Similar to the USMCA, the UKSDEA recognises the importance of risk-based approaches in developing cybersecurity regulation and the need for open and transparent industry standards.[144] This additional language is significant, especially in the context of recognising the importance of transparent and open standards for cybersecurity.

(ii) Security Exceptions in PTAs

As cybersecurity concerns have mushroomed, governments want to preserve their policy space to impose measures necessary to safeguard cybersecurity. Further, as discussed earlier, government now associate cybersecurity with a range of different political, economic and social security objectives. Therefore, recent PTAs (including digital trade chapters in some treaties such as the RCEP) contain a much broader scope to accommodate security-related interests. For instance, the CPTPP security exception reads as follows:[145]

> 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

The same language is found in the USMCA.[146] Unlike GATS, Article XIVbis, this exception is clearly self-judging in nature and can be applied to any kind of cyber-measures that can be linked to the protection of a country's essential security interests. It does not limit the situations to which essential security interests can relate, as in the case of GATS, Article XIVbis.

The RCEP also has a specific security exception in the provision relating to data localisation. Essentially, all RCEP parties are free to impose any data localisation measure that they consider necessary for their essential security interests

[142] ibid Art 18.5. For a similar provision, see the UK–Singapore Digital Economy Agreement (Singapore, 25 February 2022), Art 8.61-O.28 (UKSDEA).
[143] UKSDEA, Art 8.61-L(1).
[144] ibid Art 8.61-L(2).
[145] CPTPP, Art 29.2.
[146] USMCA, Art 32.2.

and the same cannot be subject to any dispute.[147] A clarifying footnote further provides: 'the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party'.[148] In addition, the security exception contained in Article 17.13 (which in inspired by GATS, Article XIVbis) allows parties to impose measures necessary to protect essential security so as to 'protect critical public infrastructures including communications, power, and water infrastructures'. This provision can extend to measures related to protecting critical information infrastructure within a country.

As compared to GATS, Article XIVbis, the above PTAs provide for a much broader scope and policy space to accommodate different kinds of domestic cybersecurity-related measures. Given that there is an increasing awareness and acknowledgement among governments that cybersecurity must be safeguarded and the emphasis is on data/cyber sovereignty, the expanding scope and flexibility of exceptions is not surprising. Thus, in scenarios where countries adopt data-restrictive measures on grounds of cybersecurity, they may violate obligations contained in those PTAs (especially if there are disciplines on data localisation), but are more easily justifiable under the security exceptions contained in these PTAs.

Such flexible security exceptions may be seen favourably by countries that equate cybersecurity risks to national security threats. However, without a global consensus on cybersecurity norms and best practices/international standards, such provisions can lead to a multiplication of data-restrictive measures, in turn damaging to both global digital trade and digital security. Thus, increased cooperation and collaboration on cybersecurity issues is highly important, irrespective of whether it occurs through mechanisms contained in trade agreements or through interstate cooperation in other international organisations, political cooperation such as memoranda signed between different countries and consensus-building in multistakeholder/transnational bodies.

IV. ALIGNING INTERNATIONAL TRADE LAW WITH GLOBAL CYBERSECURITY GOVERNANCE

So far, the chapter has highlighted the important link between digital trade and cybersecurity and the various ways in which international trade law can apply to domestic cybersecurity-related data-restrictive measures. It has also outlined the various ways in which new-generation PTAs and DEAs have gradually started contributing towards building global cooperation on cybersecurity. This section examines if there are other ways in which international trade agreements can contribute to developing a global regulatory framework for cybersecurity.

[147] RCEP, Art 12.14.3.
[148] ibid Art 12.14.3, fn 12.

First, this section highlights the various ways in which the existing treaties can be meaningfully interpreted and applied to cybersecurity-related trade disputes, including data restrictions. Second, the section highlights the various ways in which trade bodies can develop new institutional mechanisms to facilitate transparent policy-making on cybersecurity measures affecting digital trade. Third, it argues that international trade law can foster a culture of more competitive and robust cybersecurity standard-setting, including fostering more interoperable standards, by referring to a broader range of multistakeholder and transnational technical standards in relation data/network security. Finally, this section highlights how international trade can facilitate co-option of relevant international best practices and norms on cybersecurity, including those developed in multistakeholder bodies.

A. Dealing with Disputes Pertaining to Cybersecurity-Related Data-Restrictive Measures

International trade law already contains several provisions that can potentially facilitate a better culture of global and domestic cybersecurity regulation. For instance, obligations on non-discrimination, market access and domestic regulation facilitate more certainty and openness in the digital services market. Further, rules on domestic regulation encourage adoption of more reasonable and objective cybersecurity regulations, for example in consonance with standards adopted by international organisations. Similarly, the necessity test in GATS, Article XIV and analysis under the GATS, Article XIV chapeau can prevent countries from imposing trade-restrictive and technologically inefficient measures, and is especially effective at curtailing protectionist measures disguised as cybersecurity measures.

In dealing with trade disputes pertaining to cybersecurity-related measures, trade tribunals must adopt an objective approach as far as possible. This would require the WTO or other dispute settlement panels to look carefully at available technical evidence (in addition to relevant legal evidence), including relying upon relevant inputs from technical experts in the field. As a parallel example, Annex 1 of the TBT Agreement provides specific requirements for constitution of a technical expert communities to resolve TBT-related trade disputes before WTO panels.[149] A similar mechanism can be developed in the context of resolving cybersecurity-related digital trade disputes.

Given the sensitivity of cybersecurity issues, trade bodies must avoid making an independent assessment of the acceptable level of cyber-risk for a country, and should instead make an assessment based on the stated preference of the country. A technical expert committee could provide them with input in case

[149] TBT Agreement, Annex 1.

of disputes, such as whether a particular measure is commensurate with the stated level of cyber-risk. This approach would also be practical (although not completely free of subjectivity risks) and perhaps more judicious in navigating data sovereignty concerns.

Ultimately, if a trade dispute leads to unsatisfactory consequences such as impeding on a country's data sovereignty or national security objective, it is likely to not implement such a decision, leading to further breakdown of trust and coherence in the trade regulatory framework.[150] Therefore, as argued below, developing a global consensus on cybersecurity regulation is important rather than solely using the exceptions as a basis for safeguarding their measures.

B. A Facilitative Role for International Trade Law in a Transnational Framework for Cybersecurity Governance

(i) Building Transparency and Cooperation on Cybersecurity Policy-Making

Several scholars have suggested proposals to deal with the increasing number of trade disputes that relate to national security considerations. For instance, Lester and Zhu have recommended a new WTO committee to examine security-related measures to find political solutions to resolve conflicts between countries, including possible compensation to the affected countries.[151] Lamp has proposed using the non-violation complaint mechanism in WTO law to resolve disputes related to the security exceptions.[152] Pinchis-Paulsen notes the possible ways in which retroactive disclosure of security-related measures may help create a stronger understanding of the measures being taken on national security grounds.[153] She suggests an expanded role for the WTO Secretariat, including a more expansive administrative role for the WTO in collecting information regarding security-related disputes.[154] Several of these proposals can also be applied in the cybersecurity context.

First, the existing WTO committees must be used more fruitfully to create more open, transparent discussions on security measures being taken in relation to digital and data-driven services, including key concerns and exchange of best practices. Second, trade-related cybersecurity disputes could be addressed in a specific committee (such as the proposed WTO committee on national security),

[150] Mishra (n 18) 579.

[151] S Lester and H Zhu, 'A Proposal for "Rebalancing" to Deal with "National Security" Trade Restrictions' (2019) 42(5) *Fordham International Law Journal* 1451, 1472.

[152] N Lamp, 'At the Vanishing Point of Law: Rebalancing, Non-violation Claims, and the Role of the Multilateral Trade Regime in the Trade Wars' (2019) 22(4) *Journal of International Economic Law* 721.

[153] M Pinchis-Paulsen, 'Let's Agree to Disagree: A Strategy for Trade-Security' (2022) 25(4) *Journal of International Economic Law* 527, 543.

[154] See generally ibid.

wherein, instead of litigating the same before WTO panels, parties may seek a political resolution to the disputes. If WTO members are able to develop sound mechanisms for reporting, classifying and cataloguing security measures (as proposed by Pinchis-Paulsen), this could lead to more fruitful political resolutions of cybersecurity-related trade concerns. Over a period of time, WTO members may also arrive at a consensus regarding the specific categories of cybersecurity measures that must remain permissible despite any trade-restrictive effects.

Third, existing disciplines such as GATS, Article VII could be developed further to create more avenues for developing mutual recognition mechanisms for cybersecurity standards, to the extent that interoperable solutions are possible. Finally, GATS, Article III already facilitates the transparency of measures affecting trade in services. This could be overseen by a specific committee under the WTO to ensure that members are reporting their measures on an ongoing basis. Even mechanisms such as the Trade Policy Review Mechanism (a peer review mechanism to examine trade policies of different WTO members on a regular basis) can become an important platform for WTO members to discuss unreported cybersecurity measures affecting cross-border data flows. As chapter seven will argue, creating an accurate catalogue of data-restrictive measures could be the first step to finding a common basis for regulating data-related issues in international trade law.

(ii) Facilitating an Open, Competitive Environment for Robust Standard-Setting

The majority of standard-setting on cybersecurity is not managed by state or intergovernmental bodies, but rather is carried out through informal trust-based relationships among private bodies, including Internet service suppliers, computer security incident response teams within companies/organisations, domain name registrars, hosting companies, IT departments and private security services.[155] Technology companies also adopt security standards to protect their intellectual property as well as personal data of their customers, such as credit card or personal identification details.[156] However, as explained in chapter two, trade treaties do not provide much legal basis to recognise standard-setting bodies that do not have a traditional participation mechanism for governmental bodies. This is because an international organisation has been defined as a

[155] LM Hurel and L Lobato, 'Unpacking Cybernorms: Private Companies as Norm Entrepreneurs' (Conference Presentation, GigaNet Annual Symposium, 2018); ML Mueller, *Networks and States: The Global Politics on Internet Governance* (Cambridge MA, MIT Press, 2010) 163.

[156] M Finnemore and DB Hollis, 'Constructing Norms for Global Cybersecurity' (2016) 110(3) *American Journal of International Law* 425, 453. See generally J Wolff, 'What We Talk About When We Talk About Cybersecurity: Security in Internet Governance Debates' (2016) 5(3) *Internet Policy Review* 1, 1–4; OECD, 'Digital Security Risk Management' (n 22) 19–20.

body whose membership is at least open to all WTO members, and would thus exclude several multistakeholder, private or transnational standards.

To address the above gaps, WTO members could agree to amend the term 'international organization' to be read more broadly in GATS, Article VI:5 to include relevant Internet multistakeholder institutions (particularly those allowing government participants). The Ministerial Conference and the General Council could then adopt an 'official interpretation' of GATS, Article VI:5 to that effect.[157] However, even in that case, this decision would require a three-quarters majority of the members.[158] Given the political tussle on cybersecurity standard-setting, it may be more realistic to adopt a broader definition of internationally recognised standards/international organisation in PTAs rather than at the WTO.

The question then is if WTO law would be at risk of becoming completely irrelevant in restricting the use of restrictive cybersecurity domestic standards.[159] For instance, even the well-established ISO standards, such as ISO 27001 on information security management systems, are currently being outpaced by industry standards,[160] owing to the fast-changing nature of security risks necessitating a dynamic response from the industry.[161] As cybersecurity standards on digital services are increasingly developed by industry consortia or other co-regulatory mechanisms, it is important to account for this in international trade law.

To achieve this goal, new disciplines are necessary that allow trade bodies to recognise and acknowledge cybersecurity standards that are being used in practice (ie more inclusive of private and multistakeholder standards even if they are not mandatory), and thereby facilitate wider adoption of globally competitive, open, interoperable and market-driven standards. This would prevent the fragmentation in digital trade flows arising from the use of domestic cybersecurity standards and reduce unnecessary compliance costs while facilitating economies of scale. However, in doing so, international trade agreements must be able to take account of both input and output legitimacy in the standard-setting process.[162]

Annex 3 of the TBT Agreement (Code of Good Practice for the Preparation, Adoption and Application of Standards) provides a helpful example in the context of trade in goods. This instrument provides for principles for standard-setting bodies that they can adopt voluntarily and focuses on different aspects of standard-setting, such as transparency, accountability of standard development

[157] Marrakesh Agreement Establishing the World Trade Organization (Marrakesh, 15 April 1994), Art IX:2.

[158] ibid Art IX:2.

[159] Peng (n 12) 448.

[160] ISO standards have traditionally been considered relevant in the context of TBT disputes, although there is no similar practice under the GATS due to the lack of relevant provisions.

[161] Peng (n 12) 452.

[162] See generally Delimatsis (n 51).

bodies and objectivity of standards. A decision of the TBT Committee further sets out the core principles that must be followed in the setting of international standards: transparency of standard-setting mechanisms; openness of standard-setting organisations; impartiality and consensus; effectiveness and relevance of standards; coherence of standards; and representing the interests of developing countries.[163] A similar initiative will be instrumental in the case of data-driven services and technologies, and must be included in trade treaties dealing with cross-border trade in services and/or digital trade.

Having a common framework for recognition of cybersecurity standards could help in organising greater alignment between domestic and international standards and limited situations in which prevailing global cybersecurity standards are unable to meet the policy requirements of a country. Some scholars have proposed that if countries agree to exercise due diligence using the TBT principles and require transparent reporting by private sector, it can result in reliable standards without harming the digital industry.[164] Further, such standards can be relevant in the context of deciding trade disputes such as determining the necessity of data-restrictive measures under GATS, Article XIV or the proportionality of standards under GATS, Article VI, provided the standards meet the requirements of WTO law, including being open, clear, objective and transparent.[165]

Another important aspect is representativeness of standards especially since several private and multistakeholder bodies are driven by the interests of large corporations based in developed countries.[166] It is important for developing countries to be able to voice their concerns and ensure that the standards are in tune with their domestic needs.[167] I address this aspect further in chapters five and seven, arguing that a standards framework in international trade law must include streamlined technical support for developing countries to contribute to the discussions in standard-setting bodies.

(iii) Incorporating Multistakeholder Norms and Best Practices by Reference

As discussed earlier, certain recent PTAs already recognise the role of multistakeholder dialogues on cybersecurity regulation and the importance of a risk-based

[163] WTO, 'Principles for the Development of International Standards, Guides and Recommendations', www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm. The ISO, for instance, takes into account these core TBT principles in the development of standards. See Delimatsis (n 51) 307.

[164] PC Mavroidis and R Wolfe, 'Private Standards and the WTO: Reclusive No More' (2017) 16(1) *World Trade Review* 1, 18.

[165] ibid 20. See also UN, 'The Age of Digital Interdependence: Report of the UN Secretary-General's High-Level Panel on Digital Cooperation' (2019) 19.

[166] For broader discussions on representativeness of technical standards, see A Berman, 'Industry, Regulatory Capture and Transnational Standard Setting' (2017) 111 *AJIL Unbound* 112, 113; Thorstensen et al (n 88) 2–4. See generally Gibson (n 88).

[167] See US – Tuna II (n 73) para 390 (setting out that universally accepted standards are more likely to meet the criteria for international standards).

approach in cybersecurity. While multistakeholder engagement is unusual at the WTO, initiatives such as the e-World Trade Platform[168] and the Global Supply Chains Forum[169] indicate more willingness in trade bodies to engage with newer forms of cooperation. Similar forms of informal, multistakeholder cooperation can be especially fruitful in areas such as cybersecurity regulation, where the private sector plays a key role in both devising/implementing technical standards and monitoring cyber-risks. Co-regulatory approaches are also common in cybersecurity governance and are acknowledged in certain recent PTAs. This approach is likely to be more effective than trying to resolve cybersecurity-related trade disputes by relying solely upon dispute settlement mechanisms in trade treaties. Thus, as chapter seven further argues, it is important to develop trade rules that permit the incorporation of multistakeholder and transnational norms and best practices by reference.

V. CONCLUSION

Cybersecurity is one of the most complex and significant challenges in global data governance as it is characterised by multiple policy objectives and regulated by different stakeholders. As more governments associate cybersecurity with national, economic and social security, the interface between international trade law and cybersecurity-related domestic laws and regulations is also becoming more complex. This chapter argued that international trade law can be relevant in the assessment of cybersecurity-related data-restrictive measures. This is because such measures often create barriers to digital trade. While governments can theoretically justify these measures under the exceptions contained in trade treaties, the application of the legal tests especially under the security exception entails both legal uncertainties and political risks. Further, this chapter pointed out how new-generation PTAs and DEAs play a more central role in acknowledging the importance of cybersecurity in digital trade and aim to achieve more international regulatory cooperation and competitive standard-setting to promote cybersecurity. However, several gaps remain in the existing rules in acknowledging the transnational nature of cybersecurity regulation and standard-setting.

This chapter therefore proposed various reforms in international trade law to align its rules better with global cybersecurity governance. In addition to more meaningful application of existing WTO rules, including disciplines on domestic regulation and transparency, this chapter proposed further reforms in

[168] 'How the eWTP Makes Global Trade Accessible to All' (Alizila, 21 March 2017) www.alizila.com/video/what-is-the-ewtp/.

[169] WTO, 'WTO Offers Unique Forum for Dialogue on Global Supply Chain Issues – DG Okonjo-Iweala' (21 March 2022) www.wto.org/english/news_e/news22_e/miwi_21mar22_e.htm.

trade treaties. First, it argued that institutional innovations can be considered at the WTO and other trade bodies for transparent reporting of cybersecurity measures and proposed ideas for political (rather than legal) resolution of cybersecurity-related trade disputes. Second, it proposed creating more avenues for trade bodies to acknowledge and incorporate globally competitive private and multistakeholder cybersecurity standards by reference. Finally, the chapter argued that international trade law must be more open and receptive to multistakeholder/co-regulatory solutions to develop a global consensus on cybersecurity norms and best practices.

4

Data Access, Digital Trade and Global Data Governance

I. INTRODUCTION

The datafication of our lives has radically shifted both the manner and the extent to which governments now seek to access and control data about us. Governments now impose a variety of measures to ensure reliable and immediate access and control over the data of their citizens. This chapter terms all such governmental measures 'data access measures'. Such measures may be necessary for several reasons, including regulatory supervision, ensuring accountability of companies providing digital services, and investigating crimes and other public security threats using electronic/digital evidence.[1] Although data access measures are driven by critical domestic policy considerations, including public order and security, they often take the form of data-restrictive measures such as data localisation and thus adversely affect cross-border data flows.[2] Further, if data access measures become widespread, they are likely to affect the overall functioning of the Internet as a global platform for communications and transactions.[3]

Data access measures raise many complex dilemmas for data governance, both domestically and transnationally. For instance, they can lead to deliberate violations of human rights, wherein governments can target dissidents or minority groups, or may systematically breach privacy rights of individuals.[4] Further, such measures can disrupt the globally distributed and decentralised architecture of the cloud computing industry.[5] At the same time, basic governmental functions such as enforcement of privacy and data security laws, oversight of technology companies, and investigation of crime and security threats are impossible without governments having meaningful (and often immediate)

[1] See s IIA.

[2] E Yayboke et al, 'The Real National Security Concerns over Data Localization' (CSIS, 23 July 2021) www.csis.org/analysis/real-national-security-concerns-over-data-localization.

[3] Global Commission on Internet Governance, *A Universal Internet in a Bordered World – Research on Fragmentation, Openness and Interoperability*, vol 1 (2016) 86–89.

[4] See generally A Shahbaz et al, 'User Privacy or Cyber Sovereignty?' (Freedom House, July 2020) 5–7.

[5] J Daskal, 'Borders and Bits' (2018) 71(1) *Vanderbilt Law Review* 179, 186.

access to data of people/transactions within or related to their jurisdiction. Therefore, several initiatives are ongoing in different international and transnational bodies to understand how access to data can be facilitated in line with domestic laws such as data protection law and the fundamental principles of reasonableness, proportionality and due process.[6]

Similar to the last two chapters, this chapter investigates how data access measures directly impact cross-border data flows and implicate international trade law. As most companies increasingly rely on cloud computing solutions and Big Data processing, data access measures pose an inevitable barrier for those companies that rely on multi-country data storage and processing models and also lead to a high degree of legal uncertainty for their global operations.[7] This chapter therefore focuses on the interface between data access measures and international trade law to investigate how existing rules apply to such measures; the various global and transnational policy responses to the problems of governmental data access; and whether trade law can help resolve the tension between data access measures and cross-border data flows.

Section II begins by explaining the key rationales behind data access measures and then discusses some common tools used by governments to facilitate data access. The two most common policy rationales behind governments seeking data access are regulatory supervision and conducting investigations and law enforcement actions. However, governments may have other policy considerations behind such measures, such as enhancing their intelligence capabilities or facilitating new models of data sharing within their jurisdiction. The most common measure to facilitate governmental data access is data localisation; this may take various forms, such as requirements to store a copy of the data within the country, a complete ban on the transfer of data outside of the country or an elaborate regulatory approval process. Further, certain domestic laws may explicitly prohibit companies from transferring data abroad except through specified mechanisms, such as mutual legal assistance treaties (MLATs), even where the foreign government has a legitimate basis for requesting access to data.

Section III highlights the tension arising between data access measures and cross-border data flows due to the restrictive nature of these measures and whether such restrictions conflict with rules applicable to digital trade. Certain requirements in domestic laws, such as an explicit requirement to store data domestically or the complex processes necessary to obtain regulatory approvals for cross-border data transfers, can constitute barriers to digital trade. As already discussed in chapters two and three, these requirements can violate

[6] See the discussion in s IVA.

[7] See, eg B Smith, 'A Call for Principle-Based International Agreements to Govern Law Enforcement Access to Data' (Microsoft, 11 September 2018) www.blogs.microsoft.com/on-the-issues/2018/09/11/a-call-for-principle-based-international-agreements-to-govern-law-enforcement-access-to-data/.

non-discrimination, market access and domestic regulation requirements contained in the General Agreement on Trade in Services (GATS) and other preferential trade agreements (PTAs). While governments can argue that these restrictions relate to important policy objectives, they must be justified under the available exceptions in the trade treaties. For instance, a financial regulator can require all financial records to be stored domestically for supervisory reasons, but this must be justified as being necessary to achieve certain key public interests. The legal test under the exceptions raises several questions regarding the proportionality and reasonableness of data access measures.

Even though the conflict between governmental access to data and digital trade is evident, international trade law has so far played a limited role in addressing this tension. Certain existing PTAs contain specific clauses in relation to some of these data access requirements, especially in the financial sector. However, most meaningful initiatives expectedly occur outside trade law and are often focused on issues of law enforcement and the investigation of crimes. Section IV discusses such initiatives, which may be state-led (eg USA's Clarifying Lawful Overseas Use of Data Act (CLOUD Act)),[8] EU's e-Evidence Regulation[9]) or developed by regional or multistakeholder bodies such as the Organisation for Economic Co-operation and Development (OECD) and the Global Privacy Assembly (GPA). The Second Protocol to the Budapest Convention also addresses certain aspects of governmental access to data in the context of investigating and prosecuting cybercrimes. These initiatives can provide a core foundation for digital trust among governments inter se and between governments and businesses. Yet, there is a visible fragmentation in this area of regulation, particularly between the CLOUD Act and the requirements in data protection laws such as the General Data Protection Regulation (GDPR).

While international trade law has so far largely remained silent, it can play a more meaningful role in the complex global framework for governmental access to data, as set out in the concluding part of the chapter. First, countries negotiating digital trade agreements could agree to also sign up to the high-level principles and norms on data access and sharing set out in the OECD declaration or other similar instruments. This approach is more robust and feasible than relying upon MLATs or bilateral negotiations based on specific statutes such as the CLOUD Act. It is also possible that if more countries agree to sign up to the Budapest Convention and Second Protocol, this may deter countries from adopting blocking statutes and instead motivate them to develop more robust mechanisms for international cooperation.

[8] Clarifying Lawful Overseas Use of Data Act (CLOUD Act) [2018] HR 4943.

[9] Council of the European Union, 'Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Proceedings and for the Execution of Custodial Sentences Following Criminal Proceedings' (20 January 2023) 2018/0108(COD).

Second, as regards enabling regulatory supervision, any requirements prohibiting data localisation in digital trade agreements must be accompanied by a requirement that all service providers are under an obligation to provide regulators with relevant data irrespective of the location if such data requests follow basic requirements of legitimacy and due process. The Agreement between the United States of America, the United Mexican States, and Canada (USMCA) provides some helpful language in this regard, as discussed in greater detail later in this chapter. Similarly, trading partners may also reach a consensus on prohibiting governments from imposing mandatory requirements on service providers to share their cryptographic keys in order to access markets.

Finally, to the extent that trade disputes arise in relation to data access measures, trade tribunals must be equipped to factor in the evolving transnational norms on data access to enable more judicious resolution of these disputes, especially acknowledging that governments seek data access for a broad range of legitimate and important regulatory purposes.

II. POLICY RATIONALE AND TOOLS FOR GOVERNMENTAL ACCESS TO DATA

Before considering the interface between data access measures and international trade law, this section first outlines the key regulatory rationales driving those measures and the various ways in which governments try to secure access to data. The key regulatory rationales are: law enforcement and the investigation of crimes; regulatory audits and supervision; strengthening intelligence capabilities; and enabling data sharing to boost domestic competition. The section then highlights the key ways in which data access measures are operationalised: data localisation and other restrictions on data flows; direct access requests; and measures ensuring governmental access to cryptographic keys.

A. The Regulatory Rationale Behind Data Access

(i) Law Enforcement and the Investigation of Crimes

The most common rationale for data access measures is the need for law enforcement agencies to rely upon digital data, such as emails and user location, and communications made through messaging/social media apps to investigate crimes.[10] A large part of criminal investigation now revolves around electronic

[10] UNSC CTED, 'The State of International Cooperation for Lawful Access to Digital Evidence: Research Perspectives' (January 2022) CTED Trends Report.

or digital evidence.[11] Even the UN Security Council has recognised the increasing need to use digital data and evidence to investigate serious offences, including terrorist acts.[12]

Governments can access electronic or digital evidence in two ways: either by tapping information flows from the Internet networks (upstream surveillance) or by getting access to these communications from such digital service providers as technology companies and social media platforms (downstream surveillance).[13] Typically, there are three categories of data requested by government agencies from private companies as a part of their law enforcement activities: subscriber data, indicating the user of the digital service; traffic/transactional data, providing information about the origin, duration and access of a digital service; and content data, referring to the content, such as emails, texts and file attachments.[14] There may be some overlap between these data categories; the legal threshold to access content data is usually the most stringent.[15]

Due to the distributed nature of data storage and processing, companies often store such digital data in various jurisdictions, and sometimes this data may also be partitioned and stored in different countries.[16] This means that the law enforcement agency of a country would often be unable to access the relevant data for investigating local crimes as it may be stored in overseas servers or the agency may not even be aware of the exact location of such data.[17] This problem intensifies for developing countries, where law enforcement agencies may have limited regulatory capacity and weaker cyber-intelligence capabilities than developed countries.[18] The problem is further complicated because several countries have adopted blocking statutes, preventing service providers located

[11] T Cochrane, 'Law Enforcement Cross-Border Data Sharing: A CLOUD Act Agreement for Aotearoa New Zealand?' (2021) 3 *New Zealand Law Review* 401, 403.

[12] UNSC Res 2322 (12 December 2016) UN Doc S/Res/2322.

[13] EFF, 'Upstream vs PRISM', www.eff.org/pages/upstream-prism.

[14] Internet & Jurisdiction Policy Network, 'Framing Brief: Categories of Electronic Evidences' (31 May 2022) Ref 22/102.

[15] ibid.

[16] HH Abraha, 'Law Enforcement Access to Electronic Evidence across Borders: Mapping Policy Approaches and Emerging Reform Initiatives' (2021) 29(2) *International Journal of Law and Information Technology* 118, 122; Sometimes this is framed as 'loss of location'.

[17] L Krahulcova and D Mitnick, 'Council of Europe Cooperation Against Cybercrime – Human Rights Octopus or Fishy Deals?' (*Accessnow*, 11 July 2018) www.accessnow.org/council-of-europe-cooperation-against-cybercrime-human-rights-octopus-or-fishy-deals/; Abraha (n 16) 121; M Molinuevo and S Gaillard, 'Trade, Cross-Border Data, and the Next Regulatory Frontier: Law Enforcement and Data Localization Requirements' (2018) 3 *MTI Practice Notes* 2. Some scholars have argued that the data access debate is not specifically complex for the global cloud and can be dealt with using the same principles of jurisdictional conflict applicable in the non-digital world. See AK Woods, 'Against Data Exceptionalism' (2016) 68 *Stanford Law Review* 729.

[18] See, eg UNODC, 'UNODC and Partners Release Practical Guide for Requesting Electronic Evidence across Borders' (1 February 2019) www.unodc.org/unodc/en/frontpage/2019/January/unodc-and-partners-release-practical-guide-for-requesting-electronic-evidence-across-boarders.html.

in one country from voluntarily responding to direct data requests from the law enforcement agency of another country.[19] In particular, smaller-sized technology companies are likely to find it extremely difficult to navigate such a complex web of blocking statutes while complying with multiple government requests for data access.[20]

In scenarios where a country does not have jurisdiction over data stored in foreign servers, the most feasible option is to use available MLATs or for courts to issue Letters Rogatory to formally request such data. An MLAT is a treaty signed by two countries agreeing to exchange information for the purposes of law enforcement. Letters Rogatory are formal requests that can be sent by the court of one country to a court of another country to obtain certain information, though they are not relevant at the stage of investigation of crimes.[21] These mechanisms are, however, ill-suited for meaningful access to data in a digitalised world and there is a clear shift to either drastically reform them or seek other political alternatives.[22]

Several reasons undermine the effectiveness of MLATs in a digital world.[23] First, the process under MLATs is extremely slow and does not match the pace of online transactions, where data can be deleted or moved instantly. In some scenarios, the investigating authorities may not even know the exaction location of the data given the distributed nature of cloud computing.[24] Second, not all countries have MLATs with other countries. As MLATs operate as bilateral treaties, the reform of the MLAT system is likely to be insufficient to deal with data access problems, as it is impossible to scale it up to the global level. An estimate made by La Chapelle and Fehlinger indicates that establishing bilateral arrangements between 190 countries would require more than 15,000 MLATs.[25] Thus, service providers can always escape data requests by relocating data to a country

[19] For instance, under the Electronic Communications Privacy Act of the USA, service providers can only provide access to subscriber and traffic data in response to foreign law enforcement requests but cannot provide access to content data. To obtain such data, the foreign government must avail itself of the MLAT mechanism.

[20] The UNODC has developed certain guides, such as the Data Disclosure Framework and the Standardized Data Request Forms, to guide how companies can respond to government requests for data access. See UNSC CTED (n 10) 19.

[21] A Boutros, 'The Key Tools of the Trade in Transnational Bribery Investigations and Prosecutions: Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory' in TM Funk and A Boutros (eds), *From Baksheesh to Bribery: Understanding the Global Fight Against Corruption and Graft* (New York, Oxford University Press, 2019) 548–9.

[22] Abraha (n 16) 118.

[23] While this chapter focuses on international initiatives for enabling cross-border data access, there are certain domestic laws that address this problem head on. For instance, the Kingdom of Bahrain enacted a law wherein any data stored in servers in Bahrain would be subject to the domestic law of the data subject, thus solving the problem of jurisdictional conflict. See Legislative Decree No 56 of 2018, In Respect of Providing Cloud Computing Services to Foreign Parties.

[24] Abraha (n 16) 122.

[25] BD La Chapelle and P Fehlinger, 'Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation' (April 2016) Global Commission on Internet Governance Paper Series No 28, 12–13.

that has not yet signed an MLAT with the government making the data request or where authorities are likely to be unresponsive to data access requests.[26]

In the absence of other reliable international frameworks and the inefficiency of the MLAT system, governments therefore face an urgent crisis when investigating serious crimes, where the digital evidence could be deleted or lost easily. Thus, one of the primary drivers behind several data access measures is to secure reliable data access for law enforcement purposes. In addition to increasing compliance burdens for companies engaging in cross-border digital trade (as discussed in section IIIA below), these measures can implicate privacy violations and other human rights.

(ii) Regulatory Audits and Supervision

Another key policy rationale behind data access measures is conducting regulatory functions, such as audits and inspections, or ensuring the accountability of service providers for illegal conduct and ensuring remedies for individuals who have suffered harm therefrom. As an example of the former, in most jurisdictions, financial regulators scrutinise the data collected by various financial or electronic payment services to ensure that there are no illegal activities, particularly in the context of money laundering and terrorism financing. As an example of the latter, a regulator may pursue action against a company that, for instance, breaches domestic data protection or consumer protection laws. For instance, as chapter two discusses, in the absence of a coherent global framework for cross-border enforcement of data protection law, governments may find it easier to pursue action against companies having a local commercial presence, including local data operations.

Several countries impose data transfer restrictions in specific sectors, such as finance or insurance, in order to ensure steady and reliable access to data for conducting regulatory supervision/audits. For instance, Indonesia imposed the Regulation on Governance of Private Scope Electronic System Administrators in 2020, which requires all electronic system administrators (theoretically covering a broad range of companies) to obtain permission from the domestic regulator for the management, processing and storing of data.[27] This law provides broad powers to the government to require local data storage for the purposes of preserving various national interests, including regulatory supervision.[28] In India, the central banking regulator has imposed a strict requirement for

[26] Molinuevo and Gaillard (n 17) 3–4.

[27] Zico Law, 'Indonesia's New Regulation on Private Electronic System Operators: Important Notes for Corporate Compliance of Domestic and Foreign Information Technology Companies' (11 May 2021) www.zicolaw.com/resources/alerts/indonesias-new-regulation-on-private-electronic-system-operators-important-notes-for-corporate-compliance-of-domestic-and-foreign-information-technology-companies/.

[28] N Cory and L Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them' (ITIF, July 2021) 46.

all payment systems data to be stored within India,[29] and even temporarily banned MasterCard for violating this law.[30]

(iii) Strengthening Indigenous Intelligence-Gathering Operations

Another possible reason for countries to impose restrictions on cross-border data flows and strengthen governmental access to data is because it enables governments to conduct more effective surveillance to strengthen their own intelligence.[31] This intelligence may, for instance, be relevant in detecting national security threats and other critical threats to the economy or society. In the aftermath of the Snowden leaks in 2013, governments have remained wary that the excessive use of foreign data infrastructure and networks can be prejudicial to national security, as foreign governments may 'weaponise' them by tapping them to gather information or cutting off access to adversary states.[32] This fear is coupled with increasing recognition that indigenous intelligence capabilities can also be vital to the protection of various national interests. With more security and intelligence agencies now having access to new cyber-intelligence techniques, this phenomenon is far more common; yet, as Georgieva argues, these entities are often less visible internationally as they operate as sub-state entities.[33]

(iv) Enabling Data Sharing for Domestic Competition

While the key policy rationales behind data access measures usually relate to various regulatory and law enforcement activities, certain governments may mandate access to data to facilitate digital innovation in the domestic economy.[34] As chapter six will argue, due to the presence of a few powerful digital ecosystems in the world, data is often stored in silos, trapped within walled gardens. For smaller companies, especially those based in developing countries, the lack of access to data can be a major constraint to innovation and competing in the digital markets. Therefore, certain governments have proposed measures requiring private companies to share anonymised datasets to enable both community ownership of data and facilitate healthy competition in the domestic digital

[29] Reserve Bank of India (RBI), 'Storage of Payment System Data' (6 April 2018) DPSS.CO.OD. No 2785/06.08.005/2017-18.

[30] M Singh, 'India Lifts Ban on Mastercard' (TechCrunch, 16 June 2022) www.techcrunch.com/2022/06/16/india-lifts-ban-on-mastercard/.

[31] J Selby, 'Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?' (2017) 25(3) *International Journal of Law and Information Technology* 213, 228.

[32] H Farrell and AL Newman, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion' (2019) 44(1) *International Security* 42.

[33] I Georgieva, 'The Unexpected Norm-Setters: Intelligence Agencies in Cyberspace' (2020) 41(1) *Contemporary Security Policy* 33, 34.

[34] OECD, *Enhancing Access to and Sharing of Data* (26 November 2019).

economy. For instance, India had proposed a draft framework for non-personal sharing in 2020[35] and the EU has developed the Data Governance Act[36] and Data Act[37] to foster more data sharing and healthy competition in the domestic economy.[38] Such measures contain provisions requiring companies to mandatorily share non-personal data with the government and other market players in order to ensure more vigorous competition in the domestic digital markets.

B. Measures Facilitating Governmental Access to Data

(i) Data Localisation and Restrictions on Data Flows

The simplest route to ensure that governments have jurisdiction over data is to enforce data localisation requirements.[39] Usually, such requirements take the form of measures requiring companies to store and/or process data using servers located within the country. In addition, localisation requirements may entail companies establishing local operations with a local office, a designated representative and a local bank account. For instance, in India, in order to ensure access to data for regulatory oversight, the central banking regulator issued a directive requiring all payment service providers to store 'the entire data relating to payment systems operated by them … in a system only in India'.[40] Similar restrictions exist in Turkey,[41] the UAE[42] and Vietnam.[43]

The key assumption behind a localisation measure is that the domestic law will apply to all local operations and, therefore, the government is in a stronger position to demand access to data when it is necessary for regulatory or law enforcement purposes.[44] This viewpoint especially makes sense given that the

[35] Ministry of Electronics and Information Technology, 'Report by the Committee of Experts on Non-Personal Data Governance Framework' (2020) 111972/2020/CL&ES.

[36] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)' COM(2020) 767 final.

[37] European Commission, 'Data Act: Commission Proposes Measures for a Fair and Innovative Data Economy' (23 February 2022) www.ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

[38] See also Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union (Non-Personal Data Regulation) [2018] OJ L303/59.

[39] Daskal (n 5) 180.

[40] RBI (n 29).

[41] A Babalioglu and N Uğurlu, 'Data Localisation Requirements in Turkiye' (Lexology, 24 January 2023) www.lexology.com/library/detail.aspx?g=e132f92b-6691-45f8-a24c-3beef84be555.

[42] Regulatory Framework for Stored Values and Electronic Payment Systems (Digital Payment Regulation) C6/2020 (UAE).

[43] J Fox, 'How Are Foreign Investors Responding to Vietnam's New Data Localization Regulation' (*Vietnam Briefing*, 23 September 2022) www.vietnam-briefing.com/news/how-are-foreign-investors-responding-to-vietnams-new-data-localization-regulation.html/.

[44] UNSC CTED (n 10) 6; Abraha (n 16) 130.

framework for both cross-border data access and extraterritorial enforcement of domestic laws such as data protection law are complicated and fragile.

While the localisation approach is intuitive and logical at first sight, such requirements are harmful for digital trade and particularly impact small and medium enterprises lacking sufficient resources to localise operations in every jurisdiction where their digital services and applications are accessible.[45] The Financial Stability Board has also pointed out that data localisation measures weaken the ability of companies to implement global risk management and compliance programmes, thus prejudicing the integrity of financial systems.[46] Finally, data localisation could be counterproductive to national security as it may actually facilitate surveillance by localising data in specific geographies.[47]

In addition to de jure localisation measures, several countries impose stringent restrictions on companies preventing them from transferring data abroad. Such restrictions are typically found in data protection laws, but they can also be prescribed in other laws and regulations. For instance, the Data Security Law in China prohibits the cross-border transfer of data stored in China (irrespective of where it was collected from) to a foreign law enforcement agency without obtaining regulatory approval.[48] This law aligns with China's Personal Information Protection Law, which requires companies transferring personal data abroad to obtain the approval of the domestic regulator.[49] China's example is not an isolated one; the majority of jurisdictions across the world have now adopted a complex framework for the transfer of personal data.[50] Further, the Data Governance Act of the EU identifies that transfer of personal data to a foreign government body may hamper national security or defence interests of EU Member States.[51] As Yakovleva argues, this indicates a marked shift in the EU's cross-border data governance framework, as previously cross-border data transfer restrictions under the GDPR were premised only on protecting the privacy of individuals.[52]

[45] See generally M Bauer et al, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery' (2014) ECIPE Occasional Paper No 3; D Medine, 'Data Localization – a Hidden Tax on the Poor' (CGDev, 27 March 2023) www.cgdev.org/blog/data-localization-hidden-tax-poor.

[46] Financial Stability Board (FSB), 'Third-Party Dependencies in Cloud Services' (9 December 2019)14; FSB, 'Regulatory and Supervisory Issues relating to Outsourcing and Third-Party Relationships' (14 June 2021) 4.

[47] A Chander and UP Le, 'Data Nationalism' (2015) 64(3) *Emory Law Journal* 677, 739.

[48] People's Republic of China, Data Security Law of the People's Republic of China (10 June 2021) Order of the President No 84 (see particularly Arts 26 and 31).

[49] 'The PRC Personal Information Protection Law (Final): A Full Translation' (*China Briefing*, 24 August 2021) www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/.

[50] See, eg the various reports compiled in IAPP 'International Data Transfers', www.iapp.org/resources/topics/international-data-transfers/.

[51] Regulation (EU) 2022/868 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L152/1, recital 22.

[52] S Yakovleva, 'On Digital Sovereignty, New European Data Rules, and the Future of Free Data Flows' (2022) 49(4) *Legal Issues of Economic Integration* 339, 344.

(ii) Direct Access Requests to Service Providers

Given the unreliability of the MLAT mechanism and the lack of an international framework, several countries are now considering a legal framework that empowers the government to request direct access to overseas data. One of the most frequently discussed examples is the CLOUD Act, which allows the US courts to issue an order for direct access to data in the 'possession, custody or control' of US companies irrespective of where this data is located at the time of the order.[53] This legislation was passed in order to resolve the dispute between the Federal Bureau of Investigation in the USA and Microsoft in relation to a warrant issued under a US domestic law to access personal data stored in Microsoft servers in Ireland.[54] Given the worldwide presence of US companies, this legislation was seen as a viable solution to the slow and cumbersome process under the MLATs. This law also provides the US authorities with almost unqualified, universal access to data,[55] especially as the authorities no longer need to know the exact location of data.[56]

The CLOUD Act also provides an avenue for the US government to negotiate bilateral reciprocal agreements with foreign countries, wherein a foreign country can make direct requests to service providers for data in the USA and vice versa, thereby bypassing the MLAT process.[57] For instance, the UK signed a bilateral agreement with the USA in 2019 for cross-border data access for law enforcement under the aegis of the CLOUD Act.[58] The Preamble of the US–UK CLOUD Agreement recognises not only the need for timely access to digital data for law enforcement purposes, but also the 'harms of data localisation requirements to a free, open, and secure Internet'.[59] Australia also signed an agreement with the USA under the framework of the CLOUD Act in 2021.[60] Some civil society bodies have argued that the mechanism established under the CLOUD

[53] Clarifying Lawful Overseas Use of Data Act (CLOUD Act), 2018, HR4943, §2713.

[54] *United States v Microsoft Corp* [2018] 584 US ___, 138 S Ct 1186. Another relevant case is the dispute between the Belgian government and Yahoo!, wherein the Belgian Supreme Court held that Yahoo! was legally bound to hand over data to the Belgian law enforcement agency, even though Yahoo! had no commercial presence in the country. See P L'Ecluse and T D'Hulst, 'Belgium: Supreme Court Condemns Yahoo for Failure to Cooperate with Belgian Law Enforcement Officials' (Mondaq, 11 January 2016) www.mondaq.com/corporate-and-company-law/456514/supreme-court-condemns-yahoo-for-failure-to-cooperate-with-belgian-law-enforcement-officials.

[55] Cochrane (n 11) 404; Abraha (n 16) 149–53.

[56] Cochrane (n 11) 405.

[57] This could be in addition to bilateral arrangements for information sharing. For instance, the USA and the EU signed an agreement in relation to exchange of personal data regarding law enforcement matters so as to develop a common approach towards dealing with criminal offences.

[58] Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime (Washington, 03 October 2019) (US–UK CLOUD Agreement).

[59] ibid.

[60] Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (Washington, 15 December 2021).

Act for exchanging data with foreign countries lacks the oversight mechanism and safeguards common to MLATs.[61] Others have argued that this mechanism disregards sovereign interests of other countries.[62] Further, due to the requirements under the CLOUD Act, US service providers are likely to collect more information about their users' identity to facilitate ready compliance.[63]

The CLOUD Act is likely to conflict with other foreign laws prohibiting cross-border transfer of data. For instance, the CLOUD Act explicitly states that the US law can apply to US companies irrespective of where they store or process data. Thus, US service providers are under an obligation to provide data to the US government for law enforcement purposes. However, these US service providers could also be storing and processing data in other jurisdictions that have adopted blocking statutes prohibiting private companies from disclosing data in response to foreign government requests, including the US government.[64] For example, US service providers operating in the EU are likely prohibited under the GDPR to respond to an order from the US government to hand over personal data stored in the EU.[65] In 2015, Microsoft had responded to this evident conflict by setting up a data trustee model wherein it partnered with a German company to oversee customer data in Germany; however, this model was discontinued in 2018 and Microsoft set up its own data centres in Germany to optimise its business efficiency.[66]

The EU has also developed a framework, called the e-Evidence Regulation, to facilitate quick and efficient access to cross-border digital evidence by EU authorities for law enforcement purposes.[67] This regulation creates a mechanism called European production and preservation orders that can be issued by judicial authorities in EU Member States. These orders can be used to obtain or preserve different categories of data, such as subscriber, traffic or content data. The Regulation provides certain legal thresholds for crimes, such as the nature of offences and minimum periods of punishment, for which such orders can be

[61] K Propp, 'European Cybersecurity Regulation Takes a Sovereign Turn' (*European Law Blog*, 12 September 2022) www.europeanlawblog.eu/2022/09/12/european-cybersecurity-regulation-takes-a-sovereign-turn/.

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

[63] PM Schwartz, 'Legal Access to the Global Cloud' (2018) 118 *Columbia Law Review* 1681, 1688.

[64] Abraha (n 16) 123.

[65] See in particular Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, Art 48 (GDPR); P Church and CP Metcalf, 'US CLOUD Act and GDPR – Is the Cloud Still Safe?' (Linklaters, 13 September 2019) www.linklaters.com/en/insights/blogs/digilinks/2019/september/us-cloud-act-and-gdpr-is-the-cloud-still-safe.

[66] E Dedezade, 'Microsoft to Deliver Cloud Devices from New Datacentres in Germany in 2019 to Meet Evolving Customer Needs' (Microsoft, 31 August 2018) www.news.microsoft.com/europe/2018/08/31/microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs/.

[67] Council of the European Union (n 9).

issued. All companies offering digital services to EU residents will be required to designate a local representative to respond to these orders.[68]

(iii) Access to Cryptographic Keys

Even when governments can obtain a mandate to access data through the domestic law, this data may be encrypted by the service provider. In order to decrypt the data, governments need access to cryptography or encryption keys, which are used to scramble data in order to protect user privacy and data security.[69] To overcome this obstacle, governments adopt laws imposing restrictions on the use of encryption standards in digital technologies[70] and/or mandating access to cryptographic keys for deciphering or decrypting any encrypted data under specific circumstances.[71] Such measures are increasingly common as digital service providers often adopt end-to-end encryption technologies to protect user privacy and data security.[72] Further, several mainstream companies, such as Meta and Google, use forward secrecy protocols in their services, wherein each electronic transaction is encrypted with a unique key.[73]

Several examples exist where countries have adopted laws enabling governmental access to cryptographic keys. For instance, the Australian Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 introduced various amendments to Australian domestic laws providing power to government agencies to demand that 'designated communications providers' create a capability to provide access to encrypted communications and data.[74] Similarly, in India, the central and state governments can compel assistance from any 'subscriber or intermediary or any person in charge of the computer resource'

[68] For a general discussion of this regulation, see V Mamir, 'Anchoring the Need to Revise Cross-Border Access to e-Evidence' (2020) 9(3) *Internet Policy Review* (online) policyreview.info/articles/analysis/anchoring-need-revise-cross-border-access-e-evidence.

[69] Cloudflare, 'What Is a Cryptographic Key?', www.cloudflare.com/learning/ssl/what-is-a-cryptographic-key/.

[70] These restrictions are also driven by the fact that the majority of encryption technologies are developed by powerful tech companies, mostly based in the USA. See R Budish et al, 'Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects' (Hoover Institution, 2 March 2018) Aegis Series Paper No 1804, 9; see also Law No 86/2015/QH13 on Network Information Security (2015, Vietnam); USTR, '2015 Report on the Implementation and Enforcement of Russia's WTO Commitments' (December 2015) 14–15.

[71] See Global Partners Digital, 'World Map of Encryption Laws and Policies', www.gp-digital.org/world-map-of-encryption/; S Kantor and V Scott, 'Australia's First-in-the-World "Decryption" Laws Will Impact Tech Providers Globally' (IAPP, 20 December 2018) www.iapp.org/news/a/australias-first-in-the-world-decryption-laws-will-impact-tech-providers-globally/.

[72] 'Use of Enterprise Encryption Technologies Worldwide in 2021, by Business Area' (Statista, May 2022) www.statista.com/statistics/529961/worldwide-enterprise-encryption-use-by-area/.

[73] S Lewis, 'Perfect Forward Secrecy (PFS)' (TechTarget, September 2018) www.TechTarget.com/whatis/definition/perfect-forward-secrecy.

[74] Telecommunications and Other Legislation Amendment (Assistance and Access) Act (2018) No 148/2018, sch 1, s 317.

in decrypting information.[75] The Indian government has taken action against Twitter and WhatsApp for not providing access to decrypted data in relation to specific requests.[76] In Brazil, the Marco Civil da Internet permits the Brazilian law enforcement agency to make direct requests to companies operating within the country to share specific data necessary for investigating crimes.[77] The Brazilian government has implemented this provision against companies such as Facebook (now Meta) when they have refused to provide user information.[78]

The OECD has set out specific guidelines on the factors to be taken into account in adopting such encryption-related measures, including the benefits to public safety and national security, the risks of misuse, the costs of implementation of such measures and the various safeguards necessary to ensure that any data obtained through the process is used lawfully by governments.[79] Technical experts have also pointed out that the legal requirements for cryptographic keys can result in severe security vulnerabilities.[80]

The discussion in this section indicates that governments act upon different policy incentives in imposing data access measures. While regulatory supervision and law enforcement are the primary factors, governments may also be seeking other policy goals, such as strengthening their intelligence capabilities or even promoting the domestic digital sector. Data access measures typically hamper the global business models of technology companies. While data-restrictive measures are the most common tools to ensure data access, governments are increasingly also adopting other sophisticated mechanisms, such as direct access to data and cryptographic keys, to strengthen their control over domestic data. All these measures, however, inevitably have severe, adverse consequences for global digital trade flows, as discussed in the next section.

III. DATA ACCESS MEASURES AND INTERNATIONAL TRADE LAW

This section argues that data access measures can affect digital trade both directly and indirectly, as well as undermine the digital trust necessary to develop

[75] Information Technology Act, No 21 of 2000 (India), s 69, as amended by the Information Technology (Amendment) Act, 2008, No 10 of 2009.

[76] A Pratap, 'WhatsApp's Fight with the Indian Government Over its Data Privacy Rules May Have Global Reverberations' (Forbes, 15 June 2021) www.forbes.com/sites/aayushipratap/2021/06/15/whatsapps-fight-with-the-indian-government-over-its-data-privacy-rules-may-have-global-reverberations/?sh=41f660e15a7a.

[77] Marco Civil Law of the Internet in Brazil (2014) Law No 12.965, Art 10.

[78] V Sreeharsha and M Isaac, 'Brazil Arrests Facebook Executive in WhatsApp Data Access Case' (*New York Times*, 1 March 2016) www.nytimes.com/2016/03/02/technology/brazil-arrests-facebook-executive-in-data-access-case.html. See also the examples discussed in Molinuevo and Gaillard (n 17) 3–4.

[79] OECD, 'Recommendation of the Council Concerning Guidelines for Cryptography Policy' (27 March 1997) OECD/Legal/0289.

[80] See, eg H Abelson, 'Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications' (2015) 1(1) *Journal of Cybersecurity* 69.

a global framework for cross-border data flows. Therefore, such measures may implicate various obligations contained in international trade agreements. While it is possible to justify certain data access measures under specific exceptions, such as protecting public morals/public order or ensuring compliance with domestic laws, the legal threshold to satisfy these exceptions is high. This section argues that several data access measures may fall below this threshold, thereby raising challenging questions for the regulation of both digital trade and cross-border data flows.

A. Data Access Measures and Digital Trade Flows

As alluded to in section II, data access measures can adversely affect how technology and data-driven companies conduct business across borders. First, data access measures inevitably put companies in a difficult position, wherein a company may be obliged to comply with conflicting laws of two different jurisdictions. For instance, while the CLOUD Act imposes a mandatory requirement for US companies to share data with the US government irrespective of the location, this data could be stored in a country with a blocking statute. Consequently, companies would be placed in a position of legal uncertainty and may eventually choose to localise their data operations in every country in which they operate, even if it is technologically and economically inefficient. Relatedly, de facto data localisation increases compliance costs and, as argued in previous chapters, can be particularly burdensome for small-sized companies and smaller developing economies, where foreign companies have little incentive to invest in data infrastructure.

Second, data access measures have visibly adverse consequences for human rights. For instance, as discussed in the last section, the proliferation of laws enabling direct access data requests would force cloud companies to collect more private information about their users to equip themselves with the information necessary to comply with such requests. Further, sufficient checks and balances to protect rights and liberties of peoples may be absent in certain domestic data access measures. Therefore, the data accessed by the government could be misused to target minority groups or dissident voices within society. Although this is not directly a trade-related issue, a robust framework for cross-border data flows can have an incidental, positive impact on human rights such as freedom of expression and access to information.[81]

Third, data access measures undermine digital trust and prejudice data security. As argued in the section above, cloud computing business models are secure due to their decentralised architecture. However, to comply with data

[81] See generally A Chander, 'International Trade and Internet Freedom' (2008) 102 *Proceedings of the ASIL Annual Meeting* 37.

access measures, several companies may be forced to either localise their data operations or agree to provide governmental access to exceptional volumes of data, including providing encryption keys. These requirements, however, prejudice the security of their digital offerings and hamper the ability of companies to monitor data security risks at a global level. In the worst-case scenario, if the majority of governments adopted data access measures unilaterally, it would severely fragment the global data infrastructure and create several inefficiencies in the global cloud computing markets.

B. Consistency of Data Access Measures with International Trade Law

As data access measures restrict digital trade flows, they may breach obligations contained in international trade agreements. First, the GATS and several other PTAs contain requirements for national treatment. Any measure affecting trade in services violates the national treatment obligation in GATS, Article XVII if it accords foreign services and service suppliers 'treatment no less favourable than it accords to its own like services and service suppliers'.[82] Being a specific obligation, it applies only in sectors where WTO members have offered commitments in their GATS Schedule of Commitments.[83] Certain PTAs also contain an explicit national treatment obligation for digital products. For instance, the USMCA states that no party can accord 'less favourable treatment' to like digital products 'created, produced, published, contracted for, commissioned, or first made available on commercial terms in the territory of another Party, or to a digital product of which the author, performer, producer, developer, or owner is a person of a Party'.[84]

Assuming a country has offered national treatment commitments in sectors affected by the data access measure in their GATS Schedule,[85] the national treatment obligation requires the examination of: (i) the likeness of domestic and foreign services or service suppliers (in the case of the USMCA, it would entail examination of where there are like digital products); and (ii) whether foreign services or service suppliers (or like digital product) have received less favourable treatment compared to domestic services or service suppliers. For example, if a government has prescribed full national treatment commitments under Mode 1 for all payment and money transmission services, then a data localisation requirement for e-payment services could potentially implicate the national

[82] General Agreement on Trade in Services (Marrakesh, April 1994), Art XVII:1 (GATS).

[83] A measure violating market access obligations (GATS, Art XVI) may also fall under GATS, Art XVII. In *China – Certain Measures Affecting Electronic Payment Services*, Panel Report (adopted 31 August 2012) WT/DS413/10, paras 7.649–7.664, the WTO panel decided that if commitments are inscribed in both GATS, Art XVI and GATS, Art XVII, the inscriptions under GATS, Art XVI prevails. See also GATS, Art XX:2.

[84] USMCA, Art 19.4.1.

[85] This assessment is, however, necessary for PTAs where members have made a general obligation.

treatment obligation.[86] This is because the requirement disadvantages foreign e-payment service providers by making it extremely expensive to set up local data infrastructure or provides competitive benefits to the domestic technology players with a domestic data infrastructure.

The second obligation that could be relevant in the context of the data access measure is the provision on market access set out in GATS, Article XVI.[87] For instance, if a WTO member has made a full commitment in Mode 1 across various service sectors relying upon personal data processing, then a blanket restriction on transferring personal data abroad or a strict data localisation requirement for personal data could violate the market access obligation as this measure restricts the total number of service suppliers/service transactions within the country.[88]

The provisions on domestic regulation could also be relevant in evaluating the consistency of a data access measure with international trade law. These disciplines are contained in GATS, Article VI and are also commonly found in the trade in services chapter of PTAs. As an example, GATS, Article VI contains obligations to administer domestic regulations affecting trade in services in a 'reasonable', 'objective' and 'impartial' manner.[89] Disciplines under GATS, Article VI are especially significant when measures have a restrictive impact on trade but do not breach other legal obligations. For instance, if a domestic law requiring all foreign companies to provide direct access to personal data of domestic users or cryptographic keys for specific digital services is implemented in an arbitrary manner (such as targeting multinational companies or not following a transparent procedure for data requests), then such a measure can violate GATS, Article VI. This can include scenarios where a 'prompt review' of administrative or judicial decisions regarding data access requests is absent.[90] Such obligations are also contained in the Reference Paper on Services Domestic Regulation, which, as of July 2023, has been signed by 67 WTO members.[91]

Each of the above measures are subject to exceptions contained in GATS; this language has also been imported wholesale into the majority of PTAs. Data access measures could be justified under GATS, Article XIV if the measure is necessary to achieve the public policy objectives listed in that Article. The most

[86] In practice, this would depend on the wording of the commitment, but it is assumed here that it is a fully open commitment. Further, it could be debated if all e-payment platform services fall within the scope of this sector or could be considered under sectors such as computer and related services.

[87] GATS, Art XVI (2).

[88] Relying on *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, Appellate Body Report (adopted 20 April 2005) WT/DS285/26, paras 238, 251, 373 (US – Gambling).

[89] GATS, Art VI:1.

[90] Applying GATS, Art VI:2.

[91] See, eg WTO, 'Joint Initiative on Services Domestic Regulation – Reference Paper on Services Domestic Regulation' (26 November 2021) INF/SDR/2, Art 19.

relevant provisions would be the public order/public morals exception or if the measure is necessary to secure compliance with domestic laws. In assessing the policy objective behind a data access measure, a trade tribunal can look at various factors, including legislative proposals, domestic policies or statements made by governments imposing the measure,[92] as well as the actual content, structure and expected operation of the measure.[93] Thereafter, in light of this policy objective, the trade tribunal will engage in a comprehensive weighing and balancing test to assess the necessity of the measure. Finally, the trade tribunal will evaluate whether the measure is applied in practice in an even-handed and non-arbitrary manner and does not constitute a disguised restriction on trade.[94] Where a data access measure is overly restrictive in nature and where both its design and implementation do not clearly relate to the policy objective, there is a likelihood that a panel will find that the measure is inconsistent with the general exception.

The key challenges in applying the above test to data access measures are: (i) making a coherent assessment of the underlying policy objective of a particular data access measure, particularly where there is a huge gap between the proffered objective and real-world implementation; (ii) considering the legitimacy of data access measures in jurisdictions where there is a clear record of human rights violations or where the implementation is vague and non-transparent; and (iii) evaluating alternatives to data access measures, especially where the private sector is facing huge restrictions or a loss of consumer trust due to excessive or unreasonable data access measures being implemented within the country.

The above challenges arise due to the lack of a global consensus on the substantive standards (including on privacy) applicable to cross-border data access requests. Therefore, trade tribunals will be unable to benchmark domestic data access measures to relevant normative frameworks. Further, data access often entails (or is at least portrayed as entailing) a national security dimension. As chapter three discusses in the context of cybersecurity, the connection of trade and security issues makes the role of trade tribunals much more complicated, as governments may view an adverse decision against their data access measure as a breach of their sovereignty. Further, as section IIA indicates, governments often have strong reasons to enforce these measures, especially as MLATs have become insufficient and irrelevant in the digital world. Thus, trade tribunals may choose to take a deferential approach that can ultimately harm digital trade.

[92] See, eg US – Gambling (n 88) para 6.486; *European Communities – Measures Prohibiting the Importation and Marketing of Seal Products*, Panel Reports (adopted 18 June 2014) WT/DS400/16/Add.7 and WT/DS401/17/Add.7, paras 7.396–7.398, 7.404.

[93] *Colombia – Measures Relating to the Importation of Textiles, Apparel and Footwear*, Appellate Body Report (adopted 22 June 2016) WT/DS461/29, para 5.68.

[94] For an overview on the jurisprudence on GATS chapeau, see L Bartels, 'The Chapeau of the General Exceptions in the WTO GATT and GATS Agreements: A Reconstruction' (2015) 109(1) *American Journal of International Law* 95.

In addition to the above-discussed WTO provisions, PTAs also contain digital trade or electronic commerce rules specifically applicable to measures restricting cross-border data flows or requiring data localisation. For instance, as discussed in chapter two, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and other PTAs contain provisions prohibiting data localisation and requiring the cross-border transfer of information. These two provisions are subject to a legitimate public policy exception.[95] As several data access measures affect cross-border data flows either directly or indirectly, or even contain an explicit requirement for localising data in domestic servers, they can breach these obligations in PTAs. Although they may be justified under the legitimate public policy exception, several legal uncertainties remain. Two of the most challenging uncertainties are: (i) it may hard to assess whether there is a legitimate public policy objective, especially when the objective is unclear from the design of the measure; and (ii) the measure must satisfy the necessity and proportionality requirement embedded in the exception, entailing a complex weighing and balancing of various factors.

For instance, the cybersecurity law of a country may require data localisation of certain sensitive categories of data to enable stronger regulatory supervision or to ensure better law enforcement.[96] Such a measure could potentially violate the data localisation and cross-border data flow obligations contained in various PTAs (subject to non-conforming measures). In justifying this measure under the exceptions in the relevant PTA, the party will most likely need to adduce evidence that localisation is the least trade-restrictive route to achieving the underlying objectives of the measure, the policy objective in question is legitimate and the measure is implemented in an even-handed manner without any hidden protectionist intent. For instance, if the implementation of the measure indicates that the government routinely uses the data localisation requirement to target minority groups (instead of genuine cases of law enforcement), then it is unlikely to satisfy the threshold under the exception. However, such an assessment is politically sensitive and likely be viewed as interfering with the regulatory autonomy and sovereignty of a country.

Another relevant provision common in PTAs relates to restrictions on the use of encryption standards. For example, the CPTPP prohibits governments from imposing specific encryption standards or requiring access to encryption keys 'as a condition of the manufacture, sale, distribution, import or use of the product'.[97] The provision is significant in underlining the importance of strong encryption for instilling digital trust, necessary for conducting cross-border trade in digital services. However, this provision does not apply in the context

[95] See generally M Burri and R Polanco, 'Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset' (2020) 23(1) *Journal of International Economic Law* 187, 212–14.

[96] See ch 3.

[97] See, eg CPTPP, annex 8B, s A.3.

of law enforcement activities[98] or government networks.[99] Therefore, it has limited scope of application if the government can argue that a particular data access measure relates to law enforcement or specifically applies to government networks.

C. Relevant Provisions in PTAs on Cross-Border Data Access

Although the jurisdictional conflict over data access has become a significant problem for the global digital trade market, most treaties do not contain any specific provisions on data access. An exception is the provision in the Financial Services Chapter of the USMCA that states that

> all parties recognise that immediate, direct, complete, and ongoing access by a Party's financial regulatory authorities to information of covered persons, including information underlying the transactions and operations of such persons, is critical to financial regulation and supervision, and recognise the need to eliminate any potential limitations on that access.[100]

Therefore, while data localisation is prohibited in the financial services sector, all companies providing financial services are under an obligation to provide the regulatory authorities, for regulatory and supervisory purposes, with 'immediate, direct, complete, and ongoing access to information processed or stored' outside its territory.[101] In other words, where a party is unable to obtain immediate, direct, complete and ongoing access to data necessary to conduct regulatory supervision, then the party can impose data localisation measures.[102] This provision also states that a party can adopt or maintain any data protection, privacy or other confidentiality measures as long as such measures are not aimed at circumventing the commitments or obligations in this section.[103] I come back to the broader relevance of this provision in section IVB.

IV. ALIGNING INTERNATIONAL TRADE LAW AND DATA ACCESS MEASURES

This chapter has so far argued that data access measures can disrupt cross-border data flows and create different kinds of legal and business uncertainties for companies engaging in cross-border digital trade. Yet, data access measures

[98] ibid annex 8B, s A.3.
[99] ibid annex 8B, s A.5.
[100] USMCA, Art 17.18.1.
[101] ibid Art 17.18.2.
[102] ibid Art 17.18.3, fn 10.
[103] ibid Art 17.18.4.

are often necessary for governments to conduct basic regulatory and investigative functions. Therefore, a consistent and coherent framework for data access is needed at a transnational or global level to address this policy dilemma. This section first evaluates various normative developments in the international community covering both binding treaties and soft law mechanisms that address and facilitate cross-border data access and then outlines if international trade law can play a supportive or complementary role to support them. Although the role of international trade law seems limited at first sight, this section sets out why it can be critical, especially in the context of generating more digital trust and facilitating a balanced approach towards the regulation of data access measures. In particular, it finds that the growing network of PTAs and DEAs can play an instrumental role.

A. International and Transnational Responses to Governmental Access to Data

(i) International Treaties

Perhaps the most important example of an international treaty dealing with issues of governmental access to data is the Convention on Cybercrime, or the Budapest Convention.[104] This treaty was opened for signature in 2001 and deals with cybercrime and electronic evidence.[105] Sixty-eight countries have ratified the Convention, while two others (Ireland and South Africa) have signed the Convention but not ratified it.[106] The core objectives of this treaty are to provide a framework for harmonising law on cybercrime across countries and to set out the procedures for investigating and prosecuting cybercrimes, including a mechanism for international cooperation. It contains specific procedural mechanisms for governmental access to various kinds of data, such as traffic, subscriber and content data, including the safeguards for protecting basic human rights. Article 32 of the Budapest Convention provides for a limited mechanism for extraterritorial access to data, wherein a government can access such data in another country for investigating cybercrimes if the data is publicly available or if the person who can disclose such data provides lawful and voluntary consent to share the data.[107]

[104] Convention on Cybercrime (Budapest, 23 November 2001) ETS No 185 (Budapest Convention).

[105] Note, however, there is an ongoing discussion at the UN on a new treaty for cybercrime, discussed briefly below.

[106] As of April 2023. Council of Europe, 'Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY', www.coe.int/en/web/cybercrime/parties-observers.

[107] Budapest Convention, Art 32. There is currently some debate if this provision can apply to ISPs or only applies to individuals to whom the relevant data pertains. Several countries, including India, Brazil and China, also found this particular provision to be contrary to the principle of sovereignty.

The Second Additional Protocol to the Budapest Convention was adopted in 2021[108] and provides new mechanisms for cooperation between states and the private sector to facilitate the cross-border access to data necessary for investigating cybercrimes. For instance, it enables states to make direct requests to service providers for subscriber information, even when the provider is located outside of the state.[109] Therefore, it provides an alternative to the MLAT mechanism discussed earlier. Further, the Protocol creates a procedure for expediting MLAT requests by requiring that any information related to subscriber and traffic data must be treated in the same manner as requests by domestic authorities.[110] In the case of an emergency entailing 'a significant and imminent risk' to the safety or life of peoples, the Protocol allows a state party to request for data access to another state party through a 24/7 point of contact, which must then be acted upon as soon as possible.[111]

The Budapest Convention is often touted to be the most viable international legal solution to address concerns pertaining to governmental access to data. But there are also several criticisms. For instance, the Protocol does not incorporate any standards for proportionality or necessity to respond to data requests or safeguards to protect human rights; civil society bodies, including an internal committee of the Council of Europe, had pointed out these gaps in the Protocol to no avail.[112] Further, even though certain countries (such as in Europe) have signed the Protocol, several other countries (such as India, Brazil and China) have so far refused to participate.[113] Even if the Second Additional Protocol is widely adopted, it will not apply to content data, which is increasingly crucial for law enforcement purposes. While the Protocol does cover subscriber data, there are concerns that this data may be exploited by certain governments to target political dissidents and journalists.[114]

Since 2022, under the auspices of the UN, countries have also been negotiating a new treaty on cybercrime (scheduled to conclude in 2024).[115] Civil society advocates have raised various concerns regarding this treaty, pointing out that several provisions provide governments with highly permissive powers to deal

[108] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (ETS No 224, Strasbourg, 12 May 2022).

[109] ibid Art 7.

[110] ibid Art 8.

[111] ibid Art 9; see also Art 10 on emergency mutual assistance.

[112] T Israel and K Rodriguez, 'On New Cross-Border Cybercrime Policing Protocol, a Call for Caution' (Just Security, 13 May 2022) www.justsecurity.org/81502/on-new-cross-border-cybercrime-policing-protocol-a-call-for-caution/.

[113] A Seger, 'India and the Budapest Convention: Why Not?' (ORF, 20 October 2016) www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/; A Peters, 'Russia and China Are Trying to Set the UN's Rules on Cybercrime' (Foreign Policy, 17 October 2016) www.foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/.

[114] Israel and Rodriguez (n 112).

[115] See generally United Nations Office on Drugs and Crime, 'Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes', www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

with cybercrimes.[116] In particular, experts have pointed out the adverse impact on the freedom of expression, privacy rights and due process, especially given the broad nature of government surveillance powers prescribed in the draft text and the lack of adequate safeguards to protect individuals.[117] These safeguards are also absent in the draft provisions relating to sharing of personal data between law enforcement bodies across countries.

Several provisions of this draft treaty are also inconsistent with the recommendations of the UN Special Rapporteur on the Right to Privacy for cross-border governmental data access.[118] The Rapporteur had also recommended setting up an International Data Access Authority to protect 'personal data, privacy, freedom of expression and other fundamental human rights while facilitating the timely exchange of personal data across borders as may be required for the legitimate purposes of law enforcement agencies, intelligence and security services'.[119] No such mechanism such as setting up an independent authority is contained in the draft UN treaty on cybercrime.[120]

Another treaty containing provisions relevant to governmental access to data is the Arab Convention on Combating Information Technology Offences, which has been signed by 18 states. This treaty sets out a detailed mutual assistance mechanism (to operate in the absence of MLATs), wherein parties can submit written requests to each other.[121] However, there is no mechanism for state parties to directly submit requests to private service providers in another member state. The treaty provides negligible safeguards related to protecting the privacy of individuals in dealing with such mutual assistance requests.

(ii) Transnational and Non-binding Initiatives

In 2021, 38 members of the OECD adopted a resolution setting out the key principles for government access to personal data held by the private sector for

[116] P Collings and K Rodriguez, 'Decoding the UN Cybercrime Treaty' (EFF, 7 April 2023) www.eff.org/deeplinks/2023/04/decoding-uncybercrime-treaty.

[117] See generally D Brown, 'Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights' (HRW, 13 August 2021) www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights; C Ohanian, 'The UN Cybercrime Treaty Has a Cybersecurity Problem In It' (Just Security, 17 October 2022) www.justsecurity.org/83582/the-un-cybercrime-treaty-has-a-cybersecurity-problem-in-it/; K Bannelier, 'The UN Cybercrime Convention Should Not Become a Tool for Political Control or the Watering Down of Human Rights' (*Lawfare Blog*, 31 January 2023) www.lawfareblog.com/un-cybercrime-convention-should-not-become-tool-political-control-or-watering-down-human-rights.

[118] Mapping Project, 'Draft Legal Instrument on Government-led Surveillance and Privacy – Including the Explanatory Memorandum', Ver 0.6 (OHCHR, 10 January 2018) (Draft Legal Instrument).

[119] Draft Legal Instrument, Art 15.

[120] This idea has also been supported by other experts such as setting an independent clearing house at the global level, which could decide on the legitimacy of government data access requests. See AK Woods, 'Data Beyond Borders – Mutual Legal Assistance in the Internet Age' (Global Network Initiative, January 2015) 16.

[121] Arab Convention on Combating Information Technology Offences (Cairo, 21 December 2010), Art 32, 34.

national security and public safety purposes.[122] This resolution was developed in order to strengthen the Data Free Flow with Trust (DFFT) framework, which was previously proposed by Japan and adopted by the G20 in 2019.[123] As a part of the DFFT framework, Japan had proposed for a review of the OECD Privacy Guidelines; this included the proposal to develop specific principles for governments to access any personal data held by the private sector especially on grounds of law enforcement and national security.[124] In 2020, the OECD Committee on Digital Economy Policy[125] started developing a detailed study of this topic, leading to the adoption of the resolution in October 2021.[126] The resolution recognises that any country implementing certain key principles (as discussed below) makes 'a positive contribution towards facilitating transborder data flows'.[127]

The OECD resolution sets out seven key principles applicable to government access to personal data held by private companies: (i) all requests for data access must have a legal basis and be implemented by government bodies operating under the rule of law; (ii) government access to data is based on specified and legitimate aims consistent with the legal standards of necessity, proportionality and reasonableness, and other relevant standards set out in domestic laws; (iii) there must be appropriate mechanisms for obtaining prior approvals for data access, taking into account the sensitivity of different categories of data; (iv) governments must put in place appropriate measures for data handling that protect the confidentiality, security and integrity of data and maintain privacy; (v) governments must develop a transparent legal framework for accessing data, including independent reporting of such requests; (vi) there must be effective and impartial oversight over data access requests; and (vii) domestic laws must provide effective remedies to remedy violations.

The OECD resolution was received enthusiastically by both governments and the private sector,[128] although certain factions of civil society were dissatisfied

[122] OECD, 'Declaration on Government Access to Personal Data Held by Private Sector Entities' (12 December 2022) OECD/LEGAL/0487.

[123] See ch 1.

[124] S Wood, 'The OECD Breaks New Ground with Historic Declaration on Government Access to Private Sector Data' (JD Supra, 20 January 2023) www.jdsupra.com/legalnews/the-oecd-breaks-new-ground-with-5687493/.

[125] The objective of the Committee is to develop evidence-based policies through multistakeholder processes to ensure an 'innovative, open, inclusive, and trusted digital economy' and 'provide policy-makers with the tools … to leverage the potential of digitalisation for growth and well-being across all policy areas'. See OECD, 'Resolution of the Council renewing and revising the Mandate of the Committee on Digital Economy Policy' (11 December 2018) OECD C/M(2018)24, item 252 (OECD Resolution on Digital Economy).

[126] OECD, 'Statement of the Committee on Digital Economy Policy' (22 December 2020) DSTI/CDEP(2020)22/FINAL.

[127] OECD Resolution on Digital Economy (n 125) recital 2.

[128] International Chamber of Commerce, 'Global Business Welcomes Adoption of OECD Principles on Government Access to Personal Data' (14 December 2022) www.iccwbo.org/news-publications/statement-letters/global-business-welcomes-adoption-of-oecd-principles-on-government-access-to-personal-data/; Wood, 'The OECD Breaks New Ground' (n 124).

with the lack of multistakeholder discussions in devising these principles.[129] Some experts argued that the declaration judiciously adapts to variations in data protection frameworks across countries.[130] For instance, the requirements for oversight required effectiveness and impartiality (rather than independence, which is typically the term used in Western liberal democracies), and a range of bodies in addition to courts were acknowledged to be capable of providing such oversight.[131] Further, the OECD resolution distilled key concepts and principles from existing domestic frameworks across the world rather than imposing new ones, thus making it easier for non-OECD countries to also incorporate the principles in practice.[132] Adherence to these principles could be considered in deciding upon adequacy of the data protection framework of a country, or factored into domestic laws on law enforcement.[133]

In 2021, the GPA adopted a resolution on governmental access to data, privacy and the rule of law.[134] This resolution sets out the core data protection principles applicable to all governmental requests for data access. In particular, the principles focus on sensitive personal data, as well as recognising the need to respect the rule of law and protect democratic values and human rights. The core principles set out under this resolution are very similar to the OECD resolution discussed above. Additionally, the resolution highlights the need to ensure the robustness of cryptographic systems,[135] the need for transparent reporting of government data access requests[136] and the need for international regulatory cooperation in this area.[137]

(iii) Multistakeholder and Private Sector Initiatives

An example of norm entrepreneurship by the private sector is the 2018 proposal by Microsoft, wherein the company proposed that governments must come to an international agreement for governmental access to data and specified relevant principles: providing notice to users when government accesses their data; developing an oversight mechanism for content and sensitive user data; providing detailed grounds for data access requests; resolving jurisdictional conflicts

[129] OECD Civil Society Information Society Advisory Council, 'Statement Regarding Trusted Government Access to Private Sector Data Ministerial Declaration' (14 December 2022).
[130] ibid.
[131] Wood, 'The OECD Breaks New Ground' (n 124).
[132] ibid.
[133] ibid.
[134] Global Privacy Assembly, Adopted Resolution on Government Access to Data, Privacy and the Rule of Law: Principles for Governmental Access to Personal Data held by the Private Sector for National Security and Public Safety Purposes (43rd Closed Session of the Global Privacy Assembly, October 2021).
[135] ibid 4.
[136] ibid 4.
[137] ibid 5.

on data access; providing direct access for enterprise data; and being transparent regarding how and when governments seek access to data through international negotiations.[138] Similar proposals have also been made by certain think tanks.[139] The Internet Jurisdiction and Policy Network (IJPN), a multistakeholder body focusing on legal interoperability in cyberspace, has also conducted extensive assessment of the core principles necessary to enable cross-border data access.[140]

B. Data Access and International Trade Law: An Aligned Approach

Several of the above-discussed initiatives on cross-border data access are tailored towards addressing common problems in a digitally integrated world.[141] Experts have noted that the conflict between existing mechanisms for cross-border data access can have negative repercussions for both the protection of human rights and global digital trade flows.[142] Therefore, a more coherent framework is necessary to develop a global consensus on the fundamental norms for cross-border governmental access to data.[143] This section argues that such a framework must be multistakeholder and multilayered so as to align a wide range of issues. such as human rights protection, data security and digital trade.[144]

As previous chapters have discussed, several issues at the interface between digital trade regulation and global data governance need multistakeholder and multilayered policy intervention. The same holds true for governmental access to data. A global framework for data access must involve the right stakeholders, ensure transparency and create trust among heterogeneous actors.[145] Such a framework is unlikely if it takes the form of a global treaty. For instance, a treaty that is developed to achieve this objective is quite likely to contain deliberately vaguely worded provisions to accommodate varied regulatory concerns of members or adapt to the dynamic nature of digital technologies.

[138] 'Six Principles for International Agreements Governing Law-Enforcement Access to Data' (Microsoft, 2018) www.blogs.microsoft.com/wp-content/uploads/prod/sites/5/2018/09/SIX-PRINCIPLES-for-Law-enforcement-access-to-data.pdf.

[139] D Castro, 'Government Snooping and E-Surveillance Call for a Geneva Convention for Data' (ITIF, 18 December 2013) www.ITIF.org/publications/2013/12/18/government-snooping-and-e-surveillance-call-geneva-convention-data/.

[140] See generally Internet & Jurisdiction Policy Network, 'Toolkit: Cross-Border Access to Electronic Evidence', www.internetjurisdiction.net/data/toolkit.

[141] In addition to the above discussed examples, other initiatives for facilitating cross-border data access requests have been undertaken by the G7 24/7 Cybercrime Network and the SIRIUS Project in the EU, which is a common platform for sharing information and guidelines for data access requests based on MLATs and voluntary cooperation between EU members.

[142] UNSC CTED (n 10) 23.

[143] ibid 4.

[144] See, eg ibid.

[145] La Chapelle and Fehlinger (n 25) 21.

The examples of the Budapest Convention and the draft UN Cybercrime Treaty discussed above demonstrate several of these gaps.

Instead, a more viable approach could be a transnational one setting out high-level norms and standards that can fill in gaps in the existing mechanisms for both governments and the private sector and provide a more robust mechanism for cooperation between states.[146] For instance, these norms and standards could inform domestic laws as well as terms of use of various digital services and apps. The initiatives by the OECD, the GPA and the IJPN are more effective in this regard, but they are not necessarily focused on the trade dimension. Thus, an important question is the specific role that international trade agreements can play in this policy area. The rest of this section identifies the various ways in which trade agreements can play a meaningful role in supporting this transnational framework.

First, both at the WTO (under the ongoing plurilateral negotiations on electronic commerce) and in PTAs, countries can adopt a provision clarifying the importance of ensuring access to data of regulators for legitimate grounds such as for the purposes of regulatory supervision. As discussed in section IIIC, the USMCA incorporated such a provision in the context of financial services, thereby preventing governments from imposing data localisation in the financial sector as long as companies were willing to provide immediate access to relevant data to financial regulators. This qualification should also be added to electronic commerce chapters, wherein any prohibition on data localisation will not apply if the service providers do not provide regulators with access to relevant data necessary for regulatory supervision, provided that the government follows requirements of legitimacy and due process in making such requests. Nonetheless, this provision cannot remedy a conflict of laws situation, wherein the request for data access in one country conflicts with a blocking statute in another country.

Second, to create more consensus and coherence among trading partners regarding the fundamental requirements for cross-border data access, trade agreements must incorporate by reference the core principles set out in an OECD declaration and by the GPA. In a submission before the WTO Joint Initiative on Electronic Commerce, Canada had proposed specific provisions that would provide a minimum guarantee for basic privacy/human rights safeguards when governments access personal data.[147] However, to date, this proposal does not appear to have gained much traction in the negotiations. This proposal may, though, be a lot more relevant in the context of PTAs and DEAs, wherein parties could agree to voluntarily sign up to these instruments. In both scenarios, negotiating parties must conduct a joint regulatory mapping exercise for laws on

[146] ibid 23.

[147] WTO, 'Joint Statement on Electronic Commerce- Submission by Canada' (19 October 2020) WTO Doc INF/ECOM/58.

data access to ascertain whether there are any existing tensions or conflicts that might need to be resolved. In the long term, these arrangements could gradually lead to a more coherent model globally. Another possible alternative could be for countries to sign the Budapest Convention and Second Protocol. However, given the various deficiencies in this treaty, this option appears less attractive in creating a global framework for data access measures.

Finally, to the extent that trade disputes arise in relation to data access measures, tribunals must be equipped to consider the relevant norms on data access to facilitate judicious resolution of these disputes.[148] By incorporating a qualifier to the data localisation prohibition and incorporating by reference the relevant normative frameworks on data access within international trade agreements, trade bodies will be better equipped to address a challenge to a data access measure under international trade law. For instance, the trade tribunal could benchmark the measure against prevailing international best practices to evaluate if the measure is proportionate and necessary to a policy objective instead of conducting a half-baked deferential analysis. This approach is also more sensitive to genuine regulatory requirements and acknowledges the need for governments to strike a balance between conflicting interests.

However, to the extent that data access measures relate to core sovereignty-related concerns, trade disputes are likely to be futile. As I discussed regarding cybersecurity measures in chapter three, the alternative option of finding political solutions within trade committees might be better in such scenarios.

V. CONCLUSION

Data access measures pose a critical challenge to both digital trade and global data governance. This chapter examined how data access measures affect cross-border data flows and whether they can violate international trade law. It argued that governments impose data access measures for varied reasons, including obtaining digital evidence for law enforcement, the investigation of crimes and to conduct regulatory supervisions and audits. Data access measures may also relate to other interests, such as strengthening intelligence capabilities and enabling data sharing in the domestic economy. Several data access measures directly or indirectly affect cross-border data flows, including data localisation. Further, certain measures providing regulators with direct access to data stored abroad and/or encryption keys used by technology companies undermine digital trust and can reduce global data security. These measures can also conflict with laws in other jurisdictions, such as blocking statutes, and thereby create a high degree of uncertainty for businesses conducting cross-border digital trade.

[148] For discussions on incorporating multistakeholder norms and best practices by reference in international trade treaties, see chs 2, 3 and 7.

This chapter has argued that data access measures are likely to violate obligations contained in both WTO treaties and PTAs. While such measures may be justified under the available exceptions, this legal assessment entails several complications, especially in the absence of a coherent global framework for cross-border data access. Certain treaties, particularly the Budapest Convention and the Second Additional Protocol, provide a mechanism for governments to request access to data for law enforcement. However, these treaties are neither universally accepted nor sufficiently robust to prevent misuse by governments. Further, the UN Cybercrime Treaty (if successfully negotiated) is likely to be effective in developing a robust framework for cross-border data access. Instead, the chapter has found that multistakeholder and transnational initiatives from the GPA, the OECD and other bodies such as the IJPN are likely to be more meaningful in developing core principles and best practices for cross-border data access.

In order to bring more alignment between international trade law and these evolving normative initiatives, this chapter has made a few proposals. First, all trade treaties containing an explicit prohibition on data localisation must incorporate a qualifier that all companies (irrespective of the location of the data) must respond to legitimate and due process-compliant governmental requests for data, for instance for regulatory supervision. Second, trade treaties must incorporate by reference relevant norms and principles for data access developed in bodies such as the GPA and the OECD. This is especially important as a robust international treaty on data access seems highly unlikely in the current political scenario. Therefore, for countries actively engaged in digital trade, these normative benchmarks can ensure more trust and certainty in the digital trade framework. Finally, the incorporation of these provisions could provide a clearer legal basis for trade tribunals to adjudicate trade disputes arising in relation to data access measures.

5

Bridging the Global Data Divide Through International Trade Law

I. INTRODUCTION

The global data divide remains one of the most difficult and intractable policy challenges today.[1] This divide can be viewed from various perspectives, including from a broader perspective of the digital divide. For instance, several parts of the developing world do not have adequate infrastructure or resources to access the Internet, including access to electricity and mobile broadband.[2] Further, even where Internet access is available, certain groups such as rural communities, women, indigenous peoples and older people do not have sufficient digital education to benefit from participating in the digital economy.[3] This exclusion often extends to individual entrepreneurs or micro, small and medium enterprises (MSMEs) in developing countries, as they lack the digital education and resources necessary to benefit from digitalisation.[4] Finally, at a global scale, the digital/data divide may translate into a development divide, wherein developing countries are forced to import foreign digital technologies from developed countries (and arguably their models of data regulation)[5] without gaining meaningfully

[1] See generally World Bank, *World Development Report – Digital Dividends* (2016); K Schwab, *The Global Competitiveness Report* (WEF, 2018) 5–7.

[2] C Rodriguez, 'Why a Third of the World, Nearly Three Billion People, Have Never Used the Internet' (Forbes, 2 December 2021) www.forbes.com/sites/ceciliarodriguez/2021/12/02/why-a-third-of-the-world-nearly-three-billion-people-have-never-used-the-internet/; International Telecommunication Union (ITU), 'Connectivity in the Least Developed Countries – Status Report' (2021); ITU, 'Measuring Digital Development – Facts and Figures' (2021) 2.

[3] See generally OECD, 'Bridging the Digital Gender Divide – Include, Upskill, Innovate' (2018); F Mubarak and R Suomi, 'Elderly Forgotten? Digital Exclusion in the Information Age and the Rising Grey Digital Divide' (2022) 59(Dec–Jan) *Inquiry: The Journal of Health Care Organization, Provision, and Financing*; ITU, 'Final Report – World Telecommunication Development Conference' (Buenos Aires, 2017) Res 46 – Assistance to Indigenous Peoples and Communities Through Information and Communication Technology 419.

[4] See generally ILO, *Small Goes Digital – How Digitalization Can Bring About Productive Growth for Micro and Small Enterprises* (2021).

[5] SA Aaronson and P Leblond, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO' (2018) 21(2) *Journal of International Economic Law* 245, 269; S Weber, 'Data, Development, and Growth' (2017) 19(3) *Business and Politics* 397, 406.

from the economic flows.[6] Thus, the global data divide is multidimensional and can relate to a range of policy challenges in different regulatory areas.

This chapter focuses specifically on the data divide between the developed and developing world and how international trade law can respond to it. Several statistics indicate the magnitude of this divide. For instance, a study by Nikkei Asia found that while 23 per cent and 12 per cent of the global data flows were attributable to China and the USA respectively, developing countries in Africa and Latin America were negligible contributors to global data flows.[7] This vast gap can be explained by the lack of both data infrastructure and technical and regulatory expertise in several developing countries, especially least developed countries (LDCs). This chapter specifically focuses on how the global data divide is impacted by the variations in data regulatory frameworks across countries at different stages of development and if international trade law can provide an adequate response to address these challenges. Certain other aspects, such as access to broadband,[8] digital education[9] or the ability of developing countries to respond to labour market disruptions caused by rapid digital transformation,[10] are not specifically covered in this chapter.

As argued in chapter one, a robust global regulatory framework for cross-border data flows can support digital connectivity, which, in turn, supports digital trade. The previous three chapters have highlighted how data-restrictive measures that restrict cross-border data flows harm digital trade and can also breach international trade law. Despite the economic harms of data-restrictive measures, developing countries now increasingly adopt data-restrictive measures (often designed as instruments of industrial policy) to address the various developmental constraints that they face due to the dearth of sufficient data infrastructure and the limited amount of domestic technical expertise and regulatory capacity. While the ultimate aim behind such measures is boosting domestic digital sectors and reducing dependence on foreign data monopolies and digital technologies, the impact of such data-restrictive measures on

[6] United Nations, 'With Almost Half of World's Population Still Offline, Digital Divide Risks Becoming "New Face of Inequality", Deputy Secretary-General Warns General Assembly' (27 April 2021) DSG/SM/1579.

[7] M Uematsu and T Tsunashima, 'Divided Internet – China and US Switch Places as Data Powerhouse' (Nikkei Asia) https://vdata.nikkei.com/en/newsgraphics/splinternet/#:~:text=Escalating%20data%20friction%20between%20China%20and%20the%20U.S.&text=China%20too%20has%20shut%20the,of%20the%20global%20data%20economy; T Tsunashima, 'China Rises as World's Data Superpower as Internet Fractures' (Nikkei Asia, 25 November 2020) www.asia.nikkei.com/Spotlight/Century-of-Data/China-rises-as-world-s-data-superpower-as-internet-fractures.

[8] See, eg S Peng, 'The Uneasy Interplay Between Digital Inequality and International Economic Law' (2022) 33(1) *European Journal of International Law* 205, 215–17; see also WTO, 'Role of Digital Public Infrastructure in Promoting E-Commerce – Communication from India' (9 February 2023) WTO Doc WT/GC/W/853.

[9] See IEEE CTU, 'Digital Divide in Developing Countries: Why We Need to Close the Gap', www.ctu.ieee.org/digital-divide-in-developing-countries-why-we-need-to-close-the-gap/.

[10] See C Alonso et al, 'How Artificial Intelligence Could Widen the Gap Between Rich and Poor Nations' (IMF, 2 December 2020) www.imf.org/en/Blogs/Articles/2020/12/02/blog-how-artificial-intelligence-could-widen-the-gap-between-rich-and-poor-nations.

domestic economic growth is often shaped by a complex interplay of economic and political factors. While several experts have viewed the data divide as a new form of colonialism by digitally advanced countries, section II provides a more nuanced exploration of the global data divide, uncovering various factors creating it and the multiple dimensions of data/digital policy-making to which it can relate.

Section III then examines how the existing rules in international trade agreements relate to or address the global data divide. The section examines the extent to which international trade agreements enable robust data regulation and facilitate meaningful access and use of data by people in individual countries. It argues that international trade agreements currently contain negligible disciplines to bridge the data divide in a meaningful and effective manner. Further, international trade law does not provide any clear exceptions that allow developing countries to adopt data-restrictive measures for development-related policy objectives. Also, although certain recent preferential trade agreements (PTAs) with developing country parties incorporate rules on data flows, the developmental dimension remains largely unaddressed.

Section IV examines the existing deficiencies in international trade law, focusing on the missing links between digital trade disciplines and the developmental needs of developing countries. For instance, existing trade treaties do not contain tailored provisions for special and differential treatment (SDT) in the context of digital trade. Further, technology transfer is usually a non-negotiable issue for developed countries, even while developing countries are expected to undertake extensive reforms to provide market access in digital sectors and liberalise cross-border data flows. Further, certain PTAs impose requirements for countries to rapidly adopt domestic data regulatory frameworks without adequate and meaningful technical assistance or capacity-building support. Consequently, developing countries may be forced to adopt specific regulatory frameworks to align with the political and economic interests of certain digitally advanced countries. This power asymmetry has worsened in light of the economic uncertainties brought forth due to the ongoing technology war between the USA and China.[11]

To address these gaps, this chapter proposes several reforms within international trade law. It suggests that the obligations imposed on developing countries to implement robust domestic regulatory frameworks to enable data flows must be conditional on receiving adequate technical assistance and capacity-building support from developed countries in areas that are identified by developing

[11] See generally D Lehr, 'How the US–China Tech Wars Will Impact the Developing World' (*The Diplomat*, 23 February 2019) www.thediplomat.com/2019/02/how-the-us-china-tech-wars-will-impact-the-developing-world/; BVD Merwe, 'US–China Tech War: Which Countries Will Suffer the Most?' (*Investment Monitor*, 17 February 2021) www.investmentmonitor.ai/features/us-china-tech-war-which-countries-will-suffer-the-most/; E White and M Ruehls, 'US–China Decoupling is Hurting Innovation, World Bank Warns' (*Financial Times*, 31 March 2023) https://www.ft.com/content/93015aab-4b3d-43c7-be9b-ad4af4fc721d.

countries themselves. This support should not result in forced harmonisation of data regulations but, rather, should help developing countries build their digital regulatory frameworks contextualised to their domestic needs and circumstances. The Trade Facilitation Agreement provides a helpful prototype to build such a model. Further, this chapter highlights the need for meaningful technology transfer in the digital realm, and recommends creating suitable flexibilities and exceptions in digital trade rules, particularly for LDCs, to develop their domestic data regulatory frameworks.

The chapter also argues the need for trade bodies to experiment with new models of multilayered digital cooperation to develop inclusive and balanced norms on cross-border data flows, especially in areas that contribute to bridging the data divide such as data sharing and data access. It indicates the possibility of using digital trade agreements and regional cooperation as a basis for incorporating relevant multistakeholder principles focused on data equity, inclusion and sharing.[12] The above reforms must not be viewed as moral obligations for developed countries; instead, they represent commonly shared interests for the sustainable growth of the digital economy.[13]

II. THE INTERFACE OF CROSS-BORDER DATA FLOWS AND THE GLOBAL DATA DIVIDE

This section investigates the different dimensions of the global data divide and links it to the regulation of cross-border data flows. The global data divide is often viewed in terms of exploitation of developing countries by Big Tech companies based in richer countries due to the one-way flow of data from poor to rich countries.[14] This section argues that this perspective does not present a complete understanding of the global data divide. For instance, there could be other constraints faced by developing countries, including wide variations in their ability to implement data regulations and foster the domestic data economy through business-friendly policies due to a dearth of domestic talent and resources. Thus, this section takes a nuanced approach to unpacking the various dimensions of the global data divide and its impact on cross-border data flows.

[12] Relatedly, ch 6 discusses the importance of competition disciplines in fostering equitable data markets.

[13] Some scholars also link aspects of the data and digital divide to discussions of sustainable development. While this chapter does not delve into this topic, several aspects of SDT treatment, ensuring equitable data access, etc covered in this chapter are interrelated with Sustainable Development Goals. See M Burri and K Kugler, 'Digitization, Regulatory Barriers and Sustainable Development' (2023) Trade Law 4.0 Working Paper No 03/2023.

[14] J Hicks, '"Digital Colonialism": Why Some Countries Want to Take Control of Their People's Data from Big Tech' (*The Conversation*, 26 September 2019) www.theconversation.com/digital-colonialism-why-some-countries-want-to-take-control-of-their-peoples-data-from-big-tech-123048.

To date, no specific definition exists of the global data divide. In this chapter, global data divide is viewed from the perspective of the wide gap in the capacity of individuals and businesses in developing and developed countries to participate in and benefit from the datafied economy. Agarwal and Mishra have characterised this divide in three components: the access component, referring to the ability to access data and data-driven services; the regulatory component, focusing on the laws and regulations that protect key interests of digital users; and the use component, which focuses on the ability of individuals to use data and data-driven technologies to achieve economic growth.[15] The manifestations of the global data divide are thus visible in different aspects of the digital economy.

A widely used narrative in explaining the cause of the global data divide is that of data colonialism,[16] which, in turn, has led several developing countries to assert their right to data sovereignty,[17] including through data-restrictive measures. The key concern is that Big Tech companies based in rich countries are siphoning off raw digital data from poorer countries, leaving them in a data poverty gap, and generating enormous profits at their cost.[18] Therefore, they are depriving poorer countries from achieving meaningful development and trapping them in a vicious cycle of digital dependency, data manipulation and exploitation.[19] This narrative has informed legal and policy frameworks on data localisation and other data-restrictive measures in several countries, including India,[20]

[15] N Mishra and B Agrawal, 'Addressing the Global Data Divide through Digital Trade Law' (2022) 14(2) *Trade, Law & Development* 238, 243–46.

[16] N Couldry and UA Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford, Stanford University Press, 2019) 19, stating: 'More explicitly defined, data colonialism is our term for the extension of a global process of extraction that started under colonialism and continued through industrial capitalism, culminating in today's new form: instead of natural resources and labor, what is now being appropriated is human life through its conversion into data.'

[17] See, eg V Hofmann, 'Towards an African Narrative on Digital Sovereignty' (HIIG, 17 March 2022) www.hiig.de/en/african-digital-sovereignty/; A Basu, 'Sovereignty in a 'Datafied' World' (ORF, 18 October 2021) www.staging.orfonline.org/research/sovereignty-in-a-datafied-world/; E Matambo and ET Ugar, 'South Africa's Data Sovereignty Regulations: Merits and Possible Limitations' (2022) University of Johannesburg Centre for Africa–China Studies Policy Brief No 2, 5.

[18] M Maciel, 'The Renaissance of Industrial Policy and its Articulation with Data Governance' (IISD, 15 January 2023) www.iisd.org/articles/policy-analysis/industrial-policy-data-governance.

[19] See generally Couldry and Mejias (n 16).

[20] See, eg Department for Promotion of Industry and Internal Trade, Draft National E-Commerce Policy: India's Data for India's Development (26 February 2019); Reserve Bank of India (RBI), 'Storage of Payment System Data' (6 April 2018) DPSS.CO.OD No 2785/06.08.005/2017-18; Department of Science and Technology, National Data Sharing and Accessibility Policy (India) (9 February 2014); Department for Promotion of Industry and Internal Trade, Consolidated FDI Policy (2017) PP F No 5(1)/2017-FC-1 (India); Ministry of Corporate Affairs, Companies (Accounts) Rules, 2014 (India), rule 3(5); IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017 (India), rule 18. For further discussion of various data localisation requirements in India and its policy implications, see N Mishra, 'Data Governance and Digital Trade in India: Losing Sight of the Forest for the Trees?' (2021) ANU College of Law Research Paper No 21.16.

Rwanda,[21] South Africa[22] and Pakistan.[23] While the data colonialism narrative is politically appealing, it does not necessarily respond to all aspects of the data divide, as argued further below.

From the perspective of digital trade, the main fallout of data colonialism is the inability of developing countries to participate meaningfully in and benefit from the global data-driven economy. In other words, developing countries may be seen as getting a 'raw deal' because the majority of them do not have the infrastructure, resources and policy frameworks to capitalise on and generate value from the data generated within their borders. Thus, several developing countries and other organisations have argued for the urgent need to create fair and equitable competitive opportunities for businesses in developing countries to develop data-driven technologies/services and to reduce their long-term reliance on foreign digital imports.[24]

In order to make sense of this asymmetry in competitive opportunities, we must unpack the various factors driving the global data divide. For instance, several developing countries and most LDCs lack the regulatory capacity and resources to regulate data and data-driven sectors,[25] especially when compared with developed countries.[26] In particular, they may face cost-related challenges in enforcing a data protection framework in addition to the regulatory capacity deficit.[27] A study by Chakravorti highlighted that the blind copying of a General Data Protection Regulation (GDPR)-like framework in developing countries is often undesirable, given their lack of both financial resources and the expertise to effectively implement these laws.[28] These findings are both significant and concerning, as data protection is a core component of

[21] Several requirements exist for data localisation in Rwanda. See, eg Regulation No 02/2018 on Cybersecurity of 24 January 2018, Art 3; Law No 16/2010 Governing Credit Information Systems of 7 May 2010, Art 4; Regulation No 03/2018 on Outsourcing of 24 January 2018, Art 15.2(d); Law No 058/2021 Relating to the Protection of Personal Data and Privacy of 15 October 2021, Art 50. In its Data Revolution Policy, Rwanda views data as a 'national sovereign asset'. The document also sets out Rwanda's ambition to build a robust data industry. See Ministry of Youth and ICT, Data Revolution Policy (April 2017, Rwanda) 6, 11.

[22] See, eg Department of Communications and Digital Technologies, Invitation to Submit Written Submissions on the Proposed National Data and Cloud Policy, No 306 of 1 April 2021 (South Africa) 28.

[23] See, eg Draft Data Protection Bill, 2023 (Pakistan), s 14.1; Citizens Protection (Against Online Harm) Rules, 2020 (Pakistan), s 5(d); Ministry of Commerce & Textile (Commerce Division), E-Commerce Policy Framework of Pakistan (August 2019) 28.

[24] UNCTAD, *Digital Economy Report 2021* (2021) UNCTAD/DER/2021, 83–85. See also ch 6.

[25] See generally OECD, *Development Co-operation Report 2021: Shaping a Just Digital Transformation* (2021).

[26] See comparisons of DPA budgets especially between non-OECD countries and OECD countries in M Fazlioglu, 'How DPA Budget and Staffing Levels Mirror National Differences in GDP and Population' (IAPP, 2018) 1.

[27] M Pisa and U Nwankwo, 'Are Current Models of Data Protection Fit for Purpose? Understanding the Consequences for Economic Development' (CGDev, 09 August 2021) www.cgdev.org/publication/are-current-models-data-protection-fit-purpose-understanding-consequences-economic.

[28] B Chakravorti, 'Why the Rest of the World Can't Free Ride on Europe's GDPR Rules' (HBR, 30 April 2018) www.hbr.org/2018/04/why-the-rest-of-world-cant-free-ride-on-europes-gdpr-rules.

the regulation of cross-border data flows. Weak implementation of data protection laws entails severe costs for developing countries, such as increased incidence of data breaches and reduced user trust.[29] Additional factors for this asymmetry could be the lack of sufficient digital and data infrastructure or the energy necessary to run them, as well as a dearth of sufficient local expertise to manage the infrastructure.[30]

Instead of drastic implementation of a suite of data-related laws and regulations, the data divide can be better addressed if governments carefully implement laws to address specific domestic regulatory needs, taking into account the domestic regulatory capacity and resources. For instance, in the above example, a highly complex data protection framework may increase the costs of doing business in developing countries, especially MSMEs.[31] In contrast, bigger technology companies (foreign or domestic) are likely to be much better placed to comply with onerous obligations contained in various domestic data protection laws and regulations. In most developing countries, such an outcome is counterproductive, given that the best way to bridge the divide and increase competitive opportunities in the domestic digital market is by opening up market opportunities for MSMEs and facilitating their participation in global value chains.[32]

Another example demonstrating the mismatch of regulatory intent and real-world practice can be seen in the context of open data and data sharing. There is a broad consensus that developing countries can benefit from open data and data-sharing initiatives, in particular by using public data for domestic development.[33] Several developing countries have now adopted frameworks requiring the transparent sharing of public data, thus ensuring that it is not

[29] A Chander et al, 'World Development Report 2021 – Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation' (2021) World Bank Policy Research Working Paper 9594, 39. This argument can be extended to several other data laws and regulations, such as online consumer protection and data security.

[30] For some telling statistics in this context, see UNCTAD, 'Over Half of the People in Least Developed Countries Lack Access to Electricity' (1 July 2021) www.unctad.org/topic/least-developed-countries/chart-july-2021; ITU, 'Connectivity in the Least Developed Countries: Status Report 2021 – Highlights' (2021) www.itu.int/itu-d/reports/statistics/connectivity-in-the-least-developed-countries-status-report-2021/highlights-of-the-itu-un-ohrlls-ldc-connectivity-report-2021/. However, for the purposes of this chapter, these issues are left to one side; experts have noted the need to develop a more robust data infrastructure in developing countries. See V Foster et al, 'Improving Data Infrastructure Helps Ensure Equitable Access for Poor People in Poor Countries' (*World Bank Blogs*, 06 May 2021) www.blogs.worldbank.org/opendata/improving-data-infrastructure-helps-ensure-equitable-access-poor-people-poor-countries.

[31] See cost estimates of GDPR compliance: Statista, 'Share of European Small Businesses Spending on Compliance with the General Data Protection Regulation (GDPR) in 2019, by Budget Range' (May 2019) www.statista.com/statistics/1176050/gdpr-compliance-spending-in-small-businesses-europe/.

[32] Chander et al (n 29) 39–41.

[33] See, eg PTI, 'Data for Development Will be Integral Part of Overall Theme of India's G-20 Presidency: PM Modi' (*Outlook*, 16 November 2022) www.outlookindia.com/national/-data-for-development-will-be-integral-part-of-overall-theme-of-india-s-g-20-presidency-pm-modi-news-237773.

trapped in silos and can instead be used by local companies to foster data-driven innovation.[34] Some countries are also developing frameworks mandating private companies to share anonymised data with smaller local players to foster more domestic competition and innovation.[35] Yet, the effectiveness of these frameworks varies widely due to the lack of a robust data security law, the scarcity of digital data in several developing countries or the dearth of domestic entities that have the capacity to use such data.[36] Also, access to the Internet and digital technologies does not automatically translate to meaningful use of data-driven technologies; factors such as availability of local talent and expertise are highly relevant.[37]

The second factor relevant to the global data divide is the size of the domestic digital market. For instance, a developing country with a huge population and significant digital resources, such as India or Indonesia, cannot be compared to a small-sized developing economy in Africa or Latin America in a broad-brush manner.[38] Take the example of data localisation. This is often seen as a helpful tool to drive investments in the local digital infrastructure market and increase competitive opportunities for domestic digital players. However, for a small-sized developing economy (with a small population and limited talent), data localisation is unlikely to generate a high domestic value, even in the medium term.[39] For any company (foreign or domestic) offering digital services in such a country, it is difficult to generate the economies of scale necessary for profitably operating data-driven infrastructures and services. Even the biggest technology companies have little incentive to invest in local data infrastructure in countries where the markets are too small and thus not sufficiently profitable to justify the scale of investment. Thus, in addressing the data divide, developing countries must factor the size of the domestic market and possible prospects for economic

[34] See generally SG Verhulst and A Young, *Open Data in Developing Economies – Toward Building an Evidence Base on What Works and How* (Cape Town, African Minds, 2017); B Ubaldi, 'Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives' (2013) OECD Working Papers on Public Governance No 22.

[35] See, eg J Grover, 'Norms for Non-Personal Data Sharing in the Works' (*Financial Express*, 20 March 2023) www.financialexpress.com/industry/norms-for-non-personal-data-sharing-in-the-works/3015107/; Ministry of Electronics and Information Technology, 'Report by the Committee of Experts on Non-Personal Data Governance Framework' (2020) 111972/2020/CL&ES.

[36] M Hilbert, 'Big Data for Development: A Review of Promises and Challenges' (2016) 34(1) *Development Policy Review* 135, 139–156.

[37] J Jütting and I McDonnell, 'Overview: What Will It Take for Data to Enable Development?' in OECD, *Development Co-operation Report 2017 – Data for Development* (2017).

[38] UNCTAD, *Digital Economy Report 2021* (n 24) 116 ('a world of divergent data nationalism has only a few winners and many losers. Certain established digital economies may emerge as winners due to their advantageous market size and technological prowess, but most small, developing economies will lose opportunities for raising their digital competitiveness').

[39] Even for larger developing countries like India the benefits are sometimes inconclusive, especially in the long run. See generally R Kathuria et al, 'Economic Implications of Cross-Border Data Flows' (ICRIER and IAMAI, November 2019).

return, especially when data-restrictive measures are introduced on a broad scale to bridge the data divide with richer countries.

The global data divide is also shaped by the differences in regulatory culture across countries, particularly the mechanisms for transparency and accountability in domestic data laws and regulations. The data divide can result from the power differential between various entities: between companies and their users, between big companies and small companies, between governments and digital users, between governments and companies, and between rich and poorly resourced governments. In order to address the data divide, a robust regulatory framework is necessary to address these power differentials both domestically and transnationally. For instance, to inculcate a culture of digital trust and entrepreneurship, it is important that governments do not use data regulations as a tool to illegally monitor or control their users or demand data from companies operating in their jurisdiction.[40] A data protection law that provides wide exceptions for government entities to access personal data on vague public interest grounds is not only harmful from a human rights perspective,[41] but can also significantly reduce the trust of digital users and companies.[42] These factors are likely to skew the data divide even further.

Similarly, as will be discussed in the next chapter, in regulating anti-competitive conduct in the digital market, competitor regulators must implement laws fairly and transparently, and not specifically target foreign technology companies offering good-quality services to domestic consumers in order to protect inefficient domestic companies. In other words, if competition regulation is used as an opaque tool for protectionism, then it is more likely to adversely impact the global data divide than help to bridge it.

Further, a degree of transparency and accountability is necessary at the global scale, especially in the context of development of international treaties, data standards and transnational norms, to address the different dimensions of the global data divide. Without appropriate mechanisms to involve a wide variety of stakeholders and ensure accountability and transparent participation, these global legal and policy responses are likely to worsen the data divide rather than bridge it. Section IV below revisits some of these considerations and potential responses in the context of international trade law.

The global data divide has a direct impact on cross-border data flows. As discussed earlier, several countries have used the data colonialism narrative as a basis for implementing reactionary laws and policies that restrict data flows outside their jurisdiction. However, these measures can have a drastic long-term

[40] UNGA, 'Road Map for Digital Cooperation: Implementation of the Recommendations of the High-level Panel on Digital Cooperation – Report of the Secretary-General' (29 May 2020) A/74/821, 10–12.

[41] UNGA, 'The Right to Privacy on The Digital Age – Report of the United Nations High Commissioner for Human Rights (3 August 2018) A/HRC/39/29, 10–11.

[42] ibid.

impact on the global economy, such as fragmenting the digital economy[43] or compromising the basic rights of individuals.[44] Both these factors, in turn, exacerbate the global data divide as they can severely harm both economic and social interests of individuals in developing countries and LDCs. Further, the growth of digital trade is contingent on the interconnectivity of the Internet.[45] When governments attempt to address the global data divide predominantly through data-restrictive measures, this can adversely affect the interconnectivity of the networks necessary to ensure digital trade flows. These restrictive measures can be particularly harmful for smaller, developing economies, as argued earlier.

In the current geopolitically divided world, several developing countries on the brink of a digital transformation are forced to opt for the preferred data regulatory model of a specific digital power to be able to attract investment and new business opportunities from that power. Aaronson and Leblond have argued that there are three big data realms in the world today, representing the three biggest digital powers, China, the USA and the EU.[46] All other countries are forced to align with one of these data realms for both economic and strategic reasons.[47] While most developing countries imitate a specific data regulatory model to fit into one of the three data realms, it is important to observe the nuanced adaptation of these predominant models across the developing world and its impact on the global framework for cross-border data flows.

As an example of such nuanced implementation, several countries have rapidly adopted GDPR-like regulation (often without matching regulatory capacity) in the last few years to increase the prospects of obtaining a positive adequacy finding from the European Commission.[48] Nonetheless, in adapting disciplines from the GDPR in domestic laws, many countries have introduced variations to accommodate domestic regulatory preferences, such as including broad exemptions for public authorities obtaining personal data under data

[43] Internet Society, 'Internet Way of Networking Use Case Data Localization' (September 2020) www.internetsociety.org/wp-content/uploads/2020/09/IWN-Use-Case-Data-Localization-EN.pdf; Internet Governance Forum, 'What Does Internet Fragmentation Mean to You? – Identifying Fragmentation and Key Stakeholders' (Policy Network on Internet Fragmentation Webinar, 15 September 2022) www.intgovforum.org/en/filedepot_download/256/22932.

[44] A Plaum, 'The Impact of Forced Data Localisation on Fundamental Rights' (Access Now, 4 June 2014) www.accessnow.org/the-impact-of-forced-data-localisation-on-fundamental-rights/; A Shahbaz et al, 'User Privacy or Cyber Sovereignty?' (Freedom House, July 2020).

[45] See generally JP Meltzer, 'Supporting the Internet as a Platform for International Trade Opportunities for Small and Medium-Sized Enterprises and Developing Countries' (February 2014) Brookings Global Economy and Development Working Paper 69.

[46] See generally Aaronson and Leblond (n 5) 245–72.

[47] Geneva Trade Platform, 'Is the World Dividing into Data Realms & What Does It Mean for the Nations Outside the Realms? (S40)' (*YouTube*, 31 October 2020) www.youtube.com/watch?v=YPayhR3wtDc.

[48] M Pisa et al, 'Creating a Level Playing Field for Data Protection' in OECD, *Development Co-operation Report 2021* (n 25).

protection law[49] or imposing explicit data localisation requirements for certain categories of data.[50] Another example is the influence of China in specific countries in Africa and Asia, many of which depend heavily on Chinese digital technologies[51] and thus indirectly import the data standards and regulatory model of China. Nonetheless, as Erie and Streinz argue, this is not a one-sided export of a regulatory model.[52] Rather, there are several push-and-pull factors, wherein the Chinese data regulatory model is also gradually evolving to accommodate the business needs in different jurisdictions in which Chinese companies operate.[53]

As demonstrated in some of the above examples, there is an ongoing tension between the regulatory models of digital powers and the increasing awareness among developing countries of the need to develop indigenous data regulatory requirements suited to their own domestic needs. Consequently, the regulatory framework for cross-border data flows has become even more fragmented and is practically unnavigable for a large majority of companies operating in the digital sector. Companies based in developing countries (especially small-sized economies) and LDCs will be the most affected by such fragmentation and legal uncertainties. Therefore, in exploring how to respond to the global data divide, developing countries must consider multiple factors affecting their domestic digital economy, instead of solely relying on asserting data sovereignty through data-restrictive measures.

[49] See, eg K Trisadikoon, 'Personal Data at Risk in Govt Hands' (TDRI, 31 August 2022) www.tdri.or.th/en/2022/08/personal-data-at-risk-in-govt-hands/, referring to the Personal Data Protection Act (Thailand) BE 2562, 27 May 2019, s 4(2); A Verma, 'India's Latest Draft Bill on Data Protection: Exemption Clause and Related Privacy Concerns' (OHRH, 22 December 2022) www.ohrh.law.ox.ac.uk/indias-latest-draft-bill-on-data-protection-exemption-clause-and-related-privacy-concerns/, referring to the Digital Personal Data Protection Bill, 2022 (India), s 18(2)(a).

[50] See, eg Law No 058/2021 Relating to the Protection of Personal Data and Privacy of 15 October 2021 (Rwanda), Art 50; M Kijirah and EW Thuo, 'Data Protection and Data Localisation in Kenya: Potential Economic Impact and Effect – On Kenya's Commitments in Various Regional Treaty Frameworks' (2021) Mandela Institute Policy Brief 03, 4–5 (discussing data localisation laws in Kenya).

[51] Huaxia, 'Southeast Asia Eyes on Chinese Digital Technology to Boost Recovery' (Xinhua, 20 September 2022) www.english.news.cn/20220920/0cd0a97954394ea8bac0a6f90fc14ab8/c.html; Xinhua, 'Chinese Technology Helps Africa Pursue Quality Development' (SCIO PRC, 16 May 2023) www.english.scio.gov.cn/internationalexchanges/2023-05/16/content_85339573.htm; M Agbebi, 'China's Digital Silk Road and Africa's Technological Future' (CFR, 01 February 2022) www.cfr.org/sites/default/files/pdf/Chinas%20Digital%20Silk%20Road%20and%20Africas%20Technological%20Future_FINAL.pdf.

[52] MS Erie and T Streinz, 'The Beijing Effect: China's Digital Silk Road as Transnational Data Governance' (2021) 54(1) *Journal of International Law and Politics* 1, 23–24.

[53] Also, unlike the EU model, Chinese investment in the digital sector in developing countries or LDCs does not make any explicit requirement for the adoption of a specific regulatory framework, although it still continues to exercise 'discursive power' through technologies. `See Y Chang, 'China Beyond China, a Digital Order with Chinese Characteristics? China's Discursive Power and Its Global Digital Vision' (2023) 51(2) *Politics & Policy* 283, 289–90. See generally MFA PRC, 'Global Initiative on Data Security' (8 September 2020) www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202009/t20200908_679637.html.

III. ADDRESSING GLOBAL DATA DIVIDE IN INTERNATIONAL TRADE AGREEMENTS

Having briefly explored the multiple dimensions of the global data divide and its impact on the regulatory framework for cross-border data flows, this section investigates the extent to which international trade agreements intersect with the global data divide. While section IIIA focuses on World Trade Organization (WTO) law, section IIIB focuses on disciplines in PTAs. This section argues that existing disciplines in WTO law focusing on trade and development as well as the general exceptions do not provide a robust foundation for bridging the global data divide. Further, although disciplines on electronic commerce or digital trade chapters have now become common in PTAs, these treaties have also remained largely silent in directly addressing relevant aspects of the global data divide.

A. WTO Law and the Global Data Divide

The framework treaties of the WTO were written before the current era of digital trade; thus, they do not contain specific rules on digital trade. Nonetheless, it may be helpful to consider how WTO law broadly addresses development-related issues. The SDT disciplines lie at the crux of the trade–development interlinkage.[54] Usually, SDT provisions contain some concessions to developing countries and LDCs, such as a longer implementation period for compliance with obligations, preferential trading opportunities, the ability to incorporate flexible commitments and a greater choice of policy instruments, and specific concessions provided to LDCs.[55] Further, many WTO treaties contain specific soft law provisions, wherein developed countries are encouraged to provide capacity-building support to developing countries and take into account the need to safeguard their interests.[56]

To date, the SDT provisions in WTO treaties have generally been ineffective in addressing development-related concerns. First, the majority of SDT provisions are non-binding or aspirational in nature. For instance, as per a study conducted by Hegde and Wouters, only 21 per cent of SDT provisions found in WTO treaties are binding and provide specific privileges to developing countries.[57] The remainder of the provisions are hortatory in nature. Other

[54] See generally C Sieber-Gasser, *Developing Countries and Preferential Services Trade* (Cambridge, Cambridge University Press, 2016) 294–316.

[55] WTO, 'Special and Differential Treatment Provisions', www.wto.org/english/tratop_e/devel_e/dev_special_differential_provisions_e.htm.

[56] ibid.

[57] V Hegde and J Wouters, 'Special and Differential Treatment Under the World Trade Organization: A Legal Typology' (2021) 24(3) *Journal of International Economic Law* 551.

studies confirm that only a small percentage of SDT provisions are binding in nature, although the variations depend on how different scholars classify the binding nature of provisions.[58]

Second, the formulation of the majority of SDT provisions is unclear; in particular, it is not clear if the SDT provisions can be viewed as a right of developing countries and a duty/obligation for developed countries.[59] Lamp has even argued that SDT provisions were framed as charity provisions, rather than a meaningful obligation for developed countries.[60] Looking at the history of SDT, these provisions were created as a very limited and special exception to the language contained in general obligations in WTO law.[61]

Third, developing countries face constraints in enforcing SDT provisions, as evidenced in a number of past WTO disputes, thus raising doubts about their relevance and effectiveness.[62] Finally, scholars have found that the SDT provisions are not specifically tailored to address the different developmental needs across developing countries.[63] They are based on a flawed self-declaration criterion and do not account for the huge variations across developing countries in different sectors.

The General Agreement on Trade in Services (GATS) contains specific provisions aimed at providing support to developing countries for services trade, but none of these provisions are likely to be very effective in dealing with the concerns relating to the global data divide. For instance, GATS, Article IV sets out a general provision aimed at increasing participation of developing countries in trade in services. Without necessarily outlining a specific duty for developed countries, this provision states a high-level provision aimed at strengthening the domestic services competitiveness of developing countries through various means such as access to technology, information networks and liberalisation of market access in sectors of export interest.[64] It also contains a best efforts provision, wherein developed countries to the extent possible must establish contact points to provide information to developing countries regarding different aspects

[58] See, eg F Garcia, 'Beyond Special and Differential Treatment' (2004) 27(2) *Boston College International and Comparative Law Review* 291, 310–11.

[59] Hegde and Wouters (n 57) 555–64.

[60] N Lamp, 'How Some Countries Became "Special": Developing Countries and the Construction of Difference in Multilateral Trade Lawmaking' (2015) 18(4) *Journal of International Economic Law* 743, 744.

[61] ibid 750.

[62] Hegde and Wouters (n 57) 567 (discussing the failure of developing countries such as India to enforce SDT provisions in WTO disputes pre-Doha negotiations, citing examples such as *United States – Anti-Dumping and Countervailing Measures on Steel Plate from India*, Panel Report (adopted 29 July 2002) WT/DS206/9). See Answers of India to Questions of the Panel – First Meeting, WT/DS206/R, para 36, question 25; *European Communities – Anti-Dumping Duties on Imports of Cotton-Type Bed Linen from India*, Appellate Body Report (adopted 13 March 2001) WT/DS141/19, para 6.233.

[63] J Bacchus and I Manak, *The Development Dimension Special and Differential Treatment in Trade* (Abingdon, Routledge, 2021) 15, 19, 20.

[64] GATS, Art IV.

of services regulation, such as technical requirements and professional qualifications, with priority given to LDCs.[65]

In the Working Programme on Electronic Commerce, certain members had discussed the relevance of GATS, Article IV in the context of enabling greater participation of developing countries in e-commerce.[66] However, this provision is not specifically relevant to addressing the concerns raised earlier in the context of the global data divide, nor is it particularly meaningful due to the absence of clear, binding provisions. Article XII deals with the concessions provided to developing countries during serious balance-of-payments and external financial difficulties.[67]

The GATS Annex on Telecommunications also contains specific provisions aimed at addressing developmental concerns in developing economies.[68] It sets out a broader obligation on technical cooperation in the development of telecommunications infrastructure through both multilateral development institutions and other regional groupings.[69] It also contains a best-efforts provision to provide information to developing countries regarding the developments in information and communications technology (ICT) technologies and pays specific attention to LDCs in the context of technology transfer and other support mechanisms necessary for developing their telecommunications infrastructure.[70] Although this provision outlines certain helpful tools to help developing countries foster data-driven development, it has limited impact as it is not binding on the parties.

In addition to the above, provisions on technology transfer can also be found in the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). Article 8.2 of the TRIPS makes a cursory reference to the need for the international transfer of technology to address developing country concerns.[71] Article 66.2 of the TRIPS, which is focused on LDCs, provides that developed countries 'shall provide incentives to enterprises and institutions in their territories for the purpose of promoting and encouraging technology transfer to least-developed country Members in order to enable them to create a sound and viable technological base'.[72] While these two provisions provide a basis for technology transfer that can accelerate data-driven development in developing countries and LDCs, it is unlikely to be meaningful as they are best-efforts provisions and do not set out any clear mechanisms or tools for technology transfer.

[65] ibid Arts IV:2 and IV:3.

[66] WTO, 'Work Programme on Electronic Commerce – Progress Report to the General Council' (July 1999) S/L/74, para 10.

[67] GATS, Art XII.

[68] GATS, Annex on Telecommunications, Art 6.

[69] ibid Art 6.

[70] ibid Art 6(d).

[71] Agreement on Trade-Related Aspects of Intellectual Property Rights, Annex 1C of Marrakesh Agreement Establishing the World Trade Organization (Marrakesh, 15 April 1994), Art 8.2.

[72] ibid Art 66.2.

The Reference Paper on Domestic Services Regulation,[73] which has been signed by 67 members as of July 2023, contains certain disciplines on capacity building and technical assistance that could be relevant in the context of data regulation (although this provision is also aspirational in nature). It states that all developed and developing members (who are 'in a position to do so') are 'encouraged to provide specific technical assistance and capacity building' support to developing countries and LDCs. This support must be provided 'upon their request and on mutually agreed terms and conditions'.[74] Some of the specific areas identified for technical assistance and capacity building include: capacity-building support for regulating supply of services; assisting service suppliers of developing countries and LDCs to meet requirements in export markets and to comply with domestic services regulation; and facilitating the participation of developing countries and LDCs in relevant international bodies discussing standard-setting issues.[75] This provision provides a potential avenue to offer technical assistance and capacity building in several areas of data regulation related to the supply of digital services. However, given that this is a best-efforts provision, its implementation is dependent solely on political will.

While the digital or data divide is not specifically covered in the WTO treaties, a WTO dispute between the EU and Brazil raised certain specific questions regarding the ability of countries to justify measures aimed at addressing the digital divide under the general exception contained in the General Agreement on Tariffs and Trade (GATT), Article XX(a).[76] The language in the Article states that a measure may be justified if it is necessary to protect public morals. The Brazilian government had implemented a domestic programme under which only domestically manufactured ICT products could attract tax benefits. This measure was found to be in violation of the non-discrimination requirement set out in Article III:4 of the GATT.[77] However, the Brazilian government argued that this programme could be justified under GATT, Article XX(a) as it was necessary to protect public morals related to digital inclusion.[78] In this dispute, the WTO panel interpreted the scope of 'public morals' very broadly and agreed that it could include digital inclusion,[79] but found that the specific Brazilian programme did not meet the other requirements of the necessity test.[80]

The *Brazil – Taxation* case, discussed above, raises broader questions regarding the relevance of the general exceptions in justifying the measures

[73] WTO, 'Reference Paper on Services Domestic Regulation – Note by the Chairperson' (27 September 2021) INF/SDR/1 (Reference Paper on Services Domestic Regulation).
[74] Reference Paper on Services Domestic Regulation, s I, para 13.
[75] ibid.
[76] *Brazil – Certain Measures Concerning Taxation and Charges*, Panel Report (adopted 11 January 2019) WT/DS472/16/Add.2 (Brazil Taxation Panel Report).
[77] ibid para 7.751.
[78] ibid paras 7.544–7.549.
[79] ibid paras 5.561–5.565.
[80] ibid para 7.622.

necessary to bridge the data divide. For instance, can a developing country rely on GATS, Article XIV(a) to argue that a specific data-restrictive measure aimed at helping domestic digital sectors falls within the scope of 'public morals'? In other words, is bridging the global data divide a sufficient basis to establish a public morality under GATS, Article XIV(a)? As Peng has observed, based on the WTO panel's reasoning, it can be theoretically argued that any measure aimed at bridging the data divide within a country falls within the scope of public morals.[81] This could especially be the case if that member could provide examples of policy or regulatory frameworks that clearly set out the data divide as a public policy concern and perhaps even make references to Sustainable Development Goals relevant to digital inclusion.[82]

However, such a high degree of ambiguity in defining public morals can lead to significant legal uncertainty. Further, this exception by itself is unlikely to provide sufficient policy comfort to countries that actively seek to introduce data-restrictive measures to bridge the global data divide.[83] Thus, despite there being a slim possibility to use the general exceptions to defend data-restrictive measures implemented by developing countries to address the global data divide, the general exceptions do not provide a clear basis for imposing such measures.

B. Addressing the Global Data Divide in PTAs

This section looks at the digital trade/electronic commerce chapters in PTAs to investigate whether they contain more tailored provisions to address the global data divide. Broadly speaking, provisions that enable cross-border data flows facilitate digital trade flows and can also be beneficial for developing countries.[84] However, as argued earlier, these provisions can be meaningful only if developing countries have the resources to implement robust regulatory frameworks on data regulation and provide adequate support and market opportunities to domestic companies to participate in the domestic and global digital economies. This kind of support is especially important for MSMEs based in developing countries and LDCs, as they usually lack the expertise or resources to compete with companies based in developed countries.

Several PTAs (often led by developed economies such as the USA, Australia, Singapore and Japan, but also adopted by certain Asia-Pacific and Latin American economies) contain provisions requiring countries to not restrict cross-border data flows necessary for digital trade and prohibiting countries

[81] Peng (n 8) 220.
[82] See, eg Brazil Taxation Panel Report (n 76) para 7.592.
[83] Peng (n 8) 221.
[84] OECD, 'Fostering Cross-Border Data Flows with Trust' (2022) OECD Digital Economy Papers No 343, 8–9.

from imposing data localisation measures.[85] They are typically subject to a legitimate public policy exception, provided that the measure is not arbitrary or unjustifiable discrimination or a disguised restriction on trade. Therefore, unlike the GATS general exceptions, PTAs provide more scope to developing countries to implement data-restrictive measures for the purposes of bridging the data divide (assuming it is a legitimate public policy objective). Nonetheless, such measures may fail to satisfy the requirement of not being arbitrary or unjustifiable discrimination or a disguised restriction on trade. This is especially the case for data localisation measures, where the evidence is currently inconclusive regarding both the public policy benefits and the economic returns to the domestic digital economy.

Unsurprisingly, several developing countries have argued that the above provisions constrain their policy space to adopt digital industrial policies such as data localisation. The Regional Comprehensive Economic Partnership (RCEP) contains an alternative iteration of this provision with a self-judging exception. Under the relevant provisions on data localisation and cross-border data flows, parties have agreed that they can restrict cross-border data flows or impose data localisation measures if they consider the measure necessary to achieve a legitimate public policy objective, 'provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade'.[86] The footnote to this provision further clarifies that 'the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party'.[87] Further, any provisions contained in the RCEP digital trade chapter are not subject to dispute settlement.[88]

Developing countries concerned about their policy space to impose data-restrictive measures for digital development purposes are likely to steer towards a RCEP-like provision in their PTAs.[89] Although this provision does provide greater scope for countries to impose data-restrictive measures, including for bridging the data divide, it also creates legal uncertainty and potential for tit-for-tat protectionism. At the same time, the US approach to PTAs (as reflected in the Agreement between the United States of America, the United Mexican States, and Canada (USMCA) or the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)) also entails concerns for developing countries adversely affected by the global data divide. For instance, although there are binding obligations on the free flow of data, the provisions on developing a

[85] M Burri and R Polanco, 'Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset' (2020) 23(1) *Journal of International Economic Law* 187, 211–15.

[86] RCEP, Arts 12.15.3, 12.14.3.

[87] ibid Art 12.15.3, fn 14, Art 12.14.3, fn 12.

[88] ibid Art 12.17.

[89] N Mishra and AMP Valencia, 'Digital Services and Digital Trade in the Asia Pacific: An Alternative Model for Digital Integration?' (2023) 31(2) *Asia Pacific Law Review* 489, 510.

robust regulatory framework for cross-border data flows such as data protection and online consumer protection are much vaguer.[90]

Further, while several PTAs contain general provisions on cooperation, there is no provision outlining an obligation on the developed countries to provide technical assistance and capacity-building support to the developing countries in adopting domestic data regulatory frameworks. Recent years have seen certain countries signing separate agreements to offer such assistance/support to their developing partner countries especially in bilateral arrangements,[91] but they are not sufficient by themselves to build a framework that addresses the global data divide. The absence of robust and effective data regulatory frameworks in several developing countries and especially LDCs can contribute to the global data divide.[92]

While there is a high degree of variation across PTAs, most provisions pertaining to areas such as online consumer protection and cybersecurity are weakly worded, entailing a high-level obligation to adopt laws to prohibit fraudulent and deceptive commercial activities (with no specific reference to international benchmarks or best practices) and a general agreement that parties would cooperate on relevant matters of online consumer protection and privacy.[93] Further, although the USMCA refers to the necessity of adopting a risk-based approach to cybersecurity,[94] most developing countries/LDCs with limited regulatory expertise are likely to find it harder to monitor the implementation of a risk-based approach.

Further, as discussed previously in chapter two, the scope and comprehensiveness of the disciplines on data protection/privacy vary significantly across PTAs. Even in PTAs involving developing economies, there are no specific dedicated provisions on providing technical assistance or capacity-building support to developing countries, despite the presence of a binding obligation to adopt a domestic data protection law consistent with international standards. While digital economy agreements (DEAs) have made advancements such as explicitly agreeing upon certain high-level principles of data protection[95] and the

[90] In the context of CPTPP and the imbalance between provisions on data flows and key regulatory frameworks on digital regulation, see N Mishra, 'The Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance?' (2017) 20(1) *Journal of International Economic Law* 31.

[91] See, eg AC Koty, 'Thailand and Singapore Sign Agreements to Deepen Economic Cooperation' (ASEAN Briefing, 21 November 2022) www.aseanbriefing.com/news/thailand-and-singapore-sign-agreements-to-deepen-economic-cooperation/; MTI, 'The Singapore Australia Digital Economy Agreement (SADEA)', www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Singapore-Australia-Digital-Economy-Agreement.

[92] World Bank, *World Development Report* (n 1).

[93] This language is found in most US-led PTAs, such as the USMCA and other PTAs that follow the CPTPP model.

[94] USMCA, Art 19.15.2.

[95] See UK–Singapore Digital Economy Agreement (Singapore, 25 February 2022), Art 8.61E(3) (UKSDEA); Korea–Singapore Digital Partnership Agreement (Singapore, 21 November 2022), Art 14.17.3 (KSDPA); DEPA, Art 4.2.3; SADEA, Art 17.3.

development of mutual recognition mechanisms,[96] they do not contain any capacity-building requirements except for a general provision for information exchange.[97]

Some DEAs contain provisions on digital inclusion and data innovation that can be relevant to addressing specific concerns related to the data divide, especially if more developing countries join them.[98] For instance, Module 11 of the Digital Economy Partnership Agreement (DEPA) recognises that specific groups, such as rural populations, women, indigenous peoples and socioeconomically disadvantaged communities, face challenges to benefiting from the digital economy. Therefore, DEPA parties have agreed to cooperate to remove barriers to their digital inclusion and to cooperate in a range of areas to improve participation of digitally excluded groups in the digital economy.[99] The module further acknowledges the need to involve civil society bodies in the development of relevant initiatives.[100]

The UK–Singapore Digital Economy Agreement (UKSDEA) and the United Kingdom–New Zealand Free Trade Agreement (UK–NZ FTA) include additional provisions to foster digital inclusion, including acknowledging the impact of digital markets on labour conditions[101] and the importance of removing trade barriers for SMEs in the digital economy,[102] and agreeing to cooperate to reduce the digital divide between developed and developing countries.[103] In particular, the latter provision is significant as these two agreements currently do not have a developing country party, yet the party countries have agreed upon 'sharing best practices, collaborating on capacity building initiatives, active engagement in international fora and promoting [developing] countries' participation in, and contribution to, the global development of rules on digital trade'.[104] This provision could be instrumental in supporting developing countries participating in the ongoing e-commerce negotiations under the Joint Initiative at the WTO.

In conclusion, the majority of the existing international trade agreements, including new-generation DEAs, do not contain substantial provisions to address the global data divide. While there are some positive developments, such as digital inclusion provisions in DEAs, core issues, including providing tailored regulatory assistance and capacity-building support or developing clear mechanisms for technology transfer are not addressed. Without such fundamental reforms, the inclusion of disciplines on cross-border data flows will create more

[96] See, eg UKSDEA, Art 8.61E(6); KSDPA, Art 14.17.6; DEPA, Art 4.2.6; SADEA, Art 17.7.

[97] See, eg UKSDEA, Art 8.61E(7); KSDPA, Art 14.17.7; DEPA, Art 4.2.7, 4.2.9.

[98] Examples include DEPA, UKSDEA and UK–NZ FTA. The India–UAE Comprehensive Economic Partnership Agreement (New Delhi, 18 February 2022) also makes a reference to cooperation on digital inclusion and digital divides (see Art 9.13.2(a)).

[99] See DEPA, module 11.

[100] DEPA, Art 11.1.4.

[101] UKSDEA, Art 8.61P(1).

[102] UK–NZ FTA, Art 15.20.3.

[103] UKSDEA, Art 8.61P(4); UK–NZ FTA, Art 15.20.4.

[104] UKSDEA, Art 8.61P(4); UK–NZ FTA, Art 15.20.4.

aversion amongst developing countries to sign up to comprehensive digital trade rules. Further, the lack of robust cooperation mechanisms between developed and developing countries leads to further distrust and disengagement, resulting in more data-restrictive measures and further fragmentation.

IV. A REFORM AGENDA TO BRIDGE THE GLOBAL DATA DIVIDE

As the discussions in the previous sections illustrate, international trade law is not fit for purpose in dealing with several of the challenges pertaining to the global data divide. This section first briefly outlines the various deficiencies, focusing particularly on the lack of streamlined provisions on SDT, the absence of meaningful technology transfer mechanisms and uncertainties in the application of existing disciplines, including the moratorium on customs duties on e-commerce. Coupled with the lack of sufficient input and participation from developing countries and LDCs in ongoing trade negotiations, these deficiencies are particularly concerning. The section then provides a proposal for reforming future international trade agreements to better address this divide.

A. Deficiencies in International Trade Law

A robust system of SDT is the bedrock of developing an inclusive and equitable global economy.[105] However, as discussed in the previous section, most trade treaties have not adopted a streamlined SDT mechanism. The existing disciplines are neither precise on the substantive obligations and rights, nor have they been effective in practice. Given that the majority of these provisions are non-binding, most compliance remains voluntary and there is no accountability for developed countries in implementing SDT provisions.

In the context of the data-driven economy, the need for a tailored SDT mechanism is evident, especially given that many PTAs impose a range of obligations on developing countries to open up their digital sector and undertake massive regulatory reform to enable digital trade.[106] For instance, most treaties do little to account for the differences in regulatory capacity among countries to adopt

[105] See generally Sieber-Gasser (n 54).

[106] These concerns have been raised in the ongoing joint initiative discussions on e-commerce at the WTO. For instance, Nigeria proposed that developing countries and LDCs must enjoy a wider policy space to implement digital industrial policies. China, Indonesia and Ivory Coast all proposed a TFA-like model for digital trade. Ukraine acknowledged the need to make SDT an integral part of the plurilateral agreement on e-commerce. Ivory Coast has also made some far-reaching proposals to set up a fund to help MSMEs in LDCs as well as facilitate technology transfer to the developing world. Since the joint initiative on e-commerce negotiations are not in the public domain, it is unclear how these proposals have been received by other WTO members. See WTO, 'Electronic Commerce Negotiations – Consolidated Negotiating Text' (14 December 2020) INF/ECOM/62/Rev.1; WTO, 'Joint Statement on Electronic Commerce – Communication from Ukraine' (6 May 2019)

highly complex frameworks in areas such as data protection, cybercrime and online consumer protection. While some treaties, such as the CPTPP and RCEP, provide additional time to certain developing or LDC parties to implement data regulatory frameworks, this concession is not enough by itself to address the capacity deficit in most developing countries. While trade bodies cannot themselves develop substantive norms in areas of digital regulation, they can be effective sites to foster data/digital regulatory cooperation among countries, as argued later in chapter seven.

Second, the lack of strong disciplines on technology transfer in both WTO law and PTAs is another major deficiency in international trade law today. Digital and data-driven technologies provide enormous opportunities for economic growth and development.[107] However, in order for developing countries to benefit from these technologies, they must build digital tools suited to their domestic needs.[108] Blind use of dominant foreign digital technologies can pose various serious public policy concerns, as is well illustrated by the malfunctioning of artificial intelligence-driven technologies and the consequent harm caused to poorer populations.[109] A more judicious approach would be to enable developing country stakeholders to participate in the development and design of data-driven technologies, and especially to provide technology transfer assistance in customising dominant digital technologies to local context. This would not only benefit developing countries, but would also create new business opportunities for companies based in the developed world. Bodies such as the WTO Working Group on Transfer of Technology[110] could discuss specific modalities of technology transfer,[111] including building upon existing TRIPS mechanisms, as discussed in section IIIA.

Third, the existing disciplines in international trade law also lead to legal uncertainty for governments of developing countries, as explained briefly earlier. One of the most concerning developments is the increasing uncertainty regarding the status of the moratorium on customs duties on electronic commerce.

INF/ECOM/28; WTO, 'Joint Statement on Electronic Commerce – Communication from Cote d'Ivoire' (14 November 2019) INF/ECOM/46.

[107] Digital technologies such as AI can also impact labour markets in the developing world, especially when governments fail to undertake substantive domestic reforms. See C Alonso et al, 'How Artificial Intelligence Could Widen the Gap between Rich and Poor Nations' (*IMF Blog*, 2 December 2020) www.imf.org/en/Blogs/Articles/2020/12/02/blog-how-artificial-intelligence-could-widen-the-gap-between-rich-and-poor-nations.

[108] See generally B Hoekman et al, 'Transfer of Technology to Developing Countries: Unilateral and Multilateral Policy Options' (2005) 33(10) *World Development* 1587, 1590.

[109] See generally G Curto et al, 'Are AI Systems Biased Against the Poor? A Machine Learning Analysis Using Word2Vec and GloVe Embeddings' [2022] *AI & Society*; L Anderson, 'Artificial Intelligence in International Development: Avoiding Ethical Pitfalls' [20 May 2019] *Journal of Public & International Affairs* https://jpia.princeton.edu/news/artificial-intelligence-international-development-avoiding-ethical-pitfalls.

[110] WTO, 'WTO Members Take Steps to Invigorate Working Group on Trade and Transfer of Technology', https://www.wto.org/english/news_e/news22_e/devel_24nov22_e.htm.

[111] WTO, 'The Role of Transfer of Technology in Resilience Building – Communication from Namibia' (3 July 2023) WT/WGTTT/W/34.

This moratorium was instituted in 1998 at the Second WTO Ministerial Conference, wherein members agreed to not impose customs duties on electronic transmissions.[112] The term 'electronic transmissions' was not, however, specifically defined. Since then, the moratorium has been renewed at subsequent Ministerial Conferences.

Recent years have seen a group of developing countries, including India, South Africa and Indonesia, oppose the renewal of the moratorium.[113] The key concerns are that the moratorium leads to significant tariff losses for developing countries and that developed countries have deliberately expanded its scope to cover content of transmissions, which was not agreed at the WTO in 1998.[114] In the 13th Ministerial Conference, WTO members decided to renew this moratorium until the next ministerial meeting or until 31 March 2024.[115] While the economic evidence is in conflict,[116] at least some experts have argued that the discontinuation of the moratorium would lead to economic losses for developing countries.[117] Further, the uncertainty regarding the legal status of the moratorium translates into business uncertainty, especially for global businesses that rely heavily on cross-border data flows.

Another example of legal uncertainty is whether developing countries can use the general exceptions in WTO treaties and PTAs to defend their digital industrial policies. More specifically, as certain data-restrictive measures implicate obligations contained in trade treaties, developing countries using such measures to boost the domestic digital sector may face legal repercussions. The

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

[113] See, eg Third World Network, 'Trade: Indonesia Demonstrates Why E-commerce Moratorium Must End' (28 April 2023) www.twn.my/title2/wto.info/2023/ti230416.htm; WTO Work Programme on Electronic Commerce, 'The E-Commerce Moratorium and Implications for Developing Countries: Communication from India and South Africa' (4 June 2019) WT/GC/W/774; WTO Work Programme on Electronic Commerce, 'The Moratorium on Customs Duties on Electronic Transmissions: Need for Clarity on Its Scope and Impact' (8 November 2021) WT/GC/W/833.

[114] WTO, 'The Moratorium on Customs Duties' (n 113).

[115] WTO Work Programme on Electronic Commerce, 'Ministerial Decision' (22 June 2022) WT/MIN(22)/32 – WT/L/1143.

[116] While Banga has provided potential estimates of tariff revenue losses for developing countries and LDCs resulting from the continuation of the moratorium, the European Centre for International Political Economy (ECIPE) and the OECD have presented contrasting evidence suggesting that the discontinuation of the moratorium would lead to economic losses in the developing world. See R Banga, 'WTO Moratorium on Customs Duties on Electronic Transmissions: How Much Tariff Revenue Have Developing Countries Lost?' (3 June 2022) South Centre Research Paper No 157; A Andrenelli and JL González, 'Electronic Transmissions and International Trade – Shedding New Light on the Moratorium Debate' (13 November 2019) OECD Trade Policy Working Paper No 233; H Lee-Makiyama and BN Gopalakrishnan, 'The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions' (August 2019) ECIPE Policy Brief No 3.

[117] S Evenett, 'Is the WTO Moratorium on Customs Duties on Commerce Depriving Developing Countries of Much Needed Revenue?' (St Gallen Endowment, 12 November 2021) www.globaltradealert.org/reports/download/80; Andrenelli and González, 'Electronic Transmissions and International Trade' (n 116).

general exceptions in GATS does not specify such an exception, although the panel has previously acknowledged that addressing the digital divide could fall within the scope of the public morals exception.[118] The exception in electronic commercial chapters allowing countries to impose restrictions on data flows for 'legitimate public policy objectives' is more open. Callo-Müller and Kugler argue that these exceptions must be read in a more flexible manner to accommodate the digital development interests of LDCs.[119] However, the existing language and the lack of an illustrative list of legitimate public policy objectives can create a high degree of uncertainty for developing countries that choose data-restrictive measures as a tool for domestic industrial policy.[120]

Finally, to date, most developing countries have failed to voice their specific concerns about digital trade in appropriate trade and non-trade fora, including Internet policy bodies, leading to a high level of dissatisfaction and even disengagement with digital trade negotiations at the WTO and elsewhere.[121] This lack of voice is especially concerning as the narrative on the free flow of data is often seen as being one-sided, favouring the developed world. However, as discussed earlier, cross-border data flows also hold the potential to benefit developing countries if specific preconditions, such as robust regulations and access to economic opportunities, are satisfied. Therefore, in conducting the cost–benefit analysis of data-restrictive measures, the context is relevant. For example, the impact of a data-restrictive measure in a densely populated, middle-income Asian country could be different from the impact on a small-sized LDC in Africa or Central Asia.

Another area where the lack of voice for developing countries poses a challenge for both digital trade and global data governance is international standard setting for data-driven technologies and services. The existing processes in many of the mainstream standard-setting institutions do not address fundamental inequalities across countries or the fact that different developing countries may have different kinds of regulatory capacity or negligible capacity/expertise to participate in key standard-setting institutions.[122]

[118] See the earlier discussion on *Brazil – Taxation* in s IIIA.

[119] MV Callo-Müller and K Kugler, 'Digital Trade, Development, and Inequality' (2023) 117 *AJIL Unbound* 116, 120.

[120] This uncertainty is especially troubling as several developing countries view trade agreements as being designed to constrain policy space for digital industrial policies. See S Azmeh et al, 'The International Trade Regime and the Quest for Free Digital Trade' (2019) 22(3) *International Studies Review* 671.

[121] A Sen, 'India, South Africa, Namibia Oppose Talks at WTO on e-Commerce, Investment, MSMEs' (*The Hindu*, 28 February 2022) www.thehindubusinessline.com/economy/india-south-africa-namibia-oppose-talks-at-wto-on-e-commerce-investment-msmes/article65093297.ece.

[122] See generally P Delimatsis, 'Global Standard-Setting 2.0: How the WTO Spotlights ISO and Impacts the Transnational Standard-Setting Process' (2018) 28(2) *Duke Journal of Comparative & International Law* 273.

B. Towards Inclusive and Balanced Trade Rules for Addressing the Global Data Divide

Given that international trade agreements suffer from several deficiencies in addressing the global data divide, the next question is what can be done. The first area of reform is developing a more robust and tailored mechanism for SDT in digital trade chapters of PTAs and, subsequently, under the plurilateral joint initiative agreement on e-commerce at the WTO. To streamline SDT in the digital sectors, all obligations of a country in relation to digital trade issues must be specifically linked to its digital development status using basic indicators such as Internet penetration rates, digital education and the availability of digital and data resources. Further, using a model similar to the Trade Facilitation Agreement,[123] countries must be bound by specific obligations such as liberalising data flows contingent on developed countries offering relevant technical assistance and regulatory support to develop domestic digital regulatory frameworks.[124]

Technical assistance/regulatory support programmes can be designed in such a manner that they provide resources to developing countries to undertake evidence-based studies on what data and digital regulations would be most effective and feasible for domestic development and the areas where foreign technical assistance and support will be most necessary to develop the domestic digital industry. Thus, the agency to make these choices must shift from the developed world to developing countries, thus giving them a stronger incentive to participate in framing digital trade rules.

Further, regulatory assistance should be focused on providing support based on high-level policy outcomes (eg compliance with fundamental principles of data protection) rather than specific regulatory design (eg all countries must adopt an adequacy-based or accountability-based approach in cross-border data flows). In the absence of these safeguards to protect the autonomy of developing countries, they may remain overly cautious of signing PTAs or WTO agreements that focus on data flows and data localisation.

Second, as has already been discussed elsewhere in the literature, technology transfer is a key tool to supporting developing countries.[125] In the data-driven

[123] WTO General Council, Annex to the Protocol Amending the Marrakesh Agreement Establishing the World Trade Organization Agreement on Trade Facilitation (27 November 2014) WT/L/940.

[124] WTO, 'Trade Facilitation – Cutting "Red Tape" at the Border', www.wto.org/english/tratop_e/tradfa_e/tradfa_introduction_e.htm. Under the TFA, all developed countries have committed to the substantive obligations and will immediately enforce them. Developing countries have more flexibility and there are categories of obligations: Category A notifications, which they will implement immediately; Category B notifications, which will be implemented after a transition period; and Category C provisions, which will be implemented on the condition that these countries receive capacity-building support from developed countries.

[125] See, eg FM Abbott, 'Under the Radar: Reflections on "Forced" Technology Transfer and the Erosion of Developmental Sovereignty' (2020) 69(3) *GRUR International* 260; Hoekman et al (n 108).

world, several possibilities exist in mutually developing data-driven solutions wherein both developed and developing countries can benefit.[126] For instance, while a leading digital service provider from a rich country may have a highly successful platform, a local entrepreneur in a developing country may be able to develop customised innovations in apps and services more suited for the platform in the domestic market. This kind of limited technology transfer mechanism can be a win–win solution for both sets of countries.

DEAs providing high-level provisions on open data initiatives[127] and cross-border sandboxing for developing new digital technologies/regulatory frameworks[128] can be a foundation to developing more formal technology transfer mechanisms. For example, in the ASEAN region, the Global System for Mobile Communications Association (an industry organisation) has proposed a sandbox to enable cross-border data flows in the ASEAN region in a 'controlled environment' to test the optimal methods to transfer data while considering cybersecurity concerns.[129] Depending on how this proposal is implemented in the future, this sandbox can be used for the exchange of technical information and expertise between technology giants and local digital entrepreneurs in developing ASEAN countries.

Third, despite the breakneck speed at which the digital economy is evolving, the data regulatory framework in many LDCs and even some developing countries remains underdeveloped. For instance, 40 per cent of LDCs have no laws on data protection and 26 per cent of LDCs have no law on cybercrime.[130] The lack of a robust domestic framework for data can adversely affect the ability of many of these countries to negotiate provisions on data flows in PTAs.[131] The Friends of Ecommerce for Development (FED) also identified legal uncertainty in data regulatory frameworks as a key constraining factor for developing countries to take advantage of digital trade.[132] Therefore, it is important to create more robust institutional mechanisms to provide technical assistance/support to developing countries. In terms of viewing the evolution of such a model, Bacchus suggests that the best way to develop an inclusive, multilateral digital

[126] L Guglya and M Maciel, 'Addressing the Digital Divide in the Joint Statement Initiative on E-Commerce' (IISD, 30 December 2020) 57.

[127] DEPA, Art 9.5; UKSDEA, Art 8.61H.

[128] DEPA, Art 9.4.3; UKSDEA, Art 8.61I.

[129] GSMA, 'Proposal for TELSOM/ATRC: Advancing the ASEAN–GSMA Policy Dialogue on Cross Border Data Flows' (November 2019) www.gsma.com/asia-pacific/wp-content/uploads/2019/11/ASEAN-Sandbox-Proposal-EXTERNAL-_Final_20190403.pdf.

[130] Guglya and Maciel (n 126) 8.

[131] A Beyleveld and F Sucker, 'Cross-Border Data Flows in Africa: Policy Considerations for the AfCFTA Protocol on Digital Trade' (Mandela Institute, 21 October 2022) 56 (in the context of digital laws in several African countries).

[132] UNCTAD, 'Friends of e-Commerce for Development Launch Roadmap for International Trade and Development Policy' (04 May 2017) www.unctad.org/news/friends-e-commerce-development-launch-roadmap-international-trade-and-development-policy. See also the presentations at the workshop by the FED in 2016: WTO, 'Seminar on eCommerce for Development' (9 December 2016) www.wto.org/english/tratop_e/ecom_e/ecomdevel_e.htm.

trade regime is to gradually move from asymmetric arrangements (where developed countries bear more obligations and developing countries receive more support) to a symmetric one (where more developing countries can build themselves up and carry out a wider range of obligations contained in digital trade agreements).[133]

The existing committees under the WTO and new digital trade committees instituted under PTAs can become sites for designing and operationalising technical assistance programmes. The Trade Facilitation Agreement Facility, instituted in 2014, provides a helpful prototype in that regard.[134] In the ongoing joint initiative negotiations on e-commerce at the WTO, the co-conveners and Switzerland jointly set up an E-Commerce Capacity Building Framework to provide technical assistance to developing countries and enable them to take advantage of digital trade opportunities.[135] Other initiatives to provide support to developing countries in digital trade include the Aid for Trade,[136] the Data Innovation Fund[137] and the Enhanced Integrated Framework.[138] In addition to operationalising technical-assistance and capacity-building programmes, the above institutional mechanisms can be important sites for fostering and coordinating data regulatory cooperation, as discussed below.

Fourth, in terms of developing the right regulatory frameworks for bridging the global data divide, it will be crucial for trade bodies to align with other multistakeholder and transnational bodies working on different aspects of global data governance in order to create a multilayered model of global digital cooperation. For instance, several global initiatives are focused on developing tools to enable data sharing for development and meaningful research activities.[139] Certain bodies are also developing basic principles for data ethics sharing and creating more equitable opportunities for benefiting from data in various sectors.[140]

[133] J Bacchus, 'The Digital Decide – How to Agree on WTO Rules for Digital Trade' (CIGI, 2021) 16.

[134] WTO-TFA, 'The Facility', www.tfafacility.org/facility.

[135] WTO, 'E-Commerce JSI Co-convenors Announce Capacity-building Support', www.wto.org/english/tratop_e/ecom_e/jiecomcapbuild_e.htm.

[136] USTR, 'Aid for Trade', www.ustr.gov/issue-areas/trade-development/trade-capacity-building/aid-trade.

[137] World Bank, 'Data Innovation Fund (DIF)', www.worldbank.org/en/data/statistical-capacity-building/data-innovation-fund.

[138] Enhanced Integrated Framework, 'Who We Are', www.enhancedif.org/en/who-we-are.

[139] See, eg 'Data2x', www.data2x.org/; 'Global Partnership for Sustainable Development Data', www.data4sdgs.org; 'Data for Good', www.dataforgood.facebook.com/; 'Digital Impact Alliance', www.dial.global/about-the-digital-impact-alliance/.

[140] See, eg UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' (UNESCO's 41st General Conference, Paris, 9–24 November 2021); WHO, 'Sharing and Reuse of Health-Related Data for Research Purposes: WHO Policy and Implementation Guidance' (2022); 'Malta Urges the UN to Consider the Internet as Common Heritage of Mankind' (*Times of Malta*, 21 December 2015) www.timesofmalta.com/articles/view/malta-urges-the-un-to-consider-the-internet-as-common-heritage-of.596497; 'UN Global Pulse', www.unglobalpulse.org; M Wilkinson et al, 'The FAIR Guiding Principles for Scientific Data Management and Stewardship' (2016) 3(160018) *Scientific Data*.

It is possible to incorporate some of these principles by reference at least in some of the progressive PTAs and DEAs, thus providing a foundation for sound data governance in digital trade transactions. Certain concessions can also be made to LDCs and developing countries on a pragmatic basis; for instance, instead of having a cross-cutting adequacy requirement in data protection laws, adequacy findings could be made on a sector-specific basis.[141]

More robust provisions on digital inclusion (as discussed previously in section IIIB) can also contribute to reducing the global data divide and breaking regulatory silos. Such provisions can be tied with other development-focused initiatives at the WTO and other multilateral bodies. In particular, digital inclusion programmes must be developed based on evidence-based policy-making. The UKSDEA already provides examples, such as sharing of datasets relating to disadvantaged groups such as women.[142] Regional collaboration can also be instrumental, especially for developing countries and LDCs that may not have a sufficient voice individually to contribute to the relevant dialogues.[143] With respect to standard setting in the digital services sector, existing proposals have already highlighted the value of adopting a Code of Good Practice like the Technical Barriers to Trade, which emphasises the importance of representativeness and transparency in technical standard-setting procedures.[144]

The most important aspect of introducing meaningful reforms in international trade law, whether at the WTO or regional bodies, is getting the narrative right. As discussed throughout this chapter, developing countries have genuine concerns regarding data colonialism and loss of policy autonomy. Addressing these concerns necessitates contextualising structures of regulatory cooperation and technical assistance to protect the interests of developing countries in terms of both substantive rules and procedural/institutional mechanisms. Therefore, this chapter recommends a contingent and streamlined approach to SDT and regulatory cooperation to foster more trust among developed and developing countries.

Further, in developing the narrative, trade policy-makers must emphasise the benefits of an interconnected and secure Internet for all countries, including increased opportunities to engage in cross-border trade in services, especially with appropriate regulatory and policy interventions.[145] Trade policy-makers

[141] M Pisa and U Nwankwo, 'Do Evolving Digital Trade Rules Create an Uneven Playing Field? Understanding Global Perspectives' (CGDev, August 2021) www.cgdev.org/sites/default/files/do-evolving-digital-trade-rules-create-uneven-playing-field-understanding-global.pdf.

[142] UKSDEA, Art 8.61P(2).

[143] In the context of the African Union, see N Mishra and K Kugler, 'The Emergence of an International Community in the Global Digital Economy' (AFIELN Conference Paper, unpublished, draft on file with the author).

[144] See ch 7.

[145] OECD, *ICTs for Development – Improving Policy Coherence* (2009) 75–77, 83. An example of such provisions can be found in the UKSDEA, Arts 8.38.1, 8.38.2.

must not rush to find quick-fix solutions to the global data divide by forcing developing countries and especially LDCs to rapidly agree to obligations on developing domestic data regulatory frameworks for cross-border data flows. Instead, the proposed reforms are more likely to be sustainable if they are carefully measured, progressive and implemented in a pragmatic manner to provide sufficient scope for streamlining their implementation.[146]

On a conclusive note, creating the right incentives for developing countries to participate in the digital economy through reforms in international trade law should not be viewed as charity from the developed world. Instead, it is a shared interest (with differentiated responsibilities), especially given that the fastest expanding digital markets are now in the developing world.[147] By incorporating the above-suggested reforms in international trade law so as to make it more inclusive and balanced, cross-border data flows in the global digital economy will benefit a larger number of countries and therefore create long-term economic benefits for more people.

V. CONCLUSION

The discussion in this chapter suggested that addressing the global data divide needs a coherent, international response and a set of shared norms and a robust global cooperation model, instead of inward-looking data-restrictive measures. At the same time, this chapter found that several developing countries and the majority of LDCs do not enjoy sufficient policy autonomy to independently chart their path for the development of their domestic data economy, especially without any coercion or unwanted interference from the digitally developed countries. Therefore, international trade law faces an almost unsurmountable challenge in dealing with the global data divide.

This chapter found that existing provisions in WTO law and PTAs are inadequate in addressing several dimensions of the global data divide. In particular, the lack of streamlined provisions on SDT in relation to digital trade, the lack of meaningful mechanisms for technology transfer, and the legal uncertainties in the existing trade rules pose several concerns for developing countries. The chapter therefore proposed the development of a new framework to address the global data divide, wherein developing countries are provided with tailored technical assistance and capacity-building support by developed countries based on their self-identified needs regarding the development of their domestic data

[146] A similar moderated approach was suggested in Beyleveld and Sucker (n 131) 58–60. For a discussion on the adoption of such a pragmatic approach in ASEAN, see Mishra and Valencia (n 89).

[147] N Hawcock, 'FT-Omdia Digital Economies Index: Tomorrow's Top Tech Growth Markets' (*Financial Times*, 22 November 2022) www.ft.com/content/eb373c95-eace-4a9c-9b45-9ace63ae12d5.

regulatory frameworks. In return, developing countries would agree to gradually liberalise cross-border data flows across various digital sectors. Further, the chapter suggested the importance of building new models of digital cooperation contextualised to the needs of developing countries and based on shared goals and interests. It also suggested various flexibilities for LDCs as they face the toughest challenges in making the digital transition.

6

Reconciling International Trade Law and Competition in the Data-Driven Economy

I. INTRODUCTION

The last chapter discussed how the unprecedented growth of powerful digital technology companies in some digitally advanced countries was a key driver of the global data divide. However, in addition to these development-related concerns, the unprecedented growth of Big Tech is also a challenge more broadly for competition law and policy. To provide some context: in 2022, Apple had a market capitalisation of 2.2 trillion USD, Microsoft 1.8 trillion USD and Alphabet (Google's parent company) 1.2 trillion USD.[1] Further, technology companies such as Apple, Amazon and Microsoft are amongst the biggest companies in the world in terms of their revenue.[2] The most critical factor driving the business model of these technology companies is the unhindered access to vast hordes of data collected from their users.

As this chapter demonstrates, the 'data advantage' or 'informational advantage' enjoyed by Big Tech companies impacts competitive dynamics across markets globally.[3] Further, this market asymmetry raises deep concerns in global data governance such as safeguarding vital public/national interests as well as ensuring equitable access to and use of data. Data is critical to several aspects of the digital supply chain and innovation, including the development and customisation of new services, including artificial intelligence

[1] Statista, 'Leading Tech Companies Worldwide 2022, by Market Capitalization', www.statista.com/statistics/1350976/leading-tech-companies-worldwide-by-market-cap/.

[2] Statista, 'The 100 Largest Companies in the World Ranked by Revenue in 2022', www.statista.com/statistics/263265/top-companies-in-the-world-by-revenue/.

[3] F Jenny, 'Competition Law and Digital Ecosystems: Learning to Walk Before We Run' (2021) 30(5) *Industrial and Corporate Change* 1143; A Andreoni and S Roberts, 'Governing Data and Digital Platforms in Middle Income Countries: Regulations, Competition and Industrial Policies, with Sectoral Case Studies from South Africa', Digital Pathways Paper Series (Oxford University, November 2020) 22; OECD, *Handbook on Competition Policy in the Digital Age* (2022) 18, www.oecd.org/daf/competition/oecd-handbook-on-competition-policy-in-the-digital-age.pdf.

(AI)-driven services. Therefore, Big Tech companies such as providers of key digital platforms and social media services collecting large amounts of data (often pejoratively termed 'data monopolies' or 'data-opolies'),[4] enjoy excessive amounts of economic and (arguably) political power.[5]

The growth of data-driven Big Tech companies has been both promising and dangerous at the same time. Data accumulation has, on the one hand, enabled technology companies to innovate, develop new services at a breakneck speed and capitalise on the network economies of scale,[6] and thus increase opportunities for global digital trade. On the other hand, the growth of data monopolies has made digital trade markets far less competitive, especially for new entrants and small-sized players, as they struggle to match the offerings of technology giants enjoying disproportionate advantage due to the tipping effect (resulting in creation of near monopolies) in data-driven markets.[7]

Governments face various policy dilemmas, especially as Big Tech companies now make enormous profits[8] and severely stifle the growth of indigenous technology companies in the domestic market.[9] Further, traditional tools in competition law are increasingly under strain in capturing anti-competitive practices in data-driven markets.[10] Consequently, governments have resorted to a range of new measures to increase opportunities for domestic players, including data-restrictive measures, such as data localisation,[11] and new tools to facilitate fairer competition, such as increased scrutiny of anti-competitive conduct in digital markets and requirements for data portability, interoperability and mandatory data sharing.[12]

[4] See generally ME Stucke, 'Should We Be Concerned about Data-opolies?' (2018) 2(2) *Georgetown Law Technology Review* 275.

[5] See generally T Wu, *The Curse of Bigness: Antitrust in the New Gilded Age* (New York, Columbia Global Reports, 2018).

[6] M Wessel, 'How Big Data Is Changing Disruptive Innovation' (HBR, 27 January 2016) www.hbr.org/2016/01/how-big-data-is-changing-disruptive-innovation; A McAfee and E Brynjolfsson, 'Big Data: The Management Revolution' (HBR, October 2012) www.hbr.org/2012/10/big-data-the-management-revolution; OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being* (2015).

[7] See s IIIA.

[8] World Bank, *World Development Report 2021: Data for Better Lives* (2021) 227–28. See also AM Chowdhary and SB Diasso, 'Taxing Big Tech: Policy Options for Developing Countries' (South Centre, 21 December 2022) www.southcentre.int/wp-content/uploads/2022/12/TCPB27_Taxing-Big-Tech-Policy-Options-for-Developing-Countries_EN.pdf. Potentially this also has tax implications.

[9] D Brown, 'Big Tech's Heavy Hand Around the Globe' (Human Rights Watch, 8 September 2020) www.hrw.org/news/2020/09/08/big-techs-heavy-hand-around-globe.

[10] See s III.

[11] Andreoni and Roberts (n 3) 2–3.

[12] While this chapter briefly discusses competition law relating to data monopolisation to provide context to the readers, it does not evaluate competition law norms, but rather focuses on the interface between digital trade and competition law. For more discussion, see OECD, *Handbook on Competition Policy* (n 3); ME Stucke, *Breaking Away: How to Regain Control Over Our Data, Privacy, and Autonomy* (New York, Oxford University Press, 2022).

This chapter studies the nexus of competition law and international trade law to understand two interlinked questions. The first of these is whether trade law and competition law can be consistent with each other in the context of the digital economy. Competition law and international trade law have both become dramatically important with the digitalisation of the economy. At the same time, this chapter identifies potential dilemmas between domestic competition regulation in the digital sector and enabling data flows. To contextualise this complex interplay, the first part of the chapter follows a different structure from the previous chapters to provide the readers with some context regarding the difficult relationship of trade law and competition law (section II), and also explains the competition dynamics unique to digital markets (section III). Next, in line with previous chapters, the second question that this chapter investigates is whether international trade agreements can play a contributory role in the development of competition principles necessary to enable cross-border data flows (section IV).

As sections III and IV explain in further detail, existing disciplines on competition in trade agreements neither factor in interlinkages between digital trade and competition regulation in the digital sector nor provide many answers when competition-related measures conflict with trade rules. This has become problematic especially with the growth of massive data monopolies based in a few developed countries, leading to a trust deficit in global data governance and prompting governments to impose various kinds of data-restrictive and stringent measures to address this market asymmetry and create fairer opportunities for their domestic technology companies.

International trade agreements have played a limited role in regulating competition issues to date. There has been a gradual shift in this perception in recent years. For instance, new-generation preferential trade agreements (PTAs) and digital economy agreements (DEAs) have the potential to facilitate bottom-up convergence on high-level principles to foster fairer competition in data-driven markets and thereby contribute to a multilayered framework for cross-border data governance. This approach appears more feasible than diffusing competition rules through the top-down framework of WTO, where establishing the relationship between competition law and trade law has historically been problematic. Therefore, this chapter proposes that PTAs and DEAs must incorporate provisions referring to the relevant norms developed by transnational regulatory networks such as the International Competition Network (ICN). It also argues that regional bodies such as the African Union, the Association of Southeast Asian Nations (ASEAN) and the Organisation for Economic Co-operation and Development (OECD) can be instrumental in developing a long-term consensus on competition principles necessary for enabling fair and equitable cross-border data flows. Eventually, we may see greater focus and even convergence on basic competition principles applicable to data-driven sectors in digital trade rules implemented at the World Trade Organization (WTO), but this may only be possible in the long run.

II. THE INTERSECTION OF INTERNATIONAL TRADE LAW AND COMPETITION LAW IN THE DATA-DRIVEN ECONOMY

A. Overlapping and Conflicting Objectives of Competition Law and International Trade Law

Scholars have long debated the interface between competition law and trade law. While the idea of market competition underlies both areas, they approach it from different perspectives. As competition law is a part of domestic law, it focuses on competition within the domestic market. In contrast, international trade law focuses on competition across markets as it is a part of the multilateral/plurilateral legal framework.[13] Therefore, while both disciplines focus on market access barriers, the former is focused only on those in the domestic market, while the latter takes into account barriers faced by foreign companies.[14] This has provoked some scholars to argue that merging competition law and trade law disciplines is like 'forcing the square peg of competition policy into the round hole of trade policy'.[15]

With the integration of markets and the development of global (or regional) supply chains, international trade and competition law are, however, not isolated from each other.[16] For instance, a country can selectively enforce competition law to either protect domestic players or discriminate against foreign players despite making commitments to open their domestic markets to foreign competition in various trade treaties.[17] Further, weak enforcement of competition law in certain countries (particularly those with large markets) may result in anti-competitive conduct affecting competition in foreign markets.[18] For instance, with globalisation, cartels can operate internationally, or certain companies can now enjoy

[13] See generally SW Waller, 'Book Review: Mario Marques Mendes, Antitrust in a World of Interrelated Economies' (1991) 17(3) *Brooklyn Journal of International Law* 609.

[14] B Sweeney, 'Globalisation of Competition Law and Policy: Some Aspects of the Interface Between Trade and Competition' (2004) 5(2) *Melbourne Journal of International Law* 375, 377.

[15] D Tarullo, 'Norms and Institutions in Global Competition Policy' (2000) 94(3) *American Journal of International Law* 478, 479.

[16] JS Lee, 'Towards a Development-Oriented Multilateral Framework on Competition Policy' (2006) 7 *San Diego International Law Journal* 293, 303; WTO, 'Synthesis Paper on the Relationship of Trade and Competition Policy to Development and Economic Growth' (18 September 1998) WTO Doc WT/WGTCP/W/80, 4; M Matsushita, 'Basic Principles of the WTO and the Role of Competition Policy' (2004) 3(2) *Washington University Global Studies Law Review* 363.

[17] See comments of Clair Wilcox (one of the principal architects of the International Trade Organization) in DP Wood, 'The Impossible Dream: Real International Antitrust' (1992) 1992(1) *University of Chicago Legal Forum* 277, 282–83; A Bradford, 'Antitrust Law in Global Markets' in E Elhauge (ed), *Research Handbook on the Economics of Antitrust Law* (Cheltenham, Edward Elgar, 2012) 295; PC Mavroidis and DJ Neven, 'Competition Enforcement, Trade and Global Governance: A Few Comments' in D Gerard and I Lianos (eds), *Reconciling Efficiency and Equity: A Global Challenge for Competition Policy* (Cambridge, Cambridge University Press, 2019) 408–09; B Ikejiaku and C Dayao, 'Competition Law as an Instrument of Protectionist Policy: Comparative Analysis of the EU and the US' (2021) 36(1) *Utrecht Journal of International and European Law* 75.

[18] Mavroidis and Neven (n 17) 398.

monopoly power globally or across several countries.[19] Divergent competition law regimes across markets (eg with different merger notification thresholds or different legal standards for anti-competitive conduct) increase compliance costs and legal uncertainty for companies operating globally.[20] Certain scholars have even proposed that a global competition agreement may be necessary to address the tensions between competition and trade law in a global economy.[21]

B. International Trade and Competition Law under the Multilateral Framework

The inclusion of competition disciplines in multilateral treaties has historically been a fraught exercise. During the time of the formulation of the Havana Charter in 1948,[22] an entire chapter (Chapter V) was dedicated to competition law issues. The provisions were quite broad and covered a whole variety of issues. For instance, all members were required to take measures 'to prevent business practices affecting international trade that may restrain competition, limit access to markets, or foster monopolistic control or interfere with the objectives of economic welfare and growth'.[23] Several specific anti-competitive practices were identified in the Havana Charter, including price fixing, market sharing, output limitation and discrimination against specific companies.[24] The Havana Charter also provided for a complaint mechanism under the aegis of the International Trade Organization,[25] and identified sectors in which curbing restrictive business practices was particularly important in the context of international trade, such as telecommunications, transportation, insurance and banking services.[26]

As the USA ultimately did not support this initiative, Chapter V was not included in the General Agreement on Tariffs and Trade (GATT) framework.[27]

[19] Tarullo (n 15) 479.

[20] ibid 482; Bradford, 'Antitrust Law in Global Markets' (n 17) 283.

[21] See generally L Brittan and K Van Miert, 'Towards an International Framework of Competition Rules – Communication to the Council' (18 October 1996) Commission of the European Communities Doc No COM(96) 284; Tarullo (n 15) 478; E Fox, 'Toward World Antitrust and Market Access' (1997) 91 *American Journal of International Law* 1; A Guzman, 'Is International Antitrust Possible?' (1998) 73 *New York University Law Review* 1501; A Guzman, 'Antitrust and International Regulatory Federalism' (2001) 76 *New York University Law Review* 1142.

[22] The Havana Charter was an instrument initiated by the US and its allies in 1947 for the establishment of the International Trade Organization to deal with all matters of international trade and related economic matters. This Charter never came into force as it was not approved in the US Congress. However, a part of the Havana Charter took the form of the General Agreement on Tariffs and Trade.

[23] Final Act of the United Nations Conference on Trade and Employment (Havana, United Nations Document E/Conf 2/78, April 1948), Art 46(1) (Havana Charter).

[24] ibid Art 46(3).

[25] ibid Art 46(2).

[26] ibid Art 53.

[27] L Loevinger, 'Antitrust Law in the Modern World' (1962) 6(2) *International and Comparative Law Bulletin* 20, 21.

The UN Economic and Social Council made another unsuccessful attempt to implement a multilateral competition agreement in the 1950s,[28] while GATT members adopted a Decision in 1960 on Arrangements for Consultation of Restrictive Business Practices, recognising that anti-competitive conduct can harm world development but with no binding legal rules.[29]

After the institution of the WTO in 1995, several members broached the idea of including competition law issues within the framework of a WTO treaty. The WTO Working Group on the Interaction between Trade and Competition Policy was active from 1997 to 2003. In particular, the EU was supportive of a global competition framework under the WTO,[30] and proposed that such a framework should oblige all members to adopt fundamental rules on competition law (hard core cartels, abuse of dominance, etc), promote the principles of transparency and non-discrimination in competition law enforcement, and provide for regulatory cooperation between countries.[31] These ideas were supported by scholars who proposed that a competition law code at the WTO would prevent harmful anti-competitive conduct impeding market access[32] and deter regulators from enforcing competition laws in a manner that discriminates against foreign companies.[33]

The final attempt to integrate competition law into the WTO ended with the discontinuation of the Singapore Issues in 2003 from the Doha Negotiating Round, which included competition policy.[34] There were several reasons why WTO members were sceptical about developing competition rules under the aegis of the WTO, leading to removal of this topic from its agenda. For developing countries, the key concern was that the rich countries would use the competition agreement as a tool to discipline and control the development of successful domestic players in their countries and hinder any industrial policy initiatives.[35] Further, many developing countries were concerned about having the resources and expertise to implement a competition law regime.[36] On the other hand, certain developed countries, including the USA, were inclined to use bilateral cooperation measures for competition law instead of a binding WTO code.[37] Certain scholars have also argued that the adversarial nature of

[28] ibid 21.

[29] RD Anderson et al, 'Competition Policy, Trade and the Global Economy: An Overview of Existing WTO Elements, Commitments in Regional Trade Agreements, Some Current Challenges and Issues for Reflection' (31 October 2018) WTO Staff Working Paper ERSD-2018-12, 8.

[30] Tarullo (n 15) 478.

[31] WTO Working Group on Interaction Between Trade and Competition Policy, 'Communication from the European Community and Its Member States' (25 May 1999) WT/WGTCP/W/115.

[32] P Marsden, *A Competition Policy for the WTO* (London, Cameron May, 2003) 284.

[33] MJ Trebilcock and EM Iacobucci, 'National Treatment and Extraterritoriality: Defining the Domains of Trade and Antitrust Policy' in RA Epstein and MS Greve (eds), *Competition Laws in Conflict* (Washington DC, AEI, 2004) 154–7.

[34] Sweeney (n 14) 2.

[35] ibid 11.

[36] ibid 11.

[37] Tarullo (n 15) 478.

the WTO dispute settlement system was not suited to addressing transnational competition policy problems.[38]

C. Competition Disciplines in WTO Law

Various WTO treaties contain provisions related to competition law, including in the General Agreement on Trade in Services (GATS).[39] For instance, under Article VIII, any monopoly supplier of a service, during the supply of its monopoly service, should act consistently with the most-favoured nation obligation contained in Article II as well as other specific commitments, such as national treatment and market access. Additionally, Article IX of GATS provides for a consultation mechanism where 'certain business practices of a service supplier … may restrain competition and restrict trade in services'.

The relevance of these provisions was discussed in the Work Programme on Electronic Commerce in 1999: (i) e-commerce at that time was seen as providing more opportunities to smaller players and thereby reducing anti-competitive practices; and (ii) concerns were expressed that monopoly service providers might try to stifle e-commerce players by reducing their access to channels of distribution and the Internet.[40] As will be discussed later, these concerns have radically changed in the current economy, wherein certain e-commerce and technology companies have become disproportionately powerful and can in fact operate as monopoly providers of services.

Finally, the disciplines on non-discrimination set out in GATS and other trade treaties also automatically apply to any competition law measures that restrict trade.[41] As readers may recall from previous chapters, the legal test under the non-discrimination obligation entails ensuring that like services and like service providers can enjoy equal competitive opportunities.

The GATS Annex on Telecommunications contains disciplines affecting market entry in telecommunications such as regulation, licensing and certain aspects of network interconnection in general terms.[42] Several WTO members have also committed to the Reference Paper on Telecoms, setting out various competitive safeguards for basic telecoms services, including prevention of anti-competitive cross-subsidisation and anti-competitive conduct in the telecommunications sector, and facilitating a fair and competitive market for interconnectivity across various telecommunications networks.[43] In a dispute

[38] ibid 479; JO McGinnis and ML Movsesian, 'The World Trade Constitution' (2000) 114(2) *Harvard Law Review* 511.

[39] For discussions on relevant provisions in TRIPS, TRIMS and GPA, see Anderson et al (n 29) 15.

[40] WTO, 'Work Programme on Electronic Commerce' (27 July 1999) S/L/74, para 12–13.

[41] Mavroidis and Neven (n 17) 409.

[42] WTO Negotiating Group on Basic Telecommunications, 'Telecommunications Services: Reference Paper' (24 April 1996).

[43] ibid.

brought by the US government against certain Mexican regulations affecting international telecommunications services, the panel found that the Mexican regulations on access pricing were inconsistent with the Reference Paper.[44] Some scholars have contended that the GATS Annex and Reference Paper are relevant in the context of enabling cross-border data flows.[45]

D. Competition Disciplines in PTAs

The majority of PTAs also contain disciplines on competition, covering high-level disciplines on the adoption or maintenance of competition laws by signatories, and general provisions on international cooperation on competition policy. As of 2019, 80 per cent of the 296 FTAs notified to the WTO either have detailed chapters or provisions on competition or include less detailed provisions on competition.[46] These provisions usually address specific aspects of competition policy affecting cross-border trade.

Anderson et al have summarised the key competition-related provisions found in PTAs: (i) a general undertaking that the benefits of trade liberalisation guaranteed by the PTA are not undermined by anti-competitive conduct; (ii) recognition that the general objectives of competition policy are economic efficiency and consumer welfare, or related objectives of economic development (although the language can vary substantially across PTAs); and (iii) provisions on transparency, non-discrimination and procedural fairness in the implementation of domestic competition law.[47]

This section briefly covers competition chapters in some recent PTAs – the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the United Kingdom–New Zealand Free Trade Agreement (UK–NZ FTA),[48] the Agreement between the United States of America, the United Mexican States, and Canada (USMCA)[49] and the Regional Comprehensive Economic Partnership (RCEP)[50] – and contrasts these PTAs with general trends in the EU's PTAs. While competition chapters are increasingly longer, they are still quite weak. For instance, most PTAs lack a binding dispute settlement mechanism for the competition chapter. Certain common disciplines on transparency, procedural fairness and cooperation can be found across many of these chapters.

[44] *Mexico – Measures Affecting Telecommunications Services*, Panel Report (adopted 1 April 2004) WT/DS204/R.

[45] See LL Tuthill, 'Cross-border Data Flows: What Role for Trade Rules?' in P Sauvé and M Roy (eds), *Research Handbook on Trade in Services* (Cheltenham, Edward Elgar, 2016) 357–80.

[46] Anderson et al (n 29) 20.

[47] ibid 22.

[48] United Kingdom–New Zealand Free Trade Agreement (London, 2022) (UK–NZ FTA).

[49] Agreement between the United States of America, the United Mexican States, and Canada (Mexico City, 10 December 2019) (USMCA).

[50] Regional Comprehensive Economic Partnership (Hanoi, 15 November 2020), Art 13.2(a) (RCEP).

The CPTPP contains one of the most comprehensive chapters on competition policy amongst recent PTAs. It requires all parties 'to adopt or maintain national competition laws that proscribe anticompetitive business conduct', but clearly links this to the twin objectives of 'promoting economic efficiency and consumer welfare'.[51] It also makes a specific reference to the APEC (Asia-Pacific Economic Cooperation) Principles to Enhance Competition and Regulatory Reform.[52] It contains comprehensive provisions on procedural fairness and transparency, inspired from the work of the ICN and the OECD.[53] It also introduces the requirement for parties to maintain laws or other measures that provide a private right of action for competition law issues.[54]

The CPTPP contains two provisions on cooperation on competition issues: a general provision (common to most PTAs)[55] and another focused on technical cooperation, such as providing capacity-building support or technical assistance to parties (which is rarer in PTAs).[56] The CPTPP competition chapter draws a connection between competition policy and consumer protection, explicitly requiring each party to maintain domestic laws to proscribe fraudulent and deceptive commercial activities.[57] Any concern arising under the competition chapter is only subject to consultation between parties; binding dispute settlement is unavailable.[58]

Like the CPTPP, the UK–NZ FTA draws a clear connection between competition and trade law by stating that the promotion of 'economic efficiency and consumer welfare' and the 'maintenance and enforcement' of competition law will help 'bilateral trade and investment between the Parties'.[59] Each party is under an obligation to maintain competition laws that apply to 'all commercial activities in its territory regardless of an enterprise's nationality or ownership'.[60] Similarly, there are detailed requirements for parties to ensure procedural fairness and transparency in the enforcement of competition law.[61] This treaty also requires parties to 'maintain laws or other measures that provide a private right of action, both independently and following a finding of violation by a national competition authority'.[62] Further, as is common to most FTAs, this treaty contains a provision on cooperation between regulators, with some

[51] Comprehensive and Progressive Agreement for Trans-Pacific Partnership (Santiago, 2018), Art 16.1.1 (CPTPP).
[52] CPTPP, Art 16.1.1.
[53] ibid Arts 16.2, 16.7.
[54] ibid Art 16.3. This provision was specific to the US legal system as the USA was initially a party to the negotiations.
[55] ibid Art 16.4.
[56] ibid Art 16.5.
[57] ibid Art 16.6.
[58] ibid Arts 16.7, 16.8.
[59] UK–NZ FTA, Art 18.1.
[60] ibid Art 18.2.2.
[61] ibid Arts 18.3, 18.6.
[62] ibid Art 18.4.2.

provisions specifically focusing on information sharing in relation to competition issues in digital markets.[63] Any disputes pertaining to this chapter can also only be resolved by consultation between parties.[64]

The USMCA contains a reasonably detailed chapter on competition policy. The chapter sets out the requirement for each party to adopt and implement competition laws that would apply to all commercial activities within this territory.[65] Further, it sets out a clear non-discrimination provision, requiring that the competition regulator must treat 'persons of another Party no less favorably than persons of the Party in like circumstances'.[66] Similarly, the chapter provides that all parties must adopt transparent and fair practices and follow due process in competition law investigations and enforcement.[67] The chapter clearly sets out the basis for voluntary cooperation among competition regulators of the parties and also acknowledges other networks, such as the ICN and OECD.[68] Similar to the CPTPP, the USMCA links competition policy and consumer protection, referring to the requirement that each party maintain domestic laws to proscribe fraudulent and deceptive commercial activities.[69] Finally, as is typical of competition chapters in PTAs, any disputes pertaining to competition can be resolved only by consultation.[70]

Although the RCEP competition chapter contains provisions in several areas common to other PTAs discussed above, the language used is considerably different. For instance, while recognising the overarching goals of economic efficiency and consumer welfare, and their link with trade and investment, the chapter clearly acknowledges 'the sovereign rights of each Party to develop, set, administer, and enforce its competition laws, regulations, and policies'[71] and the variation across members in relation to the 'capacity and level of development in the area of competition law and policy'.[72] The RCEP provides a basic framework requiring all parties to adopt a law to deal with anti-competitive practices and to ensure basic levels of transparency and fairness.[73] However, there is no specific requirement for non-discriminatory treatment of foreign companies. It also contains a high-level provision on cooperation on competition law, including 'notification by a Party to another Party of its competition law enforcement activities that it considers may substantially affect the important interests of the other Party'.[74] There is a detailed provision on technical

[63] ibid Art 18.4.5.
[64] ibid Art 18.7.
[65] USMCA, Arts 21.1.1, 21.1.2.
[66] ibid Art 21.1.5(a).
[67] ibid Arts 21.2, 21.5.
[68] ibid Art 21.3.
[69] ibid Art 21.4.
[70] ibid Arts 21.6, 21.7.
[71] RCEP, Art 13.2(a).
[72] ibid Art 13.2(b).
[73] ibid Art 13.3.
[74] ibid Art 13.4.

cooperation and capacity building in the RCEP,[75] and a provision on linking consumer protection and competition law, similar to the CPTPP and USMCA.[76] As with most PTAs, any matters in relation to this chapter are only subject to consultation between parties.[77]

The above agreements can be contrasted with EU PTAs, which are generally much more detailed on competition policy. While the EU has proactively negotiated several PTAs with comprehensive competition chapters (modelled around EU competition law),[78] the USA and its allies prefer competition chapters mostly focused on international cooperation.[79] An interesting example is the competition chapter in the EU–Korea FTA,[80] which led to significant convergence between EU and Korean competition law.[81] The core principles of this treaty set out that 'benefits of the trade liberalisation process in goods, services and establishment' should not be 'removed or eliminated by anti-competitive business conduct or anti-competitive transactions'.[82] Further, this treaty requires parties to maintain 'comprehensive competition laws which effectively address restrictive agreements, concerted practices and abuse of dominance by one or more enterprises, and which provide effective control of concentrations between enterprises'.[83] The treaty also contains specific provisions on state monopolies[84] and public enterprises entrusted with special rights.[85] Nonetheless, competition chapters in most EU PTAs are also not subject to dispute settlement and all relevant matters can be addressed by consultation between parties.[86]

As can be seen above, competition disciplines are not uncommon in international trade agreements, despite the difficult relationship between competition and trade law. Some PTAs contain reasonably detailed provisions on cooperation in competition matters and also create opportunities for some degree of regulatory convergence, especially by borrowing principles from the ICN and OECD. The EU has been pushing several of its trading partners to adopt a competition law framework analogous to the EU through its PTAs – what Bradford characterises as the 'Brussels Effect'.[87] Notably, none of these PTAs are specifically focused on competition in digital sectors. With the

[75] ibid Art 13.6.
[76] ibid Art 13.7.
[77] ibid Arts 13.8, 13.9.
[78] Mavroidis and Neven (n 17) 408.
[79] Anderson et al (n 29) 23–24.
[80] European Union–South Korea Free Trade Agreement (Brussels, 06 October 2010) (EU–Korea FTA).
[81] A Bradford, *The Brussels Effect: How the European Union Rules the World* (New York, Oxford University Press, 2020) 121.
[82] EU–Korea FTA, Art 11.1.1.
[83] ibid Art 11.1.2 (footnote omitted). See further Art 11.1.3.
[84] ibid Art 11.5.
[85] ibid Art 11.4.
[86] ibid Arts 11.7 and 11–8.
[87] Bradford, *The Brussels Effect* (n 81).

evolving role of competition law in the digital economy and its strong linkages with global digital trade (as briefly set out in section I), the remaining chapter seeks to understand how competition law is specifically relevant to digital trade and cross-border data flows, and the role of trade law in addressing this interface.

III. COMPETITION LAW, DIGITAL TRADE AND CROSS-BORDER DATA FLOWS

Governments across the world are developing or deliberating upon competition rules for addressing disproportionate levels of market concentration in digital/data-driven sectors.[88] For instance, the European Commission has proposed refining existing concepts and methodologies for competition law assessment in the digital sector.[89] In the EU, the Digital Markets Act, 2022 (DMA), which came into force in May 2023, sets out various obligations and prohibitions on providers of core platform services referred as 'gatekeepers'.[90] Similarly, in the UK, the expert panel for the digital economy identified various competition law concerns arising due to the widespread prevalence of anti-competitive mergers and acquisitions in the digital markets and the consumer harms resulting from the winner-takes-all nature of digital markets.[91] In the USA, the US House of Representatives proposed several radical reforms to strengthen the enforcement of antitrust laws in the digital sector, including structural remedies to prevent digital platform providers offering e-commerce services that compete with their downstream operators and the acquisition of innovative digital start-ups by Big Tech companies.[92] While these interventions relate to different objectives, a common factor that these competition regulators appear concerned about is how Big Tech companies control and process data, with whom such data is shared, and how that influences competitive dynamics in both the domestic and global market.

A. Competition Characteristics of Digital Markets

To dive deeper into the interface between competition law and digital trade, it is first important to understand some unique competition characteristics of

[88] Jenny (n 3).

[89] J Cremer et al, *Competition Policy for the Digital Era* (European Commission, 2019).

[90] For designation of gatekeepers, see Regulation (EU) 2022/1925 of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1, Art 3 (DMA).

[91] Digital Competition Expert Panel, *Unlocking Digital Competition* (March 2019).

[92] Subcommittee on Antitrust, Commercial and Administrative Law of the Committee of the Judiciary, *Investigation of Competition in Digital Markets* (2020).

digital markets that are driven by data. Companies that offer digital platform services bring together several groups of users to interact on a single platform/ecosystem, thereby reducing several efficiencies and transaction costs for different market participants. Such markets are termed 'multi-sided markets', implying that, unlike the majority of traditional markets (where there is a buyer and seller),[93] there are several interested parties in these markets.[94] For instance, Amazon marketplace brings together sellers and buyers on two different sides of the markets, and the Google search engine or Meta brings together advertisers, content generators and ordinary users on different sides of the market.[95]

Competition operates differently in multi-sided markets as service providers leverage costs across different markets. For instance, although the Google search engine does not charge a fee from ordinary users, it can charge fees from advertisers/content generators and leverage this for its free search services. Further, as users increase on one side of the platform (eg more users use the Google search engine), the demand also increases on other sides of the platform (eg for advertising services), thus resulting in strong network effects (and also increasing the volume of data accessible to Google).[96] Further, dominant digital service providers can easily enter adjacent markets.[97] Consequently, we find that in many digital markets, such as platform services, one company (or very few companies) takes up the majority of the market share.[98] Such markets are therefore highly concentrated and susceptible to becoming uncompetitive. This, in turn, can harm consumers due to increasing costs of services or of switching digital services/platforms, as well as reducing innovation over time.[99]

The preceding views are, however, not incontrovertible. For instance, some experts have suggested that although first movers enjoy advantages in digital markets (for example, a huge user base and access to their data), this is not always sufficient to maintain market dominance.[100] Several factors contribute to the success of digital ecosystems in addition to economies of scale and data advantages. For instance, customers may have different needs or late entrants might be able to evolve faster to adjust to customer needs, and first movers sometimes simply 'get it wrong'.[101] Further, competition between different market players

[93] While multi-sided markets exist in offline markets as well (for example, the newspaper market brings together readers and advertisers), they are highly common in digital markets.

[94] S Wismer and A Rasek, 'Market Definition in Multi-sided Markets' (15 November 2017) OECD DAF/COMP/WD(2017)33/FINAL.

[95] J Veisdal, 'The Dynamics of Entry for Digital Platforms in Two-Sided Markets: A Multi-Case Study' (2020) 30 *Electronic Markets* 539.

[96] H Shelanski et al, 'Network Effects and Efficiencies in Multisided Markets' (15 November 2017) OECD DAF/COMP/WD(2017)40.

[97] A Portuese, 'The Digital Markets Act: European Precautionary Antitrust' (ITIF, May 2021) 47.

[98] Digital Competition Expert Panel (n 91) 4.

[99] ibid 32.

[100] Jenny (n 3).

[101] M Jacobides et al, 'What Does a Successful Digital Ecosystem Look Like?' (BCG, 26 June 2019) www.bcg.com/publications/2019/what-does-successful-digital-ecosystem-look-like.

is murkier due to rapidly changing consumption patterns in digital markets. For instance, a social media platform or search engine may soon compete with a mobile photo app or an AI-driven chatbot within just a few years.

Companies operating in digital markets primarily derive their competitive advantage from their capability to obtain and use data from their users in real time.[102] For instance, they have vast capacities to collect and store data about how their users interact and engage with their products and services, and then analyse this data to generate or customise their offerings.[103] Users are generally unaware of how firms collect and analyse their data, resulting in widespread information asymmetry in these markets. The ability to develop highly granular analysis of their user base enables these Big Tech companies to entrench their market position and capture new markets, making it harder for incumbents to break into new markets.

Further, because of their data resources, such companies can expand their digital ecosystems and encompass a new variety of customised services, making it harder for their users to switch to alternative providers. This is sometimes known as the data feedback loop, whereby companies that have access to data in real time can improve the quality of their products and thus have the incentive to keep collecting more data.[104] All in all, the data advantage enjoyed by Big Tech companies has resulted in altering the long-term competitive dynamics in digital markets. It is often difficult for competition regulators to understand these dynamics as most companies are not transparent regarding how they collect, analyse and process data.[105]

Traditional competition law tools have so far failed to address these concerns arising from the massive concentration of data in a few companies. Therefore, as argued below, some competition regulators have started developing ex ante regulations, including data portability and interoperability, requirements for data sharing, etc, which complement enforcement against anti-competitive conduct and thereby rebalance competitive dynamics in such data-driven markets.[106] There have also been repeated calls to reconsider prevailing competition law standards such as consumer welfare (which is based on the maximisation of economic efficiency) and competition law tools for analysing anti-competitive mergers and acquisitions. Currently, insufficient consensus exists regarding the effectiveness of these tools in regulating competition in digital markets.[107]

[102] Jenny (n 3).
[103] ibid.
[104] See generally M Farboodi et al, 'Big Data and Firm Dynamics' (2019) 109 *AEA Papers and Proceedings* 38; OECD, *Handbook on Competition Policy* 24; MS Gal and DL Rubinfeld, 'Data Standardization' (2019) 94(4) *NYU Law Review* 737, 758.
[105] F Pasquale, 'Privacy, Antitrust and Power' (2013) 20(4) *George Mason Law Review* 1009, 1024.
[106] World Bank (n 8) 230.
[107] D Ciuriak, 'The Data-Driven Economy Raises New Challenges for Global Governance' (CIGI, 03 October 2022) www.cigionline.org/articles/the-data-driven-economy-raises-new-challenges-for-global-governance/; Bradford, 'Antitrust Law in Global Markets' (n 17) 283.

B. Preventing Data Harms

As explained earlier, due to the access to vast hordes of data, Big Tech companies have (almost) unchecked capacity to manipulate the data of users to gain competitive advantage across different markets within their digital ecosystem. For instance, as Zuboff argues, several Big Tech companies have enormous ability to engage in continuous surveillance of their users by extracting excess amounts of data from the users' engagement with their digital services and apps and are thereby able to control and shape the users' choices.[108] One direct impact of such extensive data accumulation is the adverse effect on the privacy rights of individuals.[109] So far, competition law has been slow to accommodate data privacy considerations and most competition regulators still do not consider privacy as a non-price indicator of competition.[110] Further, privacy choices are not necessarily clear from consumer preferences, especially as the majority of consumers may not have much choice in terms of avoiding a dominant service such as the Google search engine.[111]

Competition law has also failed to prevent several Big Tech companies from acquiring small market players that have a low turnover but a fast-expanding user base (usually owing to some kind of new technological innovation).[112] One of the foremost examples cited in this regard is Facebook's acquisition of WhatsApp (wherein the European Commission failed to take into account the long-term adverse impact on the privacy of individuals resulting from the acquisition and the resulting exploitative behaviour by Facebook).[113] As a result of these acquisitions, some of the biggest technology companies have been able to build massive platforms or ecosystems that lock in users and thereby significantly enhance their competitive advantage by increasing their access to data of millions (and sometimes billions) of users.

The standard benchmarks used in merger analysis, particularly those focused on company turnover thresholds, have been ineffective in capturing the long-term anti-competitive effects of such transactions as the inherent value of data is often not captured in these benchmarks. Thus, competition regulators from across the world have started rethinking their examination of mergers and acquisitions in digital/data-driven sectors, including stricter scrutiny of conglomerate mergers in digital sectors and lowering thresholds

[108] See generally S Zuboff, *The Age of Surveillance Capitalism* (New York, Public Affairs, 2019).
[109] Stucke, 'Should We Be Concerned About Data-opolies?' (n 4).
[110] Ibid; Jenny (n 3).
[111] Pasquale (n 105) 1009–10.
[112] UNCTAD, *Competition and Consumer Protection Policies for Inclusive Development in the Digital Era* (2021) UNCTAD/DITC/CPLP/2021/2, 4.
[113] Commission, 'Case M.7217 – Facebook/ WhatsApp: Commission Decision Pursuant to Article 6(1)(b) of Council Regulation No 139/20041' C(2014) 7239 final, 164. But see Case C-252/21 *Meta Platforms Inc v Bundeskartellamt* ECLI:EU:C:2023:537 [2023] para 62.

for pre-merger review.[114] For instance, an amendment was introduced into the Chinese competition law in 2022 that allows its regulator to take action against companies that 'exclude or limit competition by abusing data, algorithms, technology, capital advantages as well as platform rules'.[115] Thereafter, Alibaba, one of the biggest technology companies in China and the world, announced it would break up into six different companies, thereby significantly reducing its market concentration levels in various digital markets.[116]

Digital markets also facilitate other forms of anti-competitive conduct. For instance, algorithmic collusion is an increasingly common concern in many digital markets, as companies turn towards AI-driven solutions to manage various business functions, including pricing.[117] Further, firms that enjoy market power due to data concentration can preclude smaller competitors from providing service providers with access to their platforms or data.[118] This has led several competition regulators to consider issues of anti-competitive exclusivity clauses and the tying or bundling of products in digital ecosystems.[119] As expected, regulators have become far more proactive in enforcing competition law in the digital sector; as of January 2020, 102 competition law cases across 12 different digital sectors had been finalised in both developed (predominantly EU) and developing countries (including India, South-East Asia and Latin America).[120]

C. Facilitating Data Equity

Both the access to and the capability to process data for consumer analytics are key to competing in the digital sector, particularly in AI-driven sectors, where access to massive hoards of training data is fundamental. As discussed earlier, some of the biggest technology companies in the world are also data monopolies that have unparalleled access to consumer/market analytics, making it almost impossible for small players to compete against them. Further, the largest technology companies capture data within their digital ecosystem and create

[114] M Stucke, 'The Relationship Between Privacy and Antitrust' (2022) 97(5) *Notre Dame Law Review Reflection* 400, 408; World Bank (n 8) 232; Platform Competition and Opportunity Act of 2021, HR 3826, 117th Cong (2021); Competition Authority of Kenya, 'Revised Guidelines on Relevant Market Definition' (2019).

[115] S Tabeta, 'China Completes Overhaul of Antitrust Law to Corral Big Tech' (Nikkei Asia, 25 June 2022) www.asia.nikkei.com/Business/China-tech/China-completes-overhaul-of-antitrust-law-to-corral-Big-Tech. See also AM Colino, 'The Case Against Alibaba in China and Its Wider Policy Repercussions' (2022) 10(1) *Journal of Antitrust Enforcement* 217.

[116] D Wakabayashi, 'Alibaba, China's E-Commerce Giant, Will Split Into 6 Units' (*New York Times*, 28 March 2023) www.nytimes.com/2023/03/28/business/alibaba-china-e-commerce.html.

[117] See generally OECD, 'Algorithms and Collusion: Competition Policy in the Digital Age' (2017).

[118] UNCTAD (n 112) 8–9.

[119] World Bank (n 8) 233.

[120] ibid 230.

'walled gardens'.[121] The value of data as a strategic asset has been recognised in a few competition law disputes outside of the digital sector. For instance, the French competition regulator had ordered GDF SUEZ to provide access to their customers' database (including meter number, annual consumption, name and surname of clients, billing address and telephone number) to their competing supplier.[122] However, this approach is usually premised on a particular database qualifying as an essential facility,[123] which entails a very rigorous legal test difficult to satisfy in digital markets.[124]

To address these limitations, some competition regulators have proposed new regulations to tackle data concentration. For instance, data portability and interoperability are often seen as potential solutions to data asymmetry in digital markets.[125] Data portability essentially means that, upon request, companies must provide a user with access to their digital data in a standard format so that they can easily transfer this data to other competing digital platforms or services.[126] An example is Article 20 of the General Data Protection Regulation (GDPR), which gives a right to data subjects to request that the data controller provide them with access to their own personal data in 'a structured, commonly used and machine-readable format', and further, where technically feasible, such data should be transferable from one data controller to another.[127] The DMA also contains specific requirements for gatekeepers to ensure data portability.[128] Another example of data portability is the institution of the Consumer Data Right in Australia (allowing users to access/correct their data and share it with nominated third parties).[129]

[121] A Froehlich, 'Walled Garden' (TechTarget, November 2021) www.TechTarget.com/searchsecurity/definition/walled-garden.

[122] OECD, 'Consumer Data Rights and Competition – Background Note' (5 June 2020) DAF/COMP/WD(2020)48, 7.

[123] Case T-201/04 *Microsoft Corp v Commission* ECLI:EU:T:2007:289, [2007] ECR II-3619.

[124] This would essentially require that any third party requesting access to the data (to operate in a related market) prove: (i) the data controlled by the dominant company is indispensable for the third party and cannot be replicated/gathered by any other means; (ii) there are no objective reasons why the dominant company in control of the database may refuse access to the data; and (iii) the refusal to grant access data would exclude all competition in the related market. These conditions are often hard to fulfil in digital markets. For instance, if an app service provider were to request access data from Google (a dominant provider of platform services such as Google Pay), then they might face various roadblocks: (i) the user data collected by Google can be collected/replicated by another company; (ii) Google might refuse access to the data for valid reasons, such as compliance with IP law or data protection law, or based on the inferior quality of a particular app; and (iii) there might be other app service providers who may be able to operate in the market even without access to data from Google. See UNCTAD (n 112) 61.

[125] See, eg Gal and Rubinfeld (n 104) 759.

[126] OECD, 'Data Portability, Interoperability and Competition', www.oecd.org/daf/competition/data-portability-interoperability-and-competition.htm.

[127] This right only applies to personal data processed pursuant to the consent of the data subject, in performance of a contract or where such data is processed by automated means.

[128] DMA, Art 6(9). A parallel example is the Access Act of 2021, HR 3849, 117th Cong, s 3 (2021).

[129] CB Wells, 'Platform Power and Privacy Protection: A Case for Policy Innovation' (2018) *CPI Antitrust Chronicle* 1.

Data interoperability is the 'capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units'.[130] In competition law, data interoperability is relevant because it can enable service providers to share data with each other in real time, thus allowing consumers to engage in multi-homing and combining functionalities across different digital platforms.[131] For instance, under the DMA, a gatekeeper must allow third parties to install applications or software that are interoperable with the operating system of the gatekeeper and must also remain accessible outside of this operating system.[132]

The enforcement of data portability and interoperability is expected to have two direct benefits. First, it will facilitate competition from new players in the digital platforms/applications market who may not have a similar level of access to data resources/holdings as established companies.[133] However, the repercussions could be different if the right to data portability also applied to non-dominant technology companies.[134] Second, it may increase the degree of control that the user has over their data, including allowing them to move it across platforms without being locked into a particular service provided by the dominant market player.[135]

Yet, some experts have questioned whether data portability is a judicious intervention for increasing competition in digital markets. For instance, it could disincentivise technology companies from accumulating data to offer more innovative services, thereby affecting the quality or efficiency of services.[136] It also increases the costs of compliance for service providers, especially non-dominant companies, as providing datasets in a format that is interoperable and reusable for other services can be quite complex and expensive.[137] Further, companies that transfer such data may be susceptible to further risks; for instance, the data transferred could prejudice the rights of other data subjects[138] and breach intellectual property law.[139] Finally, data portability mechanisms entail security

[130] Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' (5 April 2017) WP 242 rev.01, 14.

[131] OECD, 'Data Portability, Interoperability and Competition', www.oecd.org/daf/competition/data-portability-interoperability-and-competition.htm.

[132] DMA, Art 6(4).

[133] During the GDPR discussions, some states had mentioned that the right to data portability should be included in competition law rather than data protection law due to its competition rationale, see O Lynskey, 'Article 20. Right to Data Portability' in C Kuner et al (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford, Oxford University Press, 2020) 499; P Swire and Y Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72(2) *Maryland Law Review* 335, 338.

[134] Swire and Lagos (n 133) 339.

[135] See Lynskey (n 133) 499.

[136] Jenny (n 3); Swire and Lagos (n 133) 357–58.

[137] Swire and Lagos (n 133) 340.

[138] Lynskey (n 133) 504.

[139] Swire and Lagos (n 133) 348.

risks – for instance, if the data is intercepted while being transferred between controllers or if there is a fraudulent request for data portability.[140] A study conducted in 2019 found that data portability mechanisms offered by Facebook had limited success in promoting new players in the social media services market, although this study does not specifically discount the relevance of data portability for all other sectors.[141]

Another potential option is to create more policy consensus on creating common data spaces or pools.[142] It is expected that by preventing data silos within the ecosystems of Big Tech companies, data hoarding practices can be countered and more widespread competition can be induced in data-driven markets.[143] As an example, the DMA contains a provision that requires gatekeepers to provide any third party service providers of online search engines access to anonymised information on ranking, query, click and view data on fair, reasonable and non-discriminatory terms, in relation to both free and paid search.[144] While these options can potentially increase options for data sharing and reuse by a broader number of users, they may conflict with the principle of data minimisation contained in the privacy laws of many countries. Further, there may be potential security issues in such data-sharing models.[145]

Inequitable access to data is a sensitive concern for developing countries due to the yawning data divide, as discussed in chapter five. The majority of digital companies located outside of the USA and China, especially those in developing countries, struggle to offer credible competition to the big players. This is because these companies lack sufficient data resources/infrastructure to create competitive products and often rely on platform services provided by the Big Tech companies that serve as distribution channels for their products/services.[146] This problem is further complicated by the limited resources of competition regulators in developing countries, particularly to address the anti-competitive conduct of Big Tech companies based outside their jurisdiction.[147] Further, developing countries have traditionally been far more concentrated than developed economies in non-digital sectors, and this pattern may be replicated in digital markets. This may, however, lead to various harms, as discussed in the previous sections of this chapter. Finally, the majority of developing countries are currently dependent on several of the Big Tech platforms to ensure more

[140] Lynskey (n 133) 505.
[141] See generally G Nicholas and M Weinber, 'Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors' (Engelberg Center on Innovation Law and Policy, November 2019).
[142] O Borgogno and G Colangelo, 'Data Sharing and Interoperability: Fostering Innovation and Competition Through APIs' (2019) 35(5) *Computer Law & Security Review* 1, 3, 6.
[143] Stucke, 'The Relationship Between Privacy and Antitrust' (n 114) 411–12.
[144] DMA, Art 6(11).
[145] World Bank (n 8) 238–9.
[146] Portuese (n 97) 6.
[147] UNCTAD (n 112) 41–42.

digital inclusion in their country.[148] Therefore, unsurprisingly, developing countries have started viewing competition law as a tool of industrial policy to incentivise local digital firms to grow and stand up to competition from Big Tech companies.[149]

In a report published in 2021, the United Nations Conference on Trade and Development (UNCTAD) stated the importance of data portability and interoperability to reducing the market power of the technology behemoths and instead creating more open markets for innovative businesses.[150] Some scholars have in fact argued that before opening their local digital markets (for example, by agreeing to commitments in trade agreements to enable cross-border data flows for e-commerce), developing countries must first build their competition law framework.[151]

D. The Competition Law–Digital Trade Dilemma

The next question is why competition law matters for rules on digital trade and cross-border data flows. As can be inferred from the previous discussions, the enormous degree of global market concentration in data-driven sectors and the consequent geopolitical competition and inequalities between countries are key reasons for the trust deficit in cross-border data governance.

Competition law plays a critical role in addressing concerns such as preventing various forms of data harms and facilitating more equitable data markets. But at the same time, over-enforcement or selective enforcement of competition law against specific technology companies can adversely affect digital trade flows. Further, regulators are increasingly considering certain data-restrictive measures such as data localisation to boost domestic digital competition. Therefore, in the same way that we observed a dilemma at first sight between privacy and trade (chapter two) or cybersecurity and trade (chapter three), there is a potential dilemma between competition law and trade, as demonstrated by various examples below.

First, due to the rapid increase in data-manipulative practices by Big Tech companies, particularly the adverse impact on individual privacy and loss of user autonomy, various governments have resorted to data-restrictive measures, including restricting data flows to countries with lower levels of privacy protection and enhanced data protection compliance requirements for companies collecting and processing data. Cross-border privacy enforcement also remains particularly problematic, as the majority of these Big Tech companies are global

[148] ibid 51.
[149] ibid 54.
[150] ibid 54.
[151] A Beyleveld and F Sucker, 'Cross-Border Data Flows in Africa: Policy Considerations for the AFCFTA Protocol on Digital Trade' (CSEA, 21 October 2022) 70–74.

players but often do not have widespread presence across all markets. As an example, as of January 2023, Meta had 2.963 billion subscribers worldwide, with the majority of users located in developing countries,[152] but had operations in only 39 countries.[153] Similarly, Google controlled 93 per cent of the global market for search engines,[154] but with operations in only 50 countries.[155] Unsurprisingly, as discussed in chapters two and three, many governments have imposed data-restrictive measures to address various privacy risks and related consumer harms, but these measures may be in conflict with commitments in international trade agreements.[156]

Second, to address data asymmetry between Big Tech companies and smaller market players, competition regulators have resorted to new tools to enable fairer data sharing. For instance, as discussed in the previous subsection, many competition regulators have introduced measures to require data portability and interoperability for digital services. Certain countries are also considering introducing new requirements for digital platforms to share their data with other market players at reasonable prices and under reasonable terms and conditions, as seen in the case of the DMA. These mechanisms can have a lasting impact on cross-border data flows, especially as several of these companies have global operations.

Third, due to the data divide between developing and developed countries (see chapter five), governments – especially in the developing world – are increasingly looking towards measures to protect their domestic digital sector. For instance, creating fairer opportunities for the growth of domestic data-driven sectors is seen as one of the possible benefits of data localisation and related measures. It also seems likely that certain developing countries are likely to use competition law tools to boost industrial policy initiatives. Further, as certain digital platforms based in the USA and China become extraordinarily successful due to strategic technologies such as AI, several governments have expressed concerns about not only the impact on competition and related economic security concerns, but also the potential impact on national security.[157]

[152] S Kemp, 'Facebook Users, Stats, Data & Trends' (DataReportal, 11 May 2023) www.datareportal.com/essential-facebook-stats.

[153] D Irascu, '5 Stylish Facebook Offices Across the World' (Tech Behemoths, 20 June 2022) www.techbehemoths.com/blog/5-stylish-facebook-offices.

[154] StatCounter, 'Search Engine Market Share Worldwide', www.gs.statcounter.com/search-engine-market-share.

[155] Google, 'Our Offices', www.about.google/locations/?region=north-america&office=mountainview.

[156] Some stakeholders have even argued that trade rules on data flows could be weaponised to avoid competition laws within the country. See L Feiner, 'Democrats Warn Large Tech Firms Could Evade Competition Policies Under New Trade Rules' (CNBC, 24 April 2023) www.cnbc.com/2023/04/24/big-tech-firms-could-evade-competition-policies-under-new-trade-rules-dems-warn.html.

[157] See generally A Roberts et al, 'Toward a Geoeconomic Order in International Trade and Investment' (2019) 22(4) *Journal of International Economic Law* 655; H Sun and Peter Wat, 'Tech Wars and the Conflict of Public Interests' (2021) *5 Georgetown Law and Technology Review* 62.

Finally, competition law enforcement can also be a source of trade tension between countries, especially in the digital sector. One such example is the USA arguing that the EU has selectively prosecuted US technology companies to benefit its domestic sector.[158] Further, Western countries have complained about the discriminatory enforcement of competition laws in China, wherein Chinese state-owned enterprises are shielded to a great extent from competition law scrutiny.[159] Put simply, different approaches to competition policy can fragment global digital trade and thereby affect cross-border data flows.[160]

Given that competition law can impact digital trade and data flows, the question then arises if trade law has any role in addressing anti-competitive conduct in digital markets or where a competition law/policy requirement is trade restrictive in nature. To date, only two trade disputes have directly dealt with the interface between competition and trade law. This is unsurprising because, as discussed in section II, there are limited disciplines on competition in WTO law and the competition chapters in PTAs are mostly non-binding. The first case, the *Japan – Film* dispute, was a non-violation complaint brought by the USA challenging the inaction of the Japanese government against the exclusive distribution arrangements of Fuji (a Japanese company) that resulted in foreign firms such as Kodak from accessing the Japanese film market.[161] The USA, however, lost this dispute as it could not meet the burden of proof necessary for a non-violation complaint under WTO law. The second dispute was *Mexico – Telecoms*, where the WTO panel found that the Mexican regulations on international telecommunications services (specifically, the imposition of termination rates by Telmex) was inconsistent with requirements on access pricing in the Reference Paper on Telecoms.[162]

The above WTO disputes, however, provide little insight into how a present-day digital trade dispute interfacing with competition law is likely to be dealt with by a trade tribunal. For instance, if a government imposes a data-restrictive measure, such as a requirement to store data locally or for foreign technology platforms to mandatorily share data with smaller local players so as to create a level playing field for local technology companies, then such a measure may violate different obligations contained in international trade law.[163] However, the

[158] J Brooymans-Quinn and A Malinouski, 'Competition Policy and the International Trade Landscape: Assessing Recent Developments and Trends' (Trade Labs, 2020) 13.

[159] See generally M Wu, 'The "China, Inc" Challenge to Global Trade Governance' (2016) 57(2) *Harvard International Law Journal* 261.

[160] WEF, 'Competition Policy in a Globalized, Digitalized Economy' (11 December 2019) 4.

[161] *Japan – Measures Affecting Consumer Photographic Film and Paper*, Panel Report (adopted 31 March 1998) WT/DS44/R.

[162] *Mexico – Measures Affecting Telecommunications Services*, Panel Report (adopted 1 April 2004) WT/DS204/R.

[163] Incidentally, such a measure may also be contrary to the consumer welfare standard. However, not all countries may ascribe to that standard or may be pursuing different policy objectives through their competition law and policy regime.

exact assessment would depend on the measure at issue and the service sectors affected by the data-restrictive measure. If a member has made the relevant commitments and violates obligations under GATS, then it is quite likely that they may not be able to justify the measure under the exceptions available in GATS, especially if it is clearly a protectionist measure.

Another instance where trade law may come into play is when a regulator selectively enforces competition law to the disadvantage of foreign digital service providers (for instance, targeted competition law enforcement against US or Chinese Big Tech companies), thus resulting in a trade-restrictive impact. Such enforcement has the effect of discriminating against foreign digital services/service providers and can also prohibit market access, and thus theoretically violates obligations on non-discrimination and market access under GATS.

Measures related to data portability or a mandatory data sharing requirement may violate GATS, Article VI if the measure is not implemented in a reasonable, objective and impartial manner, although no dispute to date provides any clarity on how this provision applies in practice. A WTO member can also bring a non-violation complaint if a particular measure nullifies or impairs any benefits accruing to it, but the burden of proof in such disputes is very high and hard to fulfil.

The possibility of taking action for the above-discussed measures under PTAs is much more negligible, given that most of them exclude dispute settlement for the competition chapter. While some of these PTAs contain extensive disciplines on data-restrictive measures in other chapters (eg digital trade or electronic commerce chapter), it is unclear if a competition law requirement that restricts cross-border data flows will be examinable by the PTA tribunal.

IV. THE ROLE OF INTERNATIONAL TRADE LAW IN ENABLING COMPETITION IN THE DATA ECONOMY

The above discussion indicates two critical factors regarding the relationship between competition law and the regulation of cross-border data flows. First, competition law and policy is critical for global data governance as it can potentially prevent data harms and facilitate data equity. However, there is insufficient global consensus among competition regulators regarding the best tools available to achieve these outcomes. Second, international trade law and competition law seem to share a two-sided relationship in the context of digital trade. While competition law is fundamental to developing a holistic framework for digital trade, certain measures aimed at rebalancing competitive dynamics in the domestic market can adversely affect cross-border data flows and digital trade. The existing disciplines in international trade agreements neither provide a concrete solution in addressing the latter tension nor contain any specific rules that facilitate global competition in data-driven sectors.

To date, there has been no successful global initiative or framework on competition regulation at the WTO or under the aegis of the UN. This is perhaps unsurprising, given that different countries associate different policy objectives with their domestic competition law. Further, developed countries may not see much value in cooperating with competition regulators in developing countries, especially where such markets are insignificant in size.[164] Specific to the digital sector, certain bodies, such as the OECD and the ICN (a transnational network of competition regulators), have had limited success in developing voluntary frameworks on competition law and policy in the digital sector, as detailed below,[165] but this is also a work-in-progress.

Further, competition law and policy networks in bodies such as the ICN and the OECD often do not directly interface with trade bodies such as the WTO. Yet, there are several unexplored synergies across these two different areas of policy-making. Therefore, the first part of this section highlights the relevance of these transnational policy networks in competition regulation for the digital sector. Thereafter, the section argues for better alignment of international trade law with transnational models of competition regulation, especially through innovations in evolving digital trade/digital economy agreements.

A. Transnational Approaches to Competition Regulation

While it appears desirable at first sight to develop a legally binding, multilateral framework for global competition, the discussion so far indicates that such a framework is most likely unrealistic and infeasible. Therefore, for competition regulation in the digital sector, several scholars have repeatedly indicated the need to shift to alternate fora to develop global consensus on competition law issues.[166] Two bodies have been particularly instrumental in this regard: the OECD and the ICN.[167] This subsection briefly examines their role and relevance

[164] Bradford, 'Antitrust Law in Global Markets' (n 17) 315–16.

[165] See, eg OECD, 'Competition Issues in News Media and Digital Platforms', www.oecd.org/daf/competition/competition-issues-in-news-media-and-digital-platforms.htm; OECD, 'Data Portability, Interoperability and Competition', www.oecd.org/daf/competition/data-portability-interoperability-and-competition.htm; OECD, 'Ex Ante Regulation and Competition in Digital Markets', www.oecd.org/daf/competition/ex-ante-regulation-and-competition-in-digital-markets.htm; OECD, 'Abuse of Dominance in Digital Markets', www.oecd.org/daf/competition/abuse-of-dominance-in-digital-markets.htm; OECD, 'Competition Economics of Digital Ecosystems', www.oecd.org/daf/competition/competition-economics-of-digital-ecosystems.htm; OECD, 'Implications of E-commerce for Competition Policy', www.oecd.org/daf/competition/e-commerce-implications-for-competition-policy.htm.

[166] Tarullo (n 15); I Maher, 'Competition Law in the International Domain: Networks as a New Form of Governance' (2002) 29(1) *Journal of Law and Society* 111, 114–17.

[167] Other organisations that have developed global/transnational initiatives on competition regulation include APEC (*APEC Principles to Enhance Competition and Regulatory Reform*) and UNCTAD (*Guiding Policies on Competition Law Enforcement*).

in developing norms and best practices for competition in the digital sector, and then argues why a transnational approach to digital competition is better suited to adapting to the complexity of data-driven markets.

The OECD is an intergovernmental organisation that was founded in 1961 and consists of 38 members. Its core objective is to 'establis[h] evidence-based international standards and fin[d] solutions to a range of social, economic and environmental challenges'.[168] One of the focus areas of the OECD is competition, wherein the organisation is committed to work towards 'well-designed competition law, effective enforcement and competition-based economic reform' so as to 'promote consumer welfare and economic growth while making markets more flexible and innovative'.[169]

The OECD has been instrumental in developing various best practices, guidelines and non-binding recommendations on competition in the digital economy. For instance, it has conducted a detailed analysis of the economic models of digital markets to analyse the extent to which existing competition rules are relevant for the digital world.[170] It has also developed various tools for competition regulators to understand how to design and implement competition law interventions in digital markets, especially to address the harms arising from the widespread network effects and winner-takes-most dynamics in digital markets.[171] For instance, the OECD outlined the limitations of blind reliance on market concentration to assess anti-competitive tendencies of a digital market and instead indicated the relevance of other parameters, such as rate of entry and exit and various indicators of profitability.[172] It has also identified various competition law interventions necessary for assessing market power arising from data feedback loops[173] and negative externalities arising from network effects in multi-sided digital platforms,[174] and assessing non-price elements in digital mergers.[175]

The ICN is another influential player in global digital competition policy. It functions as a global network of competition regulators or agencies to discuss and develop a common understanding of competition law concerns, but has no ability to prescribe binding rules to governments.[176] Thus, the primary role of

[168] OECD, 'About', www.oecd.org/about/.
[169] OECD, 'Competition', www.oecd.org/competition/.
[170] OECD, 'The Digital Economy' (7 February 2013) DAF/COMP(2012)22.
[171] OECD, *Handbook on Competition Policy* 19.
[172] OECD, 'Market Concentration', www.oecd.org/competition/market-concentration.htm; OECD, 'Abuse of dominance in digital markets', www.oecd.org/daf/competition/abuse-of-dominance-in-digital-markets.htm.
[173] OECD, 'Big Data: Bringing Competition Policy to the Digital Era', www.oecd.org/competition/big-data-bringing-competition-policy-to-the-digital-era.htm.
[174] OECD, *Rethinking Antitrust Tools for Multi-Sided Platforms* (2018).
[175] OECD, 'Non-price Effects of Mergers', www.oecd.org/competition/non-price-effects-of-mergers.htm.
[176] International Competition Network, 'About', www.internationalcompetitionnetwork.org/about/.

the ICN is to facilitate joint dialogues and studies, resulting in soft law principles and best practice guidelines.[177] A wide range of stakeholders, such as academics and think tanks, are also involved in the ICN alongside government bodies. Consequently, it is an important avenue for deliberation and norm diffusion.[178]

The ICN has also been actively involved in developing a forum for knowledge and experience sharing regarding competition law issues in the global digital economy. For instance, it published a report outlining the varied experience of its global network of competition regulators in relation to undertaking competition law advocacy in the digital sector.[179] Another relevant example is a study conducted on cartels in Big Data and AI-driven industries.[180] The ICN and OECD have also collaborated on certain initiatives, such as the joint survey on international cooperation on competition law enforcement.[181]

Bodies such as the ICN and, to a certain extent, the OECD are well suited for developing global norms and best practices on competition in the digital sector. First, they act as important sites for knowledge exchange and information sharing, and are thereby instrumental in developing common terminology and a common toolbox for competition law enforcement and advocacy for the digital sector.[182] Second, given their flexible, soft approach, these organisations avoid the high politics of other multilateral bodies such as the WTO and instead focus on the incremental development of norms and best practices for highly dynamic digital sectors. Finally, given their multistakeholder composition, bodies such as the ICN are more participatory and facilitate more bottom-up policy experimentation than traditional trade institutions.

B. Aligning Transnational Competition Regulation with International Trade Law

Certain scholars have proposed that trade bodies can be instrumental in developing a global framework for competition. For instance, Matsushita proposed that the WTO members could adopt a non-binding framework for

[177] DD Sokol, 'International Antitrust Institutions' in RD Blair and DD Sokol (eds), *The Oxford Handbook of International Antitrust Economics*, vol 1 (Oxford, Oxford University Press, 2014) 193.

[178] ibid 200; Brooymans-Quinn and Malinouski (n 158) 43.

[179] International Competition Network, 'Report on ICN Members' Recent Experiences (2015–2018) in Conducting Competition Advocacy in Digital Markets' (2019).

[180] International Competition Network, 'The International Competition Network Presents a Scoping Paper on "Big Data and Cartels" Analysing the Impact of Digitalisation in cartel Enforcement' (June 2020) www.internationalcompetitionnetwork.org/wp-content/uploads/2020/06/CWG-Big-Data-scoping-paper-summaryENGFR.pdf.

[181] OECD, *OECD/ICN Report on International Co-operation in Competition Enforcement* (2021).

[182] C Carugati, 'How Best to Ensure International Digital Competition Cooperation' (Bruegel, 6 February 2023) www.bruegel.org/policy-brief/how-best-ensure-international-digital-competition-cooperation.

competition law.[183] Fox suggested a similar approach, indicating that such a competition code could be voluntary for states to adopt.[184] Drake-Brockman and others further suggested that under the joint initiative on e-commerce, WTO members must agree to update the Reference Paper on Telecoms to include new disciplines for competition in the digital sector.[185] Similarly, Peng proposed a new WTO Data Reference Paper to deal with various aspects of digital inequality resulting from the power of Big Tech platforms.[186] However, previous discussions in this chapter indicate that the WTO has historically been ill-suited to develop and implement a global framework on competition. This may equally apply to data-driven sectors. The process of developing such principles will likely be slow and costly, and there is limited possibility of finding convergence between developed and developing countries.[187]

Therefore, this section proposes an alternate route of incorporating certain rules in digital trade chapters of PTAs and DEAs to better align competition and trade law in the digital economy. This step is necessary because competition law is an important foundation for building a fair and equitable framework for cross-border data flows.[188] It is more feasible to gradually develop these frameworks under PTAs and DEAs as their parties are usually like-minded trading partners and have strong incentives to develop robust provisions for digital trade flows.

First, digital trade chapters in PTAs and DEAs can incorporate by reference best practices emerging from relevant transnational bodies such as the ICN and the OECD. Some DEAs, such as the Digital Economy Partnership Agreement (DEPA), already provide an avenue for doing so, for instance by allowing parties to share information and best practices on competition policies necessary for the digital economy.[189] Further, the Singapore–Australia Digital Economy Agreement (SADEA) includes the possibility of both countries engaging in technical cooperation on competition issues.[190] As discussed earlier, organisations such as the ICN and the OECD have considerable expertise and often enjoy a stronger degree of goodwill given the non-binding and flexible nature of their recommendations. Certain PTAs, such as the USMCA, have also borrowed from the recommendations on regulatory cooperation and procedural fairness

[183] See generally Matsushita (n 16).

[184] See generally E Fox, 'The End of Antitrust Isolationism: The Vision of One World' (1992) 1 *University of Chicago Legal Forum* 237; Fox, 'Toward World Antitrust' (n 21).

[185] J Drake-Brockman et al, 'Digital Trade and the WTO: Negotiation Priorities for Cross-Border Data Flows and Online Trade in Services' (2021) Jean Monnet TIISA Network Working Paper 2021/11.

[186] See generally S Peng, 'The Uneasy Interplay between Digital Inequality and International Economic Law' (2022) 33(1) *European Journal of International Law* 205.

[187] Bradford, 'Antitrust Law in Global Markets' (n 17) 322.

[188] Beyleveld and Sucker (n 151) 70–74.

[189] Digital Economy Partnership Agreement (12 June 2020), Art 8.4 (DEPA).

[190] Singapore–Australia Digital Economy Agreement (6 August 2020), Art 16.1 (SADEA).

in competition law enforcement from the ICN. Further, as the majority of ICN and OECD outputs are voluntary guidelines and recommendations, they provide autonomy to countries to design the implementation details based on their regulatory needs and capacity.[191] Regional bodies such as the Competition Commission of the Common Market for Eastern and Southern Africa can also play a more central role, especially for developing African economies, and can provide best practices suited to the African context.[192]

Eventually, the above approach may lead to more interoperability across domestic competition frameworks (for instance, due to a shared understanding of terminologies and high-level objectives) and minimise conflict between domestic competition law measures and international trade obligations.[193] This convergence is also necessary as certain countries are seeking to introduce competition disciplines in the plurilateral agreement on e-commerce at the WTO. A leaked draft of the plurilateral agreement being negotiated under the Joint Initiative on E-Commerce at the WTO indicates that Brazil proposed a provision on competition, wherein WTO members acknowledge that 'some characteristics of digital trade, such as platform-based business models, multi-sided markets, network effects and economies of scale, may pose additional challenges on competition policy".[194] Consequently, WTO members may eventually endeavour to develop approaches to address competition challenges in the digital economy and identify common tools for cooperation on relevant competition law issues.[195]

Second, several PTAs provide for dedicated fora or committees to deal with digital trade issues. Similarly, several regional trade/political organisations, such as ASEAN and the African Union, have dedicated bodies dealing with data governance and digital trade matters. Such committees can be an informal forum among trading partners to discuss the interface between trade and competition in the digital sector and the regulatory experience of implementation of competition law provisions on preventing data harms.

Scholars have argued that PTAs provide a laboratory for testing new disciplines, especially in emerging areas of digital trade.[196] They are far more effective than multilateral instruments in facilitating gradual regulatory convergence and finding alignment between like-minded trading partners to reduce transactional costs of variable regulation.[197] Disciplines on transparency, non-discrimination

[191] Lee (n 16) 297–8.

[192] M Burri and K Kugler, 'Digitization, Regulatory Barriers and Sustainable Development' (2023) Trade Law 4.0 Working Paper No 03/2023, 14.

[193] This aligns with the loose harmonisation approach. See A Heinemann and YS Choi, 'Competition and Trade: The Rise of Competition Law in Trade Agreements and Its Implications for the World Trading System' (2020) 43(4) *World Competition* 521, 525.

[194] WTO, 'WTO Electronic Commerce Negotiations – Consolidated Negotiating Text' (14 December 2020) INF/ECOM/62/Rev.1, Art B.4(1)(4).

[195] ibid Art B.4(1)(4).

[196] Mavroidis and Neven (n 17) 412.

[197] RP Lazo and P Sauvé, 'The Treatment of Regulatory Convergence in Preferential Trade Agreements' (2018) 17(4) *World Trade Review* 575, 576–77.

and implementation of good regulatory practices are also vital to achieve a bottom-up approach towards regulatory convergence.[198] Nonetheless, regulatory convergence necessarily involves certain adjustments for parties and, if not carefully calibrated, certain countries may view them as an attack on their regulatory autonomy.[199] Further, regulatory convergence is only possible where there are certain shared values.[200]

In the context of competition regulation in data-driven sectors, there is a difficult trade-off between promoting digital innovation and digital trade flows and protecting public interests.[201] Ultimately, like-minded trading partners need to find the best way to prevent their domestic competition laws from becoming a pretext for protectionism.[202] The PTA/DEA committees can be an important forum to discuss and debate the interplay of these complex policy considerations and explore avenues for regulatory convergence. For instance, some important questions could be how to apply existing competition law tools for the digital sector and operationalise new frameworks for data portability or interoperability. These deliberations are likely to function better without the threat of a trade dispute since most countries are likely to be dissatisfied if their domestic policy choices regarding competition law could be questioned before international trade tribunals.[203]

Developing countries are more likely to face capacity constraints in developing their competition law framework, especially in the context of competition enforcement in data-driven industries. A survey of the World Bank indicated that several competition regulators in developing countries did not have expertise dedicated to regulating the digital economy, in sharp contrast to the resources of the Big Tech companies operating in those countries.[204] Therefore, in line with the recommendations in chapter five, it is important to develop a binding and effective method for providing technical assistance and capacity-building support for developing countries to develop their domestic competition law regimes.

Finally, trade agreements can complement non-trade bodies such as the ICN in developing the regulatory cooperation necessary to stimulate competition in the digital sector. There are several possible avenues. For instance, under regional trade unions or megaregional trade agreements, finding a route for cooperation

[198] ibid 595.
[199] Lazo and Sauvé (n 197) 601.
[200] A Lang and J Scott, 'Regulatory Convergence – A Role for the WTO?' in *Proceedings of Annual BIICL WTO Conference, Gray's Inn, 23–24 May 2006*.
[201] APEC, 'Competition Law and Regulation in Digital Markets' (March 2022) APEC#222-EC-01.3, 9–10.
[202] L Chen et al, 'The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies' (T20 Japan, 29 March 2019) www.t20japan.org/policy-brief-digital-economy-economic-development/; Brooymans-Quinn and Malinouski (n 158) 3.
[203] Bradford, 'Antitrust Law in Global Markets' (n 17) 293–94.
[204] World Bank (n 8) 232.

on cross-border competition enforcement especially in complex digital sectors might be fruitful. While this kind of cooperation typically exists through bilateral arrangements between competition regulators,[205] these are likely to have a limited impact when the anti-competitive conduct affects foreign firms, especially if there is sufficient competition in the domestic market.[206] Another area where regulatory cooperation could be meaningful is in the development of common best practices to promote small and medium enterprises in the digital sector. Finally, as data access remains a key constraint for competing in digital markets, digital trade agreements and DEAs could provide for cross-border regulatory sandboxes for testing data-sharing arrangements consistent with data protection and intellectual property laws.

V. CONCLUSION

With the rapid datafication of the economy, competition law stands at a crucial juncture. While, on the one hand, there are concerns regarding widespread data monopolisation and related abuses arising due to the inherent characteristics of the digital sector, others have pointed out the adverse effects of overregulation in competition law, particularly on digital innovation and data flows.[207] It is in the midst of this complex policy environment that this chapter seeks to understand the interface between competition and trade law in the global regulatory framework for cross-border data flows.

This chapter argues that competition law is a fundamental component of the global regulatory framework for cross-border data flows as it plays an instrumental role in preventing data harms and potentially facilitates data equity. However, given the complex interface between trade law and competition law, and especially the failure to integrate a competition agenda into WTO law, it remains unclear how international trade law can play a meaningful role in future. In particular, it is likely both infeasible and counterproductive to develop a multilateral competition law instrument under the WTO. This chapter also argues that trade tribunals are not an appropriate forum to resolve most disputes arising due to a conflict of domestic competition law/policy and international trade law.

Instead, the chapter seeks a more moderate approach, acknowledging that robust competition law is necessary for a robust framework for cross-border data flows. Transnational and regional bodies, including the ICN and the OECD, are currently at the forefront of developing competition norms and best practices

[205] Tarullo (n 15) 496, 498.
[206] ibid 498.
[207] Bradford, 'Antitrust Law in Global Markets' (n 17) 307; M Bauer et al, 'The EU Digital Markets Act: Assessing the Quality of Regulation' (ECIPE, February 2022) www.ecipe.org/publications/the-eu-digital-markets-act/.

for the digital and data-driven sectors. This chapter argues that the best way forward is for international trade law to seek stronger alignment with the policy expertise in these bodies by incorporating their policy recommendations and best practices by reference. This can provide a basis for developing a consensus on shared values and thereafter explore new avenues for regulatory cooperation and mutual policy learning.

7

Conclusion: Aligning International Trade Law and Global Data Governance: Towards a Multilayered Approach

I. INTRODUCTION

The last five chapters investigated the interaction of international trade law and global data governance by looking at data-restrictive measures related to five policy objectives: data protection, cybersecurity, governmental access to data, bridging the data divide and competition law. In this final chapter, I reflect on the common features characterising the interaction of these two fields of regulation to understand what can and must be done next. In other words, can international trade law and global data governance be better aligned? What is the future role of international trade law in developing a regulatory framework for global data governance? Can international trade law navigate the conflicting ideas of free flow of data and data sovereignty?[1]

At the outset, chapter one highlighted the disconnect between international trade law and global data governance. While trade law is predominantly based on treaties signed between countries at the multilateral, plurilateral or bilateral level, global data governance can be best described as a form of polycentric governance or policy regime complex, consisting of domestic laws and policies, soft law, best practices, international treaties, technical standards and protocols, and various forms of informal understandings between stakeholders at different levels of governance. Recent years have seen a proliferation of government measures pertaining to data governance.[2] Some of these measures restrict cross-border data flows and create trade barriers for companies conducting digital

[1] See generally L Porciuncula and BD La Chapelle, 'We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty' (Internet and Jurisdiction Policy Network, 2021).

[2] U Gasser and V Almeida, 'Futures of Digital Governance' (2022) 65(3) *Communications of the ACM* 30; JS Nye, 'The Regime Complex for Managing Global Cyber Activities' (20 May 2014) Global Commission on Internet Governance Paper Series No 1; see generally SA Aaronson et al, 'DataGovHub Paradigm for a Comprehensive Approach to Data Governance – Year 1 Report' (Digital Trade & Data Governance Hub, 2021).

trade transactions. Consequently, the data-restrictive elements in these domestic measures violate obligations contained in trade treaties, as discussed in the previous chapters.

In understanding how international trade law applies to such data-restrictive measures, policy concerns in both global and domestic data governance are relevant. This is particularly the case when governments invoke exceptions contained in trade treaties to defend their domestic policy space to regulate data flows. For international trade law to play a meaningful role in such legal analysis and contribute better to cross-border data governance, questions of data regulation and governance should not be artificially segregated from international trade law. Instead, we must understand the gaps in the application of international trade law to domestic data regulations. In engaging in this exercise, it is necessary to get the right balance between liberalising data flows/digital trade and facilitating regulation of data.

In section II of this chapter, I reflect on the previous chapters to highlight the common trends and concerns in relation to applying international trade law to domestic data regulations. First, I note that there is a rapid increase in data-restrictive measures that curtail digital trade flows, thereby implicating various obligations in international trade law. This increase in data-restrictive measures also leads to regulatory fragmentation, which is harmful for the growth of the global digital economy. Second, in applying international trade law to data-restrictive measures, I find that the most judicious approach is stronger reliance on technical and legal evidence to assess the necessity, efficacy and reasonableness of such measures, without deeply scrutinising the stated policy objective behind the measures. Third, I identify a common need to develop a multilayered approach for developing cross-border data regulatory frameworks in international trade law. Such an approach must predominantly focus on building digital trust, enabling interoperability of regulatory frameworks and incorporating relevant multistakeholder and transnational norms, global best practices and standards by reference. Finally, I find an urgent need to contextualise the global data divide in different aspects of regulating digital trade.

In section III, I turn my attention to the alignment of international trade law and global data governance. While previous chapters have outlined ideas to align trade law with a specific area of data regulation, this section focuses on the big picture of how this can be done in practice. First, the section argues that international trade law must be informed by a balanced narrative, avoiding the unhelpful dichotomy between the free flow of data and data sovereignty. Instead, a new narrative must be framed around values of international cooperation, trust, alignment and inclusion. Second, with this narrative in mind, I assess how existing provisions in World Trade Organization (WTO) law and preferential trade agreements (PTAs) can be put to better use in formulating a framework for cross-border data flows. The section then proposes new instrumentalities in international trade law, such as a Reference Paper or a non-binding declaration on data governance, a standards framework for data-driven services and new disciplines to foster broader forms of international regulatory cooperation,

including engagement with multistakeholder bodies. Finally, it outlines the need for a mixture of both formal and informal institutional mechanisms to operationalise the proposed normative frameworks.

While the discussion in section III indicates the need to develop a sophisticated, multilayered framework for cross-border data flows and digital trade, implementing it requires a significant shift in attitudes that have long underpinned the international trade law framework. Section IV highlights new areas of research and policy reflection necessary to carry this reform agenda forward, focusing on the operationalisation of interoperability and building a model of digital trade regulation that combines both multilateral and multistakeholder approaches. This chapter concludes by emphasising the importance of developing a multilayered approach for regulating cross-border data flows in international trade law. There is already some movement in this direction, especially in the digital economy agreement (DEA) model, as discussed in previous chapters. Certain countries are also showing more openness to experiment with various forms of informal and soft understandings,[3] particularly focused on far-reaching technical and policy cooperation under their PTA frameworks.[4]

The core argument of the book is that international trade law can play a meaningful and proactive role in the global framework for cross-border data flows by providing important 'building blocks'. This is not to say that all areas of data regulation can be addressed by simply reforming international trade law. For instance, I have argued elsewhere that international trade law is ill-suited to addressing sensitive concerns around online censorship measures, even if the implemented measures are trade restrictive.[5] International trade law also faces several constraints in dealing with issues of international human rights.[6] The previous chapters indicated the limitations of international trade law

[3] The Digital Economy Partnership Agreement (DEPA), UK–Singapore Digital Economy Agreement (UKSDEA), Korea–Singapore Digital Partnership Agreement and Singapore–Australia Digital Economy Agreement (SADEA) contain soft provisions in new areas such as data innovation, AI ethics, open government data, fintech and regulatory sandboxes, all of which can facilitate technical cooperation on emerging areas of data regulation by relying upon common regulatory frameworks and principles.

[4] See, eg 'Ministerial Text for Trade Pillar of the Indo-Pacific Economic Framework for Prosperity' (USTR, 2022) www.ustr.gov/sites/default/files/2022-09/IPEF%20Pillar%201%20Ministerial%20Text%20(Trade%20Pillar)_FOR%20PUBLIC%20RELEASE%20(1).pdf; European Commission, 'EU–US Trade and Technology Council', www.commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/EU-US-trade-and-technology-council_en#documents; European Commission, 'First EU–India Trade and Technology Council Focused on Deepening Strategic Engagement on Trade and Technology' (16 May 2023) www.ec.europa.eu/commission/presscorner/detail/en/ip_23_2728.

[5] N Mishra, 'Breaking Down Digital Walls: The Interface of International Trade Law and Online Content Regulation through the Lens of the Chinese VPN Measure' (2022) 47(2) *Brooklyn Journal of International Law* 359.

[6] SA Aaronson, 'What Are We Talking About When We Talk About Digital Protectionism?' (2018) 18(4) *World Trade Review* 541, 546–47, 559.

(particularly under the multilateral framework) to address controversial aspects of digital competition and data access measures. Multiple forces are at play in the complex political economy of digital trade: varying ideological preferences towards data and digital regulation; differences in social and moral values; asymmetry of development levels; geopolitical conflicts; and diverging consumer/public preferences in different countries. International trade law cannot provide a solution to all these conflicts, but it can at least navigate these concerns and conflicts more judiciously.

The existing tensions in digital trade should not deter policy-makers from pursuing a pragmatic approach in areas where transactional efficiency is possible by creating a more coherent, clear and robust framework for cross-border data flows. Further, increased digital trade will engender long-term trust between countries and help in dealing with more complex policy areas in the future. It can also facilitate more openness among governments in experimenting with new models of regulatory cooperation in difficult areas of global data governance. Ultimately, participating meaningfully in the global data-driven economy benefits the entire world and contributes to global economic welfare. It is thus timely for international trade law to move in a direction where it can contribute to the development of a robust, inclusive and cohesive global digital economy.

II. RECAPPING THE INTERFACE OF INTERNATIONAL TRADE LAW AND GLOBAL DATA GOVERNANCE

International trade law and data governance intersect and conflict in complex ways, creating several challenges in the regulation of data flows. Despite such complexities, the previous chapters highlighted both the necessity and the prospects of aligning trade rules with emerging norms, standards and best practices in global data governance. This alignment is fundamental to creating a balanced and holistic framework for cross-border data flows in international trade law. However, in developing such a global framework, we must first reflect on the common features characterising the interaction between trade law and different kinds of data regulations.

First, the discussions in previous chapters reveal that the complex political economy of digital trade has resulted in increased adoption of data-restrictive measures in domestic laws and regulations. Such measures adversely affect digital trade flows and lead to global regulatory fragmentation. Although such measures may be implemented in achieving important policy objectives, including data privacy, cybersecurity, governmental access to data, regulating data monopolies and ensuring data equity, they can create economic and technological inefficiencies across the global digital supply chains. Ultimately, such inefficiencies are likely to be passed on to end consumers, resulting in a decline of global economic welfare.

Despite their inefficiency, several factors explain the rise of data-restrictive measures. First, as discussed in chapter one, countries increasingly view data regulation from the lens of sovereignty; therefore, asserting control over data flows is seen as being fundamental to exercising digital sovereignty. Second, as chapters two, three and four in particular highlight, not all countries view data regulatory issues from a similar perspective. For instance, countries may adopt different ideologies and policy rationales for implementing laws on privacy and cybersecurity protection, or adopt varied policy tools to ensure governmental access to data.

Third, due to the global data divide, the increase in the economic and political power of Big Tech companies and the uncertain nature of cyber-threats, the digital ecosystem is characterised by a widespread trust deficit. This deficit makes governments highly cautious and leads to more widespread adoption of data-restrictive measures, as discussed in chapters five and six. Finally, as previous chapters indicate, an international consensus on the normative frameworks for data regulation in vital areas, including privacy, cybersecurity, governmental access to data, digital industrial policy and competition in digital sectors, is still nascent and evolving. In the absence of sufficient international legal frameworks, governments are unsurprisingly adopting several data-restrictive laws and policies in tune with their domestic interests, without necessarily considering the global, long-term repercussions.

Data-restrictive measures often breach international trade law. I have discussed several examples of such breaches in the previous chapters, using examples of measures aimed at achieving a variety of policy objectives. Where data-restrictive measures are inherently protectionist in nature (even though they may be disguised to achieve a legitimate policy objective, such as bridging the data divide or increasing data privacy and security), they are more likely to breach international trade law. However, for other data-restrictive measures that achieve legitimate policy objectives with an incidental trade-restrictive impact, the application of international trade law is much more complicated. Governments are expectedly worried about data-related disputes coming before trade tribunals, particularly if it is likely to constrain their data/digital sovereignty. Understanding the interface between trade rules and data regulatory frameworks is thus important in framing an appropriate narrative for the global regulation of cross-border data flows.

Second, the previous chapters suggest that dealing with trade disputes pertaining to data restrictions requires an apolitical and somewhat scientific approach (at least to the extent possible). Thus, trade tribunals must avoid deliberately delving deep into the genuineness of policy objectives proffered by governments while adopting data-restrictive measures. Instead, they must focus on relatively more objective questions, such as assessing the causal relationship between the measure and the stated policy objective. In doing so, trade tribunals can employ both legal and technical evidence, especially by hiring relevant

technical experts to assist in making crucial decisions, such as assessing the necessity and reasonableness of technical standards and the effectiveness/relevance of de jure or de facto data localisation measures. The focus must thus be on the measure employed to restrict data flows, not the genuineness of the policy objective. This approach is judicious as it better acknowledges the plurality of policy objectives driving data-restrictive measures across different countries and the limitations of trade bodies in resolving political conflicts arising due to varied ideological preferences on data regulation.

Ultimately, however, questions will inevitably arise in the above legal analysis that pertain to global/domestic data governance and not international trade law. For instance, in applying general exceptions to data-restrictive measures, trade tribunals must also consider less trade-restrictive alternatives. This is especially difficult as the available evidence may not always be entirely clear or robust regarding the efficacy of various legal/policy measures. As an example, there might be competing technical standards for privacy or cybersecurity. Further, the ability of the government to regulate technology companies, especially data monopolies, may vary significantly across jurisdictions. Also, where a regulation is closely linked to national security or access to personal data for law enforcement, governments may be unwilling to shift their regulatory stance, even when there is a trade-restrictive impact. Ultimately, if trade tribunals get heavily involved in the high politics of data regulation, it can lead to adverse consequences, including countries wilfully ignoring decisions of dispute settlement bodies.

Third, the previous chapters indicate that data regulation is inherently multilayered in nature. This means that the regulation of cross-border data flows is a product of a complex, polycentric framework consisting of domestic laws and regulations, international treaties, soft law, policy frameworks, best practices and technical standards. While several examples indicate that states now play a more predominant role in exercising control over data flows, several regulatory and policy responses to cross-border data regulation are still centred in transnational regulatory bodies as well as international organisations. Some of the key examples discussed in this regard are the Organisation for Economic Co-operation and Development (OECD), the Asia-Pacific Economic Cooperation (APEC), the International Competition Network (ICN, for competition), the Global Privacy Assembly (GPA, for privacy regulation), the International Telecommunication Union (ITU, for cybersecurity), regional bodies such as the Association of Southeast Asian Nations (ASEAN) and the African Union, Internet multistakeholder bodies and several types of standard-setting bodies. Thus, data governance is inherently transnational in nature.

However, international trade law does not provide sufficient scope to take into account this complex nature of global data governance. For instance, previous chapters argue about the limited relevance of private, multistakeholder and transnational norms and technical standards in interpreting and applying

the existing provisions in trade treaties. Further, the majority of trade treaties, including the General Agreement on Trade in Services (GATS), do not contain tailored, comprehensive provisions applicable to domestic regulations pertaining to digital trade or data flows. Consequently, the existing trade rules fall short when applied in the context of regulating data-restrictive measures. Thus, previous chapters provide specific legal and policy options to address these gaps. A common factor across these solutions is the necessity of a multilayered framework in international trade law to address the cross-cutting nature of data flows. Mechanisms also need to be integrated for political resolution of disputes in this framework to address certain core data sovereignty issues, such as cybersecurity-related and data access measures.

To develop such a multilayered framework, trade bodies (ie the WTO and other regional trade organisations) must develop appropriate normative frameworks and institutional mechanisms. As regards the normative framework, the previous chapters indicate the need to shift attention from the high politics of dispute settlement to building a core normative framework for digital trade, including trust-based solutions such as developing interoperable regulatory frameworks, incorporating relevant global norms, standards and best practices by reference in trade law, and creating more avenues for political dialogues and cooperation. This means that trade bodies must strengthen and enhance their deliberative, administrative and facilitative roles, and foster more technical and policy cooperation on relevant matters. In terms of institutional mechanisms, the purely state-driven nature of trade bodies needs to be reoriented to accommodate deeper engagement with a variety of other international organisations, multistakeholder bodies and transnational regulatory bodies with expertise in different aspects of global data governance.

Finally, another common thread across the previous chapters is the impact of the global data divide between developing and developed countries on the regulation of cross-border data flows. With the concentration of Big Tech companies and data monopolies in a handful of digitally advanced economies, most developing countries are facing an uphill challenge in creating meaningful economic opportunities for their domestic digital sector and reducing long-term dependence on foreign technologies. Further, developing countries do not enjoy sufficient autonomy in designing their domestic data and digital regulatory frameworks as they are often coerced by leading digital powers to adopt a specific regulatory model without due consideration of their local needs. These factors lead to a critical trust deficit in the global digital economy.

The preceding chapters argued that there is an urgent need to address this data divide by creating a tailored mechanism to provide technical assistance and capacity-building support to developing countries, discussing more transparently issues of technology transfer in digital sector and creating proper incentives for developing countries to liberalise cross-border data flows. Further, least developed countries (LDCs) need additional support to build basic regulatory

frameworks and digital infrastructure to participate meaningfully in the global digital economy. Without looking at questions of fair data sharing, regulation of data monopolies and data equity, the yawning global data divide cannot be bridged.[7] In that regard, frameworks developed by regional bodies consisting of developing countries, such as the ASEAN, the Pacific Alliance and the African Union, can play a significant role, alongside multistakeholder and global initiatives focusing on data sharing and interoperability in different sectors of public importance.[8]

III. CHARTING PATHWAYS FOR ALIGNING INTERNATIONAL TRADE LAW AND GLOBAL DATA GOVERNANCE

The previous section recapped the key features of the interaction of international trade law and global data governance, and concluded that there is a need for stronger alignment between these two areas of regulation. To achieve this alignment in a multilayered framework, a coherent narrative is necessary in addition to appropriate rules/norms and institutions.

A. Framing a Balanced Narrative

We live in a world that is divided by geopolitical tensions and deep ideological conflicts between leading powers. These divisions are also clearly visible in the context of digital trade and data regulation.[9] Chapter one highlighted how the current narrative in global data governance is split between two opposing ideologies: the free flow of data and data sovereignty. These divisions were also reflected in how data-restrictive measures were imposed by governments to realise different domestic policy objectives. However, such dichotomy is unhelpful in addressing the most basic issues in digital trade. For instance, as previous chapters illustrate, data sovereignty considerations may create policy dilemmas

[7] See generally N Evertsz et al, 'What Constitutes Equitable Data Sharing in Global Health Research? A Scoping Review of the Literature on Low-Income and Middle-Income Country Stakeholders' Perspectives' (2023) 8(e010157) *BMJ Global Health* 1.

[8] UNSTATS, 'UN Launches First of Its Kind "Privacy Lab" to Unlock Benefits of International Data Sharing' (25 January 2022) www.unstats.un.org/bigdata/events/2022/unsc-un-pet-lab/UN%20PET%20Lab%20-%20Press%20Release%20-%2025%20Jan%202022.pdf; 'The UN Is Testing Technology that Processes Data Confidentially' (*The Economist*, 29 January 2022) www.economist.com/science-and-technology/the-un-is-testing-technology-that-processes-data-confidentially/21807385.

[9] See generally D Lippoldt, 'Mitigating Global Fragmentation in Digital Trade Governance – A Case Study' (January 2023) CIGI Papers No 270; SJ Evenett and J Fritz, 'Emergent Digital Fragmentation: The Perils of Unilateralism' (Hinrich Foundation, 28 June 2022); C Buckridge, 'Fragmentation: Still the Internet's Big Bad' (Ripe Lab, 28 November 2022) www.labs.ripe.net/author/chrisb/fragmentation-still-the-internets-big-bad/; DW Arner et al, 'The Transnational Data Governance Problem' (2021) 37(2) *Berkeley Technology Law Journal* 623.

for trade tribunals when they apply international trade law to several data-restrictive measures. Similarly, a narrative purely focused on the free flow of data ignores other important policy considerations pertaining to data governance. For instance, it is important to balance the principle of Internet openness with other core policy objectives, such as protecting privacy and ensuring data and network security.[10]

Further, adopting a dichotomous approach to cross-border data governance is futile because the ground realities are more nuanced. As chapter one briefly argued, most countries adopt legal and policy frameworks that reflect a balance of different priorities, such as promoting domestic opportunities for digital trade, participating in the global digital economy, dealing with geopolitical divides and protecting domestic interests. Thus, there is no clear choice between the free flow of data and data sovereignty. For instance, the USA, which is seen as an advocate of the free flow of data, has also adopted the Clean Network Initiative, a programme essentially restricting the use of Chinese technologies in the digital infrastructure of the USA, such as application software, cloud services and telecommunications networks.[11] Similarly, the EU, despite being an advocate of multistakeholder Internet governance, has passed various proposals aimed at achieving digital sovereignty and strategic autonomy, reflecting a combination of human rights and geopolitical concerns, as well as internal market-related interests.[12]

A multilayered framework for cross-border data flows necessitates a fundamental shift of narrative to focus on international cooperation, trust and regulatory interoperability/alignment. In this regard, the idea of Data Free Flow with Trust (DFFT), discussed in chapter one, is a helpful starting point. It looks at trade agreements and other digital/data policy interventions through the lens of trust-based frameworks.[13] The proposal for the multilayered framework outlined in this book and the concept of DFFT are complementary. In both cases, data governance will be conducted by multiple institutions at different levels of governance, including relevant transnational or multistakeholder bodies, to ultimately increase trust between countries in critical areas such as privacy, consumer protection, cybersecurity and data ethics. Further, both these ideas can be tied to broader policy goals, such as enabling secure

[10] See generally N Mishra, 'Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows' (2019) 52(2) *Vanderbilt Journal of Transnational Law* 463.

[11] US Department of State, 'The Clean Network', www.2017-2021.state.gov/the-clean-network/; see also HBR, 'How the Clean Network Changed the Future of Global Technology Competition' (05 October 2021) www.hbr.org/podcast/2021/10/how-the-clean-network-changed-the-future-of-global-technology-competition.

[12] See generally D Broeders et al, 'In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions' (2023) 61(4) *JCMS: Journal of Common Market Studies* 1.

[13] A Arasasingham and M Goodman, 'Operationalizing Data Free Flow with Trust (DFFT)' (CSIS, April 2023) 3.

and privacy-compliant data sharing and creation of international 'data spaces' where different entities can conduct digital trade transactions.[14]

In developing a framework for cross-border data flows, it would be pragmatic to first focus on areas in which policy and technical cooperation are more feasible. For instance, like-minded trading partners could agree upon a common data classification mechanism, or adopt common or interoperable technical standards for digital services and applications. This can gradually metamorphose into more elaborate models of international regulatory cooperation across a larger group of countries to address more difficult areas, such as developing high-level principles for transfer of personal data or policy/legal criteria for implementing data localisation. Important elements that must be further woven into this framework are those of digital inclusion and bridging the data divide between the developed and developing world. A balanced narrative on cross-border data flows would be instrumental in this regard. The next question, then, is how to operationalise such a narrative, which I discuss below.

B. Developing Relevant Trade Law Disciplines for Alignment

This section now turns towards the core normative frameworks necessary to develop alignment between trade rules and global data governance. Several scholars and policy experts have already outlined different kinds of reforms necessary to make trade law more compatible with the digital economy.[15] Building on those proposals, this subsection specifically focuses on the creation and implementation of meaningful norms, principles and rules on cross-border data flows in trade law, both highlighting the need to better use existing rules in international trade agreements and suggesting new provisions to strengthen the alignment of international trade law and global data governance.

This subsection focuses on both normative and institutional responses under the multilateral framework of the WTO, PTAs, DEAs and other regional trade bodies. Ideally, a multilateral approach is the best forum to address trade-related concerns on cross-border data flows as it reduces transactional costs, benefits from the long-standing rules-based framework of the WTO and provides a

[14] F Casalini, 'Cross-Border Data Flows – Taking Stock of Key Policies and Initiatives' (OECD, 2022) 16–17.

[15] See, eg U Ahmed, 'The Importance of Cross-Border Regulatory Cooperation in an Era of Digital Trade' (2019) 18(S1) *World Trade Review* s99; JP Meltzer, 'Governing Digital Trade' (2019) 18(S1) *World Trade Review* s23; PF Cowhey and JD Aaronson, *Digital DNA: Disruption and the Challenges for Global Governance* (Oxford, Oxford University Press, 2017); Mishra, 'Building Bridges' (n 10); AD Mitchell and N Mishra, 'Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute' (2019) 22(3) *Journal of International Economic Law* 389; AD Mitchell and N Mishra, 'Data at the Docks: Modernizing International Trade Law for the Digital Economy' (2018) 20(4) *Vanderbilt Journal of Entertainment & Technology Law* 1073; M Burri, 'New Legal Design for Digital Commerce in Free Trade Agreements' (2017) 107(3) *Digiworld Economic Journal* 1, 2, 5.

relatively powerful voice to developing countries. Nonetheless, existing political difficulties currently plague the multilateral framework of the WTO.[16] I have also discussed in previous chapters various practical difficulties in arriving at a clear multilateral consensus in specific areas of data regulation, especially in the short term. For instance, it is quite difficult to arrive at a common consensus among WTO members on issues such as data certification mechanisms for personal data transfers, competition regulation for data-driven sectors and principles for governmental access to data. The consensus mechanisms developed under the PTA and DEA frameworks will therefore be important at least in the short run to work towards incremental, long-term solutions at the multilateral level.

Besides the divergence among WTO members regarding the moratorium on customs duties on electronic transmissions,[17] even the member proposals and drafts being discussed at the plurilateral Joint Initiative on Electronic Commerce (Joint Initiative) reveal stark differences of opinion among countries.[18] For instance, it is still unclear how members will schedule commitments on service sectors under the new plurilateral agreement, especially with developing countries being reluctant to open up their markets to new digital sectors.[19] Several WTO members have disagreed on the scope and relevance of the exceptions for the digital world.[20] For instance, Nigeria has proposed expanding the policy space for LDCs and developing countries so that they can implement digital industrial policies, including data localisation laws,[21] while New Zealand has requested wide exceptions for indigenous peoples' data.[22] China has made a proposal for self-judging security exceptions to protect the cyber sovereignty of members.[23]

Given these differences, PTAs and DEAs can be feasible options to execute, at least in the short run.[24] Further, it may be easier to address and incorporate

[16] See generally P Low, 'The WTO in Crisis: Closing the Gap between Conversation and Action or Shutting Down the Conversation?' (2022) 21(3) *World Trade Review* 274.

[17] WTO Work Programme on Electronic Commerce, 'Ministerial Decision' (22 June 2022) WT/MIN(22)/32 – WT/L/1143; see also WTO, 'WTO Members Intensify Discussion on e-Commerce Moratorium' (18 July 2023) www.wto.org/english/news_e/news23_e/ecom_18jul23_e.htm.

[18] For accessing the available documents pertaining to joint initiative on e-commerce, see WTO, 'Joint Initiatives', www.docs.wto.org/dol2fe/Pages/FE_Browse/FE_B_009.aspx?TopLevel=10785.

[19] WTO, Exploratory Work on Electronic Commerce, 'Non-paper from Brazil' (25 March 2019) INF/ECOM/3, 4.4, 4.13; WTO, Joint Statement on Electronic Commerce, 'Communication from Brazil' (25 March 2019) INF/ECOM/17; WTO, Joint Statement on Electronic Commerce, 'Communication from China' (24 April 2019) INF/ECOM/19.

[20] WTO, Exploratory Work on Electronic Commerce, 'Non-paper from Brazil' (n 19) 4.4, 4.13.

[21] WTO, Electronic Commerce Negotiations, 'Updated Consolidated Negotiating Text – September 2021' (8 September 2021) INF/ECOM/62/Rev.2.

[22] WTO, Joint Statement on Electronic Commerce, 'Communication from Côte d'Ivoire' (25 November 2022) INF/ECOM/70.

[23] WTO, Joint Statement on Electronic Commerce, 'Communication from China' (9 May 2019) INF/ECOM/32.

[24] MD Froese, 'Digital Trade and Dispute Settlement in RTAs: An Evolving Standard?' (2019) 53(5) *Journal of World Trade* 783, 785–86. As compared to traditional FTAs, most DEAs have been

new disciplines in some emerging and complex areas, such as competition policy and data standards, in PTAs and DEAs than in WTO law, where convergence among diverse groups of countries is unlikely in the short term. Nonetheless, discussions at the WTO would also benefit from ideas of successful regulatory models from the PTAs and DEAs.[25]

As discussed in the previous chapters in different contexts, there is a considerable degree of fragmentation across PTAs on different aspects of regulating data flows.[26] Another potential risk of the growing network of PTAs and DEAs is the formation of powerful exclusionary clubs, which may exclude certain countries, particularly ones that are developing and/or have non-democratic political systems. To avoid such fragmentation and exclusions, the proposals underlined below take into account how PTAs can facilitate gradual regulatory alignment. While some reforms suggested below are likely to be operationalised faster by groupings of more open, liberal and digitally advanced economies, it is important to avoid widespread fragmentation or exclusionary structures in the global regulatory framework for digital trade. Further, certain policy aspects, such as bridging the global data divide, would be best addressed (at least eventually) under a multilateral framework such as the WTO instead of isolated efforts in PTAs and DEAs.

(i) Meaningful Use of Existing Trade Disciplines

(a) Transparency and Notification of Data-Restrictive Measures

Recent years have seen various initiatives to map the complex regulatory landscape of data regulations.[27] Although data-restrictive measures are now common, they are often implemented in a non-transparent and vague manner by governments. A clearer understanding of the different types of data-restrictive measures and their trade-restrictive impact is a helpful starting point to understanding how international trade law can address them.

The provisions on transparency contained in international trade treaties can be relevant here. For instance, under GATS, Article III, WTO members are bound to: (i) publish all domestic measures and signed international agreements

negotiated in a very short span of time, ranging from few months to about a year. The fact that these DEAs are developed as digital-only agreements and provide multi-track soft law solutions is an added advantage. See N Mishra, 'Digital Economy Agreements as a Response to Digital Trade Fragmentation' (Working Paper, presented at the SIEL Biennial Conference 2023, copy on file with the author).

[25] D Ciuriak and R Fay, 'The Digital Economy Partnership Agreement: Should Canada Join?' (2022) CIGI Policy Brief No 171.

[26] See generally I Willemyns, *Digital Services in International Trade Law* (Cambridge, Cambridge University Press, 2021) 287–335.

[27] See, eg 'Digital Policy Alert', www.digitalpolicyalert.org/; R Chen, 'Mapping Data Governance Legal Frameworks Around the World – Findings from the Global Data Regulation Diagnostic' (2021) World Bank Policy Research Working Paper 9615.

pertaining to or affecting trade in services;[28] (ii) inform the Council for Trade in Services (a subsidiary body of the WTO facilitating the operation of GATS) of new measures or changes to existing measures affecting trade in services;[29] and (iii) establish enquiry points to respond to queries from other members regarding their measures or international agreements pertaining to trade in services.[30] These rules are, however, underutilised.[31] Transparency obligations are also common in trade in services chapters and electronic commerce chapters of PTAs.[32]

In the digital context, the transparency obligation would essentially require all WTO members or PTA parties to provide details regarding how they regulate cross-border data flows, including certifications/regulatory approvals required for data transfers, technical standards for data processing and the regulatory criteria for blocking certain digital services or data transfers. Some scholars have argued that the disciplines on transparency can be used to provide more clarity regarding bilateral arrangements for data transfers among countries.[33]

Another tool to ensure more transparency is the Trade Policy Review Mechanism,[34] though there are other, similar monitoring mechanisms under PTAs. Scholars have also discussed the different ways in which notification of Specific Trade Concerns by the Technical Barriers to Trade (TBT) committee has helped members bring up different concerns regarding technical regulations and standards, and even resolve some of these concerns through consultations.[35] Such a mechanism, however, is not available for trade in services. A Reference Paper signed by 67 WTO members on domestic services regulation in 2021 also contains extensive transparency requirements for governments imposing specific requirements for the authorisation of services.[36] Thus, at the outset, trade bodies must utilise better the existing transparency and notification mechanisms contained in international trade law.

With increased transparency and notification of data-restrictive measures, trade bodies – especially multilateral bodies such as the WTO – can create a

[28] GATS, Art III:1.

[29] ibid Art III:3.

[30] ibid Art III:4.

[31] M Halle and R Wolfe, 'A New Approach to Transparency and Accountability at the WTO' (IISD, 2010) ENTWINED Issue Brief No 6, 3.

[32] For detailed mapping of provisions in Electronic Commerce Chapters in PTAs, see University of Lucerne, 'TAPED – A Dataset on Digital Trade Provisions', www.unilu.ch/en/faculties/faculty-of-law/professorships/burri-mira/research/taped/.

[33] A Mattoo and JP Meltzer, 'International Data Flows and Privacy: The Conflict and Its Resolution' (2018) 21(4) *Journal of International Economic Law* 769, 788.

[34] WTO, 'Trade Policy Reviews: Ensuring Transparency', www.wto.org/english/thewto_e/whatis_e/tif_e/agrm11_e.htm.

[35] TJ Bollyky and PC Mavroidis, 'Trade, Social Preferences and Regulatory Cooperation: The New WTO-Think' (2017) 20 *Journal of International Economic Law* 1, 10; S Lester and I Manak, 'A Proposal for a Committee on National Security at the WTO' (2020) 30(2) *Duke Journal of Comparative & International Law* 267, 269.

[36] WTO, Declaration on the Conclusion of Negotiations on Services Domestic Regulation (2 December 2021) WT/L/1129.

catalogue of data-restrictive measures imposed by their members, thus providing more visibility to both policy-makers and companies engaging in digital trade. This initiative would be particularly helpful for micro, small and medium enterprises, who often lack the resources to keep track of compliance requirements across jurisdictions, as well as developing countries that are currently in the process of building their own regulatory frameworks. Further, such information can be used to develop certain informal benchmarks for data-restrictive measures and enable discussions in relevant committees regarding the most harmful kinds of such measures. This information can at least be fruitful in seeking political resolution of sensitive data sovereignty-related disputes between countries, as discussed in chapters three and four in the context of cybersecurity and data access measures respectively.

(b) Mutual Recognition and Interoperability Mechanisms

Certain regulatory differences are inevitable in the context of data regulation. In some scenarios, however, mutual recognition can be a possible alternative because it enables different regulatory frameworks to interoperate, without requiring any drastic changes to domestic laws.[37] Further, if mutual recognition mechanisms are linked to market access, then they can facilitate trade flows.[38] While there is widespread industry support for mutual recognition mechanisms,[39] these mechanisms are usually much easier in areas where there is some degree of regulatory convergence (eg agreement on high-level principles) and/or if it can be defined well and carried out by specialised bodies.[40]

Some scholars have advocated that mutual recognition mechanisms can be useful for enabling cross-border data flows.[41] We have already seen some clear examples in PTAs; for instance, in certain PTAs, parties have recognised the APEC Cross-Border Privacy Rules (CBPR) as a valid instrument for enabling cross-border data transfers.[42] Some treaties also provide that parties will endeavour to negotiate mutual recognition mechanisms, such as trustmarks, to enable personal data transfers.[43] Currently, various countries are also discussing the facilitation of data flows for digital trade under the Global CBPR Forum,[44] building on the pre-existing APEC CBPR initiative, as discussed in chapter two.

[37] OECD, *International Regulatory Cooperation: Addressing Global Challenges* (2013) 16, 54.

[38] Bollyky and Mavroidis (n 35) 10.

[39] L Cernat, 'How Important Are Mutual Recognition Agreements for Trade Facilitation?' (December 2022) ECIPE Policy Brief No 10; ACD Brito et al, 'The Contribution of Mutual Recognition to International Regulatory Cooperation' (2016) OECD Regulatory Policy Working Papers No 2, 50.

[40] Brito et al (n 39) 12.

[41] Mattoo and Meltzer (n 33) 787–88.

[42] See, eg USMCA, Art 19.8.6; SADEA, Art 17.2.

[43] See, eg DEPA, Art 4.2.8.

[44] US Department of Commerce, 'Global Cross-Border Privacy Rules Declaration', www.commerce.gov/global-cross-border-privacy-rules-declaration.

For such mutual recognition mechanisms to be meaningful, it is important that they are inclusive, non-discriminatory and accessible/available to as many countries as possible, especially in the developing world.

In this regard, the WTO framework under GATS, Article VII is quite relevant, although it has been underutilised to date.[45] It provides that WTO members may recognise licences, certifications, etc granted by other members to ensure greater compatibility of 'standards or criteria for the authorization, licensing or certification of services suppliers'.[46] These arrangements, however, cannot be discriminatory or arbitrary in nature.[47] Thus, when a member enters into such mutual recognition arrangements with one member, other members have any 'adequate opportunity' to negotiate similar arrangements.[48] All mutual recognition agreements also need to be notified to the WTO.[49] Finally, this provision recognises the importance of using 'multilaterally agreed criteria' as a basis of mutual recognition and also provides an avenue for WTO members to cooperate with both intergovernmental and non-governmental bodies in the facilitation of common international standards and criteria for mutual recognition.[50]

While it currently seems like a distant goal in the context of data transfers, the above provision could become relevant in the multilateral context, once there is greater international consensus around specific data transfer mechanisms, data standards, privacy seals or other trustmarks. The consensus generated through the PTAs on mechanisms such as the APEC CBPR would be instrumental in that regard. In section IV, I highlight the need to conduct feasibility studies for mutual recognition and interoperable mechanisms in different areas of global data governance.

(ii) Formulating New Legal and Policy Interventions

International trade agreements have largely remained silent on several key issues of global data governance. While it is possible to extend the applications of existing provisions to matters related to cross-border data flows as discussed above, new legal and policy interventions are necessary to create more alignment between international trade law and global data governance. I discuss several proposals below. While each of these proposals can stand on its own, in an ideal

[45] In fact, the GATS, Art VII mechanism has only been used once in developing the *Guidelines for Mutual Recognition Agreements or Arrangements in the Accountancy Sector* which 'provide[s] practical guidance for governments, negotiating entities or other entities entering into mutual recognition negotiations on accountancy services'. See WTO (Council for Trade in Services), 'Guidelines for Recognition of Qualifications in the Accountancy' (28 May 1997) WT/S/L/38.

[46] GATS, Art VII:1.

[47] ibid Art VII:3.

[48] ibid Art VII:2.

[49] ibid Art VII:4.

[50] ibid Art VII:5.

scenario, trade policy-makers must combine as many of them as possible as they complement each other.

(a) A Non-binding Framework for Cross-Border Data Flows

Certain countries have now proposed that it might be helpful to develop a framework in international trade law that sets out high-level principles applicable to cross-border data flows. For instance, in the ongoing Joint Initiative at the WTO, certain members (eg Brazil and the EU) have made proposals for members to agree upon the core principles for cross-border data flows.[51] Similarly, the DFFT advocates for developing a regulatory framework on cross-border data flows (although it is a multi-track approach and not restricted to trade agreements).

While PTAs increasingly contain provisions on cross-border data flows and cover other related areas such as privacy protection and cybersecurity more extensively, there is no PTA incorporating a holistic principles-based framework for cross-border data flows. However, some aspects, such as data protection, are increasingly comprehensively covered in many PTAs and DEAs, including convergence on certain high-level principles. For instance, as discussed in chapter two, the Agreement between the United States of America, the United Mexican States, and Canada (USMCA) and several DEAs such as the Digital Economy Partnership Agreement (DEPA) incorporate the key principles on data protection, especially borrowing from the OECD Privacy Framework.

The first key question is what kind of provisions should such a framework contain. As I have discussed in the previous chapters, the regulation of cross-border data flows touches upon several sensitive and complex issues in both domestic regulation and transnational data governance. Various organisations, such as UN agencies, the OECD, APEC, regional bodies, transnational regulatory frameworks such as the ICN and GPA, and Internet multistakeholder bodies, have played key roles in formulating principles on different aspects of cross-border data governance.

In an ideal scenario, the framework for cross-border data flows must be developed based on distilling and assimilating the core principles of different aspects of the data governance found in the above legal and policy instruments. To be comprehensive and balanced, the Reference Paper/declaration should not only include principles related to data protection and data and network security,[52]

[51] WTO, Exploratory Work on Electronic Commerce, 'Non-paper from Brazil' (n 19) 1.2; WTO, Joint Statement on Electronic Commerce, 'Communication from the European Union' (12 July 2018) INF/ECOM/13.

[52] PF Cowhey and JD Aronson, 'Digital Trade and Regulation in an Age of Disruption' (2018) 22(1) *UCLA Journal of International Law and Foreign Affairs* 8, 12. Some countries, such as Japan, the USA, Korea and the UK, have also made proposals to include a risk-based approach to cybersecurity in the ongoing WTO plurilateral discussions on e-commerce. See WTO, Electronic Commerce Negotiations, 'Updated Consolidated Negotiating Text – September 2021' (n 21).

but also reflect shared norms among members on complex issues such as governmental access to data, digital competition, data interoperability,[53] data sharing and data ethics. However, agreeing upon high-level principles in some new and underexplored areas such as competition and data access may be much harder than more established disciplines such as data protection. This is where policy developments in DEAs and PTAs will remain instrumental.

The above framework should also recognise the importance of addressing the digital and data divide as a concern cutting across different aspects of global data governance.[54] As chapter five outlines, the global data divide can be best addressed at the WTO; however, regional bodies comprising developing countries as well as international development agencies must also have an active voice in shaping the high-level principles for cross-border data flows. For instance, the framework could incorporate a principle acknowledging the need to bridge the global data divide and promote digital inclusion. Borrowing from international environmental law, the framework could also acknowledge that the development of fair and robust global data markets is a shared but differentiated responsibility. Such high-level principles could eventually provide the legal basis for developing a tailored special and differential treatment (SDT) mechanism for digital trade, as proposed in chapter five.

The OECD outlines the core components of a good regulation, which includes: identification and effective achievement of clear policy goals; a sound legal and empirical basis; benefits outweigh the costs of regulation; clarity and simplicity; and compatibility with competition, trade and investment-facilitating principles at the domestic and international levels.[55] Trade policy-makers must consider such factors in developing the principles and guidelines in the above-suggested framework. This is especially because governments are likely to rely upon such a framework and use it as a guideline for developing domestic regulations on data flows. Eventually, if more governments adhere to these principles, it can also facilitate interoperability between different domestic regulatory frameworks. The framework can also be a helpful complement to existing trade agreements and inform ongoing initiatives such as the Joint Initiative or the DFFT. It can also be practically relevant in the long run. For instance, it could provide some helpful context in applying the exceptions to justify data-restrictive measures. Moreover, even developed in the multilateral context, it can also be incorporated voluntarily by PTA or DEA parties.

[53] Some of these issues have also been identified by WTO members in the Joint Initiative on Electronic Commerce. For instance, Brazil had recommended provisions on competition policy in an earlier draft. Certain members, such as the EU and the UK, have proposed including a provision on competitive safeguards in the telecommunications sector. See WTO, 'Electronic Commerce Negotiations – Consolidated Negotiating Text' (14 December 2020) INF/ECOM/62/Rev.1.

[54] See, eg WTO, Joint Statement on Electronic Commerce, 'Communication from China' (n 19) (this proposal, however, only proposes a voluntary obligation for SDT).

[55] OECD, 'Guiding Principles for Regulatory Quality and Performance' (29 October 2008) 3.

The next question is the form/architecture of the framework. While some proposals use the Reference Paper on Telecoms as a reference (in other words, members can voluntarily sign up to it), other scholars have suggested alternatives such as developing a non-binding WTO declaration.[56] The most feasible form in the current scenario is a non-binding WTO declaration or a voluntary instrument that WTO members can sign up to. The voluntary or non-binding nature of this instrument does not necessarily reduce its normative appeal. For instance, countries would have the incentive to follow the principles of this framework as it would reduce trade costs, facilitate a robust domestic regulatory framework and generate new opportunities for domestic digital service suppliers and consumers. Ideally, the declaration should also contain a clause outlining a clear mechanism for WTO members/signatories to revisit the principles on an ongoing basis and update it as and when needed. Further, in developing this framework, it is essential to consult relevant stakeholders, including the private sector, civil society and technical bodies. While the WTO would be the body that oversees these consultations, other organisations such as the OECD and ASEAN, Internet policy bodies such as the Internet Governance Forum, regional organisations in the developing world or UN agencies could play a supportive role.

WTO members have in the past relied upon non-binding instruments in other fields of trade regulation. For instance, the Understanding on Commitments on Financial Services is a non-binding WTO document that has informed how several WTO members have structured their GATS commitments on financial services.[57] An example of a successful initiative outside the WTO is the Santiago Principles developed by the International Working Group of Sovereign Wealth Funds, comprising various agencies and banks administering Sovereign Wealth Funds.[58] Although these principles are non-binding, they have been endorsed by the International Monetary Fund and play a central role in the management of Sovereign Welfare Funds in various countries.[59]

(b) Balanced Provisions on Cross-Border Data Flows and Data Localisation

Chapter two discussed the increase in binding provisions in PTAs on cross-border data flows and data localisation. Some scholars have argued that PTA provisions are more effective in liberalising data flows as they apply across all

[56] Mitchell and Mishra, 'Regulating Cross-Border Data Flows' (n 15) 405–06.

[57] WTO, 'Understanding on Commitments in Financial Services', www.wto.org/english/tratop_e/serv_e/21-fin_e.htm.

[58] International Working Group of Sovereign Wealth Funds, 'Sovereign Wealth Funds – Generally Accepted Principles and Practices – Santiago Principles' (October 2008).

[59] J Chaisse and M Matushita, 'Maintaining the WTO's Supremacy in the International Trade Order: A Proposal to Refine the Role of the Trade Policy Review Mechanism' (2013) 16(1) *Journal of International Economic Law* 9, 13.

service sectors, unlike GATS, where several obligations apply on a sector-by-sector basis.[60] However, PTA provisions are also subject to non-conforming measures listed in the parties' schedule.

The lack of explicit provisions on cross-border data flows and data localisation in the WTO *acquis* poses various legal uncertainties, as discussed in earlier chapters. Therefore, in an ideal scenario, there must be an express provision on cross-border data flows and data localisation applicable to WTO members. Several countries have proposals in the ongoing WTO Joint Initiative on this aspect, consistent with their PTA practices on data flows and data localisation. In the current political climate, several countries might be reluctant to adopt a broad cross-sectoral obligation on cross-border data flows or data localisation. However, it is still important to consider the possible ways in which this provision can be designed.

The foremost consideration in developing a provision on cross-border data flows and data localisation is achieving the right balance between enabling data flows and protecting important public policy concerns. Certain DEAs, such as DEPA, provide good ideas. For example, the provisions on cross-border data flows are contained in the same module as privacy protection, thus recognising the inextricable link between data protection and cross-border data flows.[61] It is also important than any obligations on data flows or data localisations are qualified with clear and flexible exceptions allowing the data-restrictive measures necessary to achieve domestic public policy objectives.

While it is possible to incorporate the general and security exceptions found in WTO treaties by reference to any horizontal rules on cross-border data flows or data localisation, the exception can also be tailored more specifically in the Joint Initiative. For instance, as discussed in chapter three, the security exception can explicitly include cybersecurity-related risks. Further, as discussed in chapter four, the data localisation provision must be qualified by a provision permitting governments to request companies to provide access to data on legitimate grounds (following due process), irrespective of the location of data. Additionally, as discussed in chapter two, if WTO members choose to adopt a broad general exception like the one in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) referring to 'legitimate public policy objectives', they can consider adding an illustrative list of policy objectives to ensure WTO panels have sufficient guidance on interpreting which policy objectives qualify as legitimate public policy objectives.[62] Finally, members might need to consider if specific language needs to be inserted to address developing country

[60] M Burri, 'The Regulation of Data Flows Through Trade Agreements' (2017) 48(1) *Georgetown Journal of International Law* 407, 443.

[61] See DEPA, Module 4 (covering provisions on cross-border data flows, data localisation and personal information protection).

[62] N Mishra, 'The Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance?' (2017) 20(1) *Journal of International Economic Law* 31, 39.

concerns such as adopting digital industrial policies or at least providing more flexibilities to LDCs, as discussed in chapter five.

As the discussions in previous chapters suggest, the exceptions contained in trade agreements, particularly very broadly worded and flexible ones, can be misused by governments to disguise protectionist data-restrictive measures. At the same time, several countries impose data-restrictive measures to pursue important domestic policy objectives, and the lack of trust in the digital ecosystem often exacerbates the use of such measures. In that regard, the non-binding framework proposed in section IIIB2a can provide baseline principles on different aspects of global data governance, especially data protection and cybersecurity.[63] This can help create more trust between countries and minimise the use of exceptions to exceptional circumstances.

Some other pragmatic issues must also be resolved in the context of adopting horizontal disciplines on data flows and data localisation in the plurilateral agreement on e-commerce at the WTO. For example, existing GATS Schedules of members would need to be read consistently with horizontal commitments on data flows/data localisation. For instance, certain members may choose to revise their Schedule to reflect their understanding on data-driven services or undertake additional commitments under GATS, Article XVIII. Further, members will need to decide if they can permit these obligations to apply on a most-favoured nation (MFN) basis to all other WTO members (including those who have not undertaken similar commitments) or should take a new route, such as a non-MFN-based plurilateral agreement.[64]

(c) A Standards Framework for Data-Driven Technologies

In addition to explicit data restrictions, data flows are also restricted by mandatory requirements imposed by governments to use incompatible, indigenous technical standards in digital and data-driven technologies. As previous chapters discussed in detail, no clarity exists regarding the relevance of technical standards developed outside state-driven bodies in the context of digital services in international trade law. However, several important and globally recognised standards and protocols in relation to data security and privacy, data exchange and data classification are developed in multistakeholder or industry bodies.[65] To ensure that such standards remain relevant in assessing the reasonableness and necessity of standards under international trade law (such as under GATS,

[63] See also R Wolfe, 'Learning About Digital Trade: Privacy and e-Commerce in CETA and TPP' (2019) 18(S1) *World Trade Review* s63, s78; Cowhey and Aaronson, *Digital DNA* (n 15) 234–36.

[64] See Mitchell and Mishra, 'Data at the Docks' (n 15) 1127–29.

[65] See, eg GitLab, 'GitLab Data Classification Standard', https://about.gitlab.com/handbook/security/data-classification-standard.html#:~:text=The%20Data%20Classification%20Standard%20defines,GitLab%20data%20throughout%20its%20lifecycle; Open Standards for Data, 'Types of Open Standards for Data', https://standards.theodi.org/introduction/types-of-open-standards-for-data/; resources.data.gov, 'Data Standards', https://resources.data.gov/standards/.

Article VI) or to improve the prospects for technical interoperability and cooperation, a standards framework for data-driven technologies must be developed in international trade law. This proposal is especially pertinent as disciplines on trade in services under GATS and PTAs do not contain concrete provisions on standard setting.[66]

WTO's experience in implementing the TBT and sanitary and phytosanitary measures agreements is a helpful starting point. As discussed earlier, the WTO can play a more instrumental role in cataloguing different kinds of data-restrictive measures. This can also help in cataloguing the best practices and technical standards used in digital services and technologies. Further, the core principles of standard-setting set out in the TBT Agreement, namely transparency, openness, impartiality, consensus, effectiveness, relevance, coherence and incorporating a development perspective, would be equally applicable in the digital context. Standard-setting bodies often take into account these TBT principles in developing their standards.[67] In particular, it is necessary that the benchmarks for relevant standards and standard-setting bodies require scrutiny of the model of participation/design formulation, especially stakeholders from developing countries. The standards framework developed in the context of digital and data-driven services can also be incorporated as a part of the non-binding framework on cross-border data flows, discussed in a previous section.

The growing importance of private and industry standards for data-driven services and technologies presents a particularly complex challenge.[68] As these standards are developed in a manner different from traditional standard-setting bodies such as the ISO,[69] international trade law must address how to take them into account, if and when relevant in assessing specific data-restrictive measures. The same TBT principles must apply in the context of private standards, even if such standards have become the de facto market standard.

To address some of these challenges on standard-setting, Girard has recommended constituting an independent body called the Digital Standards Task Force, which would create a single data area with common standards, taking

[66] The UKSDEA contains a dedicated provision on standards and conformity assessment, setting out high-level obligations for cooperation in setting technical standards and conformity assessment procedures relevant to digital trade, but does not set any clear principles or mechanisms to operationalise international cooperation. See UKSDEA, Art 8.61D. However, both these countries have signed a separate memorandum on cybersecurity cooperation to engage in further dialogues on relevant issues. See UK Government, 'Memorandum of Understanding on Cyber Security Cooperation', www.gov.uk/government/publications/memoranda-of-understanding-with-singapore-digital-trade-facilitation-digital-identity-and-cyber-security/memorandum-of-understanding-on-cyber-security-cooperation.

[67] See, eg IEEE, 'IEEE Position Statement – IEEE Adherence to the World Trade Organization Principles for International Standardization' (19 August 2020).

[68] M Girard, 'Big Data Analytics Need Standards to Thrive – What Standards Are and Why They Matter' (2019) CIGI Papers No 2091.

[69] For an overview of the standard-setting process in leading SDOs, see ibid.

into account both technical and policy aspects.[70] However, such an initiative must be treated with caution especially in the context of the WTO, because it may easily exclude voices of developing countries. While it is important for countries to adopt the most competitive standards in the context of data-driven technologies, standards should not be considered credible if they are developed and implemented without the participation of sufficient voices from the developing world.

(d) Incorporating Multistakeholder and Transnational Norms and Best Practices

In addition to standards, I also discussed in previous chapters the evolution of norms and regulatory practices in data governance in various transnational regulatory networks, regional bodies and multistakeholder organisations. However, the role of such norms and best practices in the context of international trade law is currently unclear. Although certain DEAs have expanded the scope of engagement, for instance by providing for consultation with civil society bodies and participation in relevant multistakeholder bodies in areas such as digital inclusion and online safety and cybersecurity,[71] these provisions are also mostly cursory.

To align international trade law and global data governance, it will be critical for international trade agreements to refer to evolving norms and best practices in a variety of non-trade bodies: (i) by inserting clear provisions that allow reference to relevant norms and regulatory practices developed by multistakeholder bodies and transnational regulatory bodies; and (ii) by broadening the permissible scope of international regulatory cooperation to include different forms of international, transnational and multistakeholder engagement. These provisions may be implemented more quickly in PTAs and DEAs among like-minded trading partners rather than at the WTO level. But even at the WTO level, such provisions have a significant value to add as they can leave the policy space open for considering a broader range of data governance norms and practices in the application/interpretation of WTO treaties.

In incorporating relevant transnational and multistakeholder norms and practices by reference in international trade law, it is important that whatever is incorporated by reference is robust, effective and representative. Thus, similar to the standards framework explained above, a legal threshold is necessary to scrutinise both the input and output legitimacy of the said norms and regulatory practices. This is especially the case as legitimacy and accountability are lingering concerns in multistakeholder or transnational processes.[72] In particular,

[70] M Girard, 'Standards for Digital Cooperation' (2020) CIGI Papers No 237.

[71] Mishra, 'Digital Economy Agreements' (n 24).

[72] J Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (2008) 2(2) *Regulation & Governance* 137.

norms and regulatory bodies emerging from exclusionary, club-like bodies often wilfully exclude stakeholders in developing countries.

I have discussed several examples previously where specific transnational regulatory bodies or multistakeholder bodies, including the GPA, ICN, APEC, G20 and OECD, have provided normative frameworks or best practices on different aspects of data regulation.[73] Certain aspects of data governance, such as the importance of access to information and choice of services to Internet users, importance of innovation and generativity on the Internet, achieving interoperable and competitive cybersecurity standards, and incorporating fundamental data protection principles in the technical designs of digital services, are well discussed by multistakeholder Internet bodies.[74] Some of these aspects have also been covered in PTAs and DEAs.[75] The OECD Principles for Internet Policymaking, formulated through a multistakeholder process and endorsed by 34 countries, sets principles for developing a free and open Internet and balancing various policy concerns, such as privacy, security, intellectual property protection and the free flow of information.[76] The G20 members have also endorsed the DFFT, as discussed earlier. I have also indicated in chapter five both the scope and need for regional bodies such as the African Union, ASEAN and the Pacific Alliance to offer frameworks and policy ideas for supporting developing countries and LDCs, and for bridging the global data divide.

Certain scholars argue that using soft law norms and best practices originating in non-treaty institutions such as transnational regulatory frameworks (termed 'informal international law') can be relevant in applying and interpreting international law.[77] Despite the informality of actors, processes and outputs in informal international law, it is followed extensively[78] while remaining flexible, agile and adaptable to complex policy and technological changes.[79] This approach can be particularly helpful for developing disciplines on data flows[80]

[73] J Wouters and D Geraets, 'The G20 and Informal International Lawmaking' in A Berman et al (eds), *Informal International Lawmaking: Case Studies* (Torkel Opsahl Academic EPublisher, 2012) 19, 22; M Matsushita, 'A View on Future Roles of the WTO: Should There Be More Soft Law in the WTO?' (2014) 17(3) *Journal of International Economic Law* 701, 711, 713.

[74] See generally Mishra, 'Building Bridges' (n 10).

[75] See, eg CPTPP, Art 14.10 (discussing principles for access to the internet); DEPA, Arts 2.2, 2.5 (discussing the relevance of interoperable standards for paperless trading and e-invoicing); USMCA, Art 18.8.3 (incorporating OECD privacy principles in the text); UKSDEA, Art 8.61I (focusing on promoting data innovation).

[76] OECD, 'Recommendation on Internet Policy Making Principles' (2014) 4.

[77] See generally Wouters and Geraets (n 73); J Pauwelyn et al (eds), *An Introduction to Informal International Lawmaking* (Oxford, Oxford University Press, 2012).

[78] J Pauwelyn et al, 'When Structures Become Shackles: Stagnation and Dynamics in International Lawmaking' (2014) 25(3) *European Journal of International Law* 733, 743–44.

[79] ibid; see also A Mckay et al, 'International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World' (Microsoft, 2015) 19.

[80] See, eg F Casalini et al, 'A "Digital" Convention to Protect Cyberspace?' (International Economic Law Clinic, Trade Lab, 18 January 2018) 10.

because, in complex and delicate areas of global data governance, flexible, soft law norms will be more acceptable to countries than binding and inflexible rules contained in treaties.[81]

The second important element is developing international regulatory cooperation in the broadest way possible. Scholars have pointed out that regulatory cooperation is like an accordion,[82] and the OECD has listed a range of mechanisms that can qualify as regulatory cooperation: harmonisation, specific treaties/agreements, regulatory partnerships, intergovernmental organisations, regional agreements, mutual recognition agreements, transnational regulatory networks, requirements to incorporate by reference, recognition of international standards, soft law and policy dialogues.[83] In the context of cross-border data flows, international regulatory cooperation must be understood broadly: cooperation among governments and regulators, different international/regional organisations, and regulators and non-state entities such as multistakeholder Internet bodies. Transnational bodies (eg those consisting of regulatory agencies) can also play a key role as they have specialised expertise.[84]

International regulatory cooperation has many advantages, such as ensuring more accountability and transparency, reducing discriminatory practices (especially unilateral practices) and supporting interoperability of technological standards and regulatory frameworks.[85] It also optimises resources spent on dealing with individual issues in different fora.[86] Some scholars have argued that disciplines on regulatory cooperation could lead to stronger compliance with international trade agreements.[87] For example, international regulatory cooperation is essential in developing mutual recognition agreements under GATS, Article VII. Further, dialogues on establishing cooperation mechanisms can help determine baseline regulatory frameworks in relevant areas of digital trade.

[81] UN, 'The Age of Digital Interdependence: Report of the UN Secretary-General's High-Level Panel on Digital Cooperation' (New York, 2019) 31.

[82] Bollyky and Mavroidis (n 35) 3.

[83] Brito et al (n 39) 14.

[84] See generally A Berman, 'Industry, Regulatory Capture and Transnational Standard Setting' (2017) 111 *AJIL Unbound* 112, 113; G Teubner and P Korth, 'Two Kinds of Legal Pluralism: Collision of Transnational Regimes in the Double Fragmentation of World Society' in MA Young (ed), *Regime Interaction in International Law: Facing Fragmentation* (Oxford, Oxford University Press, 2012) 23, 26–31, 53.

[85] E Benvenisti, 'Upholding Democracy Amid the Challenges of New Technology: What Role for the Law of Global Governance?' (2018) 29(1) *European Journal of International Law* 9, 14. F Casalini et al, 'Approaches to Market Openness in the Digital Age' (2019) OECD Trade Policy Papers No 219, 16.

[86] Bollyky and Mavroidis (n 35) 3.

[87] See, eg E Sheargold and AD Mitchell, 'The TPP and Good Regulatory Practices: An Opportunity for Regulatory Coherence to Promote Regulatory Autonomy' (2016) 15(4) *World Trade Review* 587; S Peng, 'The Rule of Law in Times of Technological Uncertainty: Is International Economic Law Ready for Emerging Supervisory Trends?' (2019) 22(1) *Journal of International Economic Law* 1, 18; WTO, *World Trade Report 2018* (2018) 132.

Trade partners may also rely upon other external mechanisms, such as bilateral understandings in sensitive areas.[88]

International trade law already provides various avenues for international regulatory cooperation, but some of them remain under-used. For instance, Article V of the WTO Agreement allows the General Council (consisting of representatives from all WTO members) to cooperate and consult with both other intergovernmental organisations and non-governmental bodies.[89] Wolfe has emphasised the importance of informal learning within the WTO and emphasised the importance of funding and organising thematic sessions at the WTO to understand complex and emerging issues in international trade law, especially encouraging active participation from developing countries.[90] Such informal models of regulatory cooperation can be particularly instrumental in better understanding the possible areas of regulatory convergence in difficult areas of data regulation.[91]

As an example, Meltzer argues that regulatory cooperation on privacy achieved in regional bodies such as the APEC or OECD can be integrated into existing trade disciplines, for example, by incorporating their guidelines or principles by reference in international trade agreements.[92] This solution appears controversial at first sight as the APEC or OECD privacy frameworks are not universally considered representative or robust. However, this mechanism is intended to ensure that trading partners adopt baseline regulations that are interoperable and functional but does not deter them from adopting higher standards in their domestic laws. In fact, regulatory cooperation, especially among countries with evolved regulatory frameworks, could lead to widespread adoption of high-quality international standards and best practices in cybersecurity and privacy.

Although regulatory cooperation efforts are happening in different international and regional fora, the WTO, as an institution with a membership of 164 members, has a special role as a site for information exchange and encouraging

[88] See, eg Australian Government, 'Australia and the Republic of Korea Sign New MoU on Cyber and Critical Technology Cooperation', www.internationalcybertech.gov.au/Australia-and-Korea-sign-MoU; Australian Government, 'Australia and Indonesia Sign an Expanded MoU on Cyber and Emerging Cyber Technology Cooperation', www.internationalcybertech.gov.au/Australia-and-Indonesia-sign-MoU; Australian Government, 'Australia–India Cyber and Critical Technology Partnership (AICCTP)', www.internationalcybertech.gov.au/our-work/AICCTP; E Yu, 'Singapore to Collaborate with Australia on Cybersecurity' (ZDNet, 04 June 2017) www.zdnet.com/article/singapore-to-collaborate-with-australia-on-cybersecurity/.

[89] WTO Agreement, Art V. But see GATS, Art XXVI, which has a limited scope and states that the General Council can make 'appropriate arrangements for consultation and cooperation with the United Nations and its specialized agencies as well as with other intergovernmental organizations concerned with services'.

[90] R Wolfe, 'Informal Learning and WTO Renewal: Using Thematic Sessions to Create More Opportunities for Dialogue' (2021) 12(S3) *Global Policy* 30, 37.

[91] See, eg Mattoo and Meltzer (n 33); Meltzer (n 15); Ahmed (n 15) s100–s101; Mitchell and Mishra, 'Regulating Cross-Border Data Flows in a Data-Driven World' (n 15).

[92] Meltzer (n 15) s47–s48.

cooperation, such as through discussions and the exchange of relevant information in Committee meetings and the Work Programme on Electronic Commerce. Thus, it can indirectly support regulatory cooperation in other international/regional/transnational bodies. It can also play a vital role in disseminating information on relevant data laws and policies to developing countries, LDCs and other countries that are not members of bodies such as the OECD and APEC.

C. Institutional Mechanisms to Achieve Alignment

After exploring the normative frameworks to strengthen alignment between international trade law and global data governance, it is also necessary to consider the institutional mechanisms necessary to operationalise these frameworks. The discussion so far demonstrates that a multilayered approach necessitates involvement of both formal and informal legal mechanisms to address concerns in relation to cross-border data flows and digital trade. Therefore, the institutional framework must also complement this normative framework. While the existing committees and bodies in trade organisations can play a vital role in operationalising the normative framework, here I propose combining them with informal institutional mechanisms and experimental models of institutional cooperation to provide a holistic institutional response.

First, as noted earlier, existing trade committees (or new ones such as a proposed Committee on National Security, discussed in chapter three) play a critical role in fostering deliberations, exchanging information and generating some degree of consensus on important issues. In addition to the WTO, several PTAs and recent DEAs create committees that enjoy broad powers to deliberate on several issues. One core function of these committees should be monitoring provisions on data flows and data localisation to understand how these provisions are being implemented by parties and what the potential regulatory and policy roadblocks are in enabling cross-border data flows. In particular, these deliberative and consultation mechanisms are important for members to reach political agreements on sensitive issues rather than rely solely upon the dispute settlement fora of the PTA/WTO panel or resort to unilateral measures.

In addition to the treaty body committees, informal bodies could be important as they are inherently more flexible and can involve a greater number of stakeholders. For instance, such bodies can perform a supportive role to the WTO or other trade bodies in identifying relevant regulatory practices and soft law principles essential for cross-border data flows and can facilitate participation of non-state stakeholders, including Internet policy and technical bodies, standards development organisations and transnational regulatory bodies.

The WTO is increasingly more receptive to informal mechanisms. For instance, Pauwelyn discusses the initial successes of Trade and Environmental Sustainability Structured Discussions (with 71 members) and Informal Dialogue

on Plastics Pollution and Environmentally Sustainable Plastics Trade (with 76 members), both of which are aimed at fostering policy dialogues on tough environmental issues and involve multiple stakeholders.[93] Another example in the digital context is the Electronic World Trade Platform, a collaboration between the WTO, Alibaba and the World Economic Forum to foster public–private dialogue on rules affecting cross-border electronic commerce.[94] Under the DFFT, the government of Japan has recommended constituting an Institutional Arrangement for Partnership, a multistakeholder body discussing how trust issues can be addressed in the context of cross-border data flows.[95]

The experience of the World Health Organization (WHO) in dealing with non-state actors, including its 'Framework for Engagement with Non-state Actors',[96] is a helpful reference for trade bodies aiming to develop cooperation with multistakeholder/transnational bodies and the private sector.[97] Some key principles outlined in this framework include exercising due diligence (including checking the funding of the non-state actors, their agenda and degree of representativeness); ensuring accountability of processes; promoting transparent engagement; preventing conflict of interests; and mutual respect for institutional values.[98]

IV. MOVING TOWARDS A MULTILAYERED APPROACH: A FUTURE RESEARCH AGENDA

Multilayered approaches to digital regulation are not without its risks or challenges. In fact, scholars have pointed out that polycentric regulation inevitably raises questions of legitimacy and accountability.[99] Further, as several transnational/multistakeholder bodies are not clearly grounded in domestic or international law, there could be legal uncertainty where there is a conflict of jurisdictions.[100] Multistakeholder or transnational bodies may also suffer from the same participation constraints for developing countries and LDCs as for other state-based international organisations.[101]

[93] J Pauwelyn, 'Taking Stakeholder Engagement in International Policy-Making Seriously: Is the WTO Finally Opening Up?' (2023) 26(1) *Journal of International Economic Law* 51.

[94] 'Electronic World Trade Platform', www.ewtp.org.

[95] S Wood, 'Global Policy Makers Take Further Steps to Support Data Free Flow with Trust' (JDSupra, 19 May 2023) www.jdsupra.com/legalnews/global-policy-makers-take-further-steps-2406526/.

[96] WHO, 'Framework for Engagement with Non-state Actors' (28 May 2016) WHA69.10.

[97] Berman (n 84) 115.

[98] WHO, 'Framework for Engagement with Non-state Actors' (n 96) annex 4–7, 22, 27, 32.

[99] Black (n 72) 137.

[100] ibid 143.

[101] O Tene and JT Hughes, 'The Promise and Shortcomings of Privacy Multistakeholder Policymaking: A Case Study' (2014) 66(2) *Maine Law Review* 437, 452–56.

Despite the above constraints and challenges, it is increasingly clear that transnational legal mechanisms, especially the soft and informal international law that they generate, are important in creating trust-based solutions.[102] I have arrived at a similar conclusion regarding the significance of a multilayered framework in international trade law to address digital trade, which provides sufficient scope to accommodate soft law mechanisms, best practices and other forms of informal understanding between different stakeholders. However, policy-makers have not yet figured out the details regarding the implementation of such frameworks.

Below, I highlight two fundamental areas of research to carry this reform agenda forward in international trade law to address cross-border data flows: the development of legal/regulatory interoperability in international trade law and the building of new international legal models that combine multilateral rulemaking with multistakeholder processes.

Several proposals discussed above highlight the need to use interoperable solutions to address divergences across countries in data regulatory frameworks. Interoperability is often defined as the ability of different systems, working procedures, devices and organisational protocols to work together to achieve a common goal.[103] To date, the majority of discussions on interoperability have focused on technical interoperability; for instance, the ability of different kinds of hardware/software and computing systems such as digital platforms to engage in machine-to-machine communication, such as between two cloud computing systems, would be an example of technical interoperability.

There have also been several instances of technical interoperability solutions discussed in the digital trade context, especially in recent DEAs.[104] However, the reforms suggested in section IIIB also require at least a degree of legal or regulatory interoperability. This means that policy-makers need to identify norms, guidelines, mechanisms and/or institutions based on shared regulatory goals that enable different laws and regulations across countries to work with each other.

Operationalising interoperability in practice, however, needs further scrutiny. The first question would be to understand what the optimal level of interoperability should be in the context of cross-border data flows, ie how to facilitate data flows without compromising other objectives, including ensuring

[102] See generally R Hagemann, 'Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future' (2018) 17(1) *Colorado Technology Law Journal* 37, 99–100; G Shaffer and T Halliday, 'With, Within, and Beyond the State: The Promise and Limits of Transnational Legal Ordering' in Peer Zumbansen (ed), *The Oxford Handbook of Transnational Law* (Oxford, Oxford University Press, 2021).

[103] J Palfrey and U Gasser, *Interop: The Promise and Perils of Highly Interconnected Systems* (New York, MIT Press, 2012).

[104] See, eg DEPA, Art 2.2, 2.5 (discussing the relevance of interoperable standards for paperless trading and e-invoicing).

the security and privacy of digital services.[105] Similarly, we may also need to consider the extent to which interoperable legal solutions may harm developing country interests.

Second, in devising legal interoperability, we also need to consider the feasibility of options. For instance, if two countries have contrasting models of data protection law (say, Country A uses an accountability-based approach, while Country B uses an adequacy-based approach), how can these two models interoperate? Without answering such questions, it is impossible to create transnational legal or policy mechanisms for data transfers, such as certification mechanisms or trustmarks. To create such interoperable mechanisms, scholars need to engage in extensive regulatory mapping across jurisdictions and then conduct a careful legal exercise to distil the core principles that can be the basis of legal interoperability in different aspects of global data governance.

In developing principles for interoperability in the context of digital trade, it is also important to take into account the core principles of international trade law, such as non-discrimination, transparency and respecting the regulatory autonomy of different countries. Further, it is unclear if such interoperability-based solutions should be sector-specific or cross-cutting in nature. While this book does not cover these important questions, it is necessary to identify this as an important area of future research.

Second, the sections above propose a new vision for international trade law in the context of the digital economy. Instead of sticking to the traditional boundaries of a strictly treaty-based regime, I have examined flexible options that combine traditional multilateral rulemaking (eg binding treaty provisions) with a variety of multistakeholder processes, such as formulation of soft law, good regulatory practices and building consensus on technical standards and protocols. A key risk in this approach is that more digitally advanced countries are likely to form issue-specific clubs that operate in an exclusionary manner. For instance, several existing proposals regarding the formation of digital standards and data regulatory bodies are restricted to a few Western powers (the EU, the USA, Canada) and Japan, and often exclude China, India and the majority of smaller developing countries.[106] Therefore, instead of creating a cohesive international community for digital trade, these proposals can exacerbate the existing geopolitical divide in global data governance and appear counterproductive in the long run.[107] Further, as highlighted previously, outputs

[105] Palfrey and Gasser (n 103) 11, 81, 88.

[106] See, eg Cowhey and Aronson, 'Digital Trade and Regulation' (n 52) 28; For a proposal on an international data standards board, see P Leblond and SA Aaronson, 'A Plurilateral "Single Data Area" Is the Solution to Canada's Data Trilemma' (2019) CIGI Papers No 226. Another proposal was also put forward for a digital stability board. See M Emanuele, 'Towards the Digital Stability Board for a Digital Bretton Woods' (The Science of Where, 1 February 2021) www.thescienceofwhere-magazine.it/2021/02/01/towards-the-digital-stability-board-for-a-digital-bretton-woods/.

[107] N Mishra and K Kugler, 'The Emergence of an International Community in the Global Digital Economy' (AFIELN Conference Paper, 2023, unpublished, draft on file with the author).

from multistakeholder/transnational processes do not enjoy the same degree of legitimacy, accountability and public sanction as traditional treaty mechanisms, despite some of them enjoying what Pauwelyn and others have termed 'thick stakeholder consensus'.[108]

A pragmatic question that scholars must thus address is how to develop a more balanced and inclusive multilayered framework, taking into account the various constraints discussed above. This study would require specific consideration of how data regulations are being formulated in different regulatory networks and global organisations. Different questions must be addressed in that regard. For instance, should soft law derived from multistakeholder processes only play a complementary role? What should be the legal threshold to assess policy outputs of multistakeholder and transnational bodies? Should multistakeholder bodies engage in domestic politics? Should they play more clearly outlined roles as auditors in international lawmaking? Can they be effective certification bodies especially for cross-border data transfers? While several of these questions have been cursorily referred to in this chapter, there is a need to scrutinise them more intensively by using examples of real-world practices in global data governance.

V. CONCLUSION

International trade law is under immense pressure in the current times. Some have argued that the only response to this crisis is for the discipline to move in a new direction that looks beyond economic losses and gains.[109] A similar narrative is also shaping up in the context of regulating the global digital and data economy. This concluding chapter suggested various ways in which dialogues on cross-border data flows can be framed beyond traditional trade narratives to focus on a new multilayered approach, which puts cross-border regulatory alignment and international regulatory cooperation at the core of policy-making in digital trade. It also highlighted the need for international trade law to be more responsive to norm evolution in other fields such as global data governance. Both the WTO treaties and various PTA/DEA bodies can play an instrumental role in achieving these goals. But we also need more dramatic changes in normative and institutional frameworks to respond to the challenges of data-driven trade in the digital world.

Although the proposals suggested in this concluding chapter may seem both vague and ambitious at the same time, they are grounded in pragmatic considerations. In fact, while this book is specifically focused on cross-border

[108] Pauwelyn et al, 'When Structures Become Shackles' (n 78) 734.

[109] N Lamp, 'Toward Multipurpose Trade Policy? How Competing Narratives about Globalization Are Reshaping International Trade Cooperation' (IISD, 15 January 2023) www.iisd.org/articles/policy-analysis/multipurpose-trade-policy.

data flows, the broader conclusions regarding the need for developing multi-layered legal and policy responses would also apply to other aspects of digital trade, as well as trade in other kinds of goods and services. While it seems easy for governments to give in to inward-looking narratives on data governance and digital trade in the short run, we can ultimately hope that more governments will be inclined to view the core questions of this book from a long-term perspective and move towards more coherent, inclusive and sustainable approaches for building a global regulatory framework for digital trade and cross-border data flows.

Bibliography

BOOKS

Bacchus, J and Manak, I, *The Development Dimension Special and Differential Treatment in Trade* (Abingdon, Routledge, 2021)

Berman, A et al (eds), *Rethinking Participation in Global Governance* (Oxford, Oxford University Press, 2022)

Borchert, I, 'Addressing Impediments to Digital Trade: A New eBook' (*VoxEU*, 27 April 2021)

Bradford, A, *The Brussels Effect: How the European Union Rules the World* (New York, Oxford University Press, 2019)

Broeders, D, *The Public Core of the Internet: Towards an International Agenda for Internet Governance* (Amsterdam, Amsterdam University Press, 2016)

Bygrave, LA, *Data Privacy Law* (Oxford, Oxford University Press, 2014)

Couldry, N and Mejias, UA, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford, Stanford University Press, 2019)

Cowhey, PF and Aaronson, JD, *Digital DNA: Disruption and the Challenges for Global Governance* (Oxford, Oxford University Press, 2017)

Cremer, J et al, *Competition Policy for the Digital Era* (European Commission, 2019)

DeNardis, L, *The Internet in Everything: Freedom and Security in a World with No Off Switch* (New Haven, Yale University Press, 2020)

Hon, WK, *Data Localization Laws and Policy* (Cheltenham, Edward Elgar, 2017)

Hsieh, PL, *New Asian Regionalism in International Economic Law* (Cambridge, Cambridge University Press, 2021)

Kitchin, R, *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences* (London, Sage Publications, 2014)

Kuner, C et al (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford, Oxford University Press, 2020)

Marsden, P, *A Competition Policy for the WTO* (London, Cameron May, 2003)

Mueller, ML, *Networks and States: The Global Politics on Internet Governance* (Cambridge MA, MIT Press, 2010)

O'Hara, K and Hall, W, *Four Internets: Data, Geopolitics and the Governance of Cyberspace* (New York, Oxford University Press, 2021)

Palfrey, J and Gasser, U, *Interop: The Promise and Perils of Highly Interconnected Systems* (New York, MIT Press, 2012)

Pauwelyn, J et al (eds), *An Introduction to Informal International Lawmaking* (Oxford, Oxford University Press, 2012)

Schwab, K, *The Global Competitiveness Report* (WEF, 2018)

Shackelford, SJ, *Managing Cyber Attacks in International Law, Business, and Relations in Search of Cyber Peace* (Cambridge, Cambridge University Press, 2013)

Sieber-Gasser, C, *Developing Countries and Preferential Services Trade* (Cambridge, Cambridge University Press, 2016)

Smeets, M, *Adapting to the Digital Trade Era: Challenges and Opportunities* (WTO, 2021)

Stucke, ME, *Breaking Away: How to Regain Control Over Our Data, Privacy, and Autonomy* (New York, Oxford University Press, 2022)

Verhulst, SG and Young, A, *Open Data in Developing Economies – Toward Building an Evidence Base on What Works and How* (Capetown, African Minds, 2017)

Weiss, TG, *Global Governance, Why? What? When?* (Cambridge, Polity Press, 2013)
Willemyns, I, *Digital Services in International Trade Law* (Cambridge, Cambridge University Press, 2021)
Wu, T, *The Curse of Bigness: Antitrust in the New Gilded Age* (New York, Columbia Global Reports, 2018)
Zuboff, S, *The Age of Surveillance Capitalism* (New York, Public Affairs, 2019)

BOOK CHAPTERS

Aaronson SA, 'The Difficult Past and Troubled Future of Digital Protectionism' in I Borchert and LA Winters (eds), *Addressing Impediments to Digital Trade* (London, CEPR, 2021) 141–68
Baird, S, 'The Government at the Standards Bazaar' in L DeNardis (ed), *Opening Standards: The Global Politics of Interoperability* (Cambridge MA, MIT Press, 2011) 13–32
Boutros, A, 'The Key Tools of the Trade in Transnational Bribery Investigations and Prosecutions: Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory' in TM Funk and A Boutros (eds), *From Baksheesh to Bribery: Understanding the Global Fight Against Corruption and Graft* (New York, Oxford University Press, 2019) 547–70
Bradford, A, 'Antitrust Law in Global Markets' in E Elhauge (ed), *Research Handbook on the Economics of Antitrust Law* (Cheltenham, Edward Elgar, 2012) 283–326
Buchan R, 'Cyber Espionage and International Law' in N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Cheltenham, Edward Elgar, 2015) 168–89
Burri, M, 'Designing Future-Oriented Multilateral Rules for Digital Trade' in P Sauvé and M Roy (eds), *Research Handbook on Trade in Services* (Cheltenham, Edward Elgar, 2016) 331–56
Burri, M, 'Understanding the Implications of Big Data and Big Data Analytics for Competition Law: An Attempt for a Primer' in K Mathis and A Tor (eds), *New Developments in Competition Behavioural Law and Economics* (Cham, Springer, 2018) 241–64
Bygrave, LA, 'Hardwiring Privacy' in R Brownsford et al (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford, Oxford University Press, 2017) 754–75
Chang, LY and Wei-Liu, H, 'Ensuring Cybersecurity for Digital Services Trade' in JW Kang et al (eds), *Unlocking the Potential of Digital Services Trade in Asia and the Pacific* (Manila Asian Development Bank, 2022) 184–204
Ghosh, R, 'An Economic Basis for Open Standards' in L DeNardis (ed), *Opening Standards: The Global Politics of Interoperability* (Cambridge MA, MIT Press, 2011) 75–96
Henderson, C, 'The United Nations and the Regulation of Cyber-security' in N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Cheltenham, Edward Elgar, 2015) 582–614
Kastner, P and Mégret, F, 'International Legal Dimensions of Cybercrime' in N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Cheltenham, Edward Elgar, 2015) 253–71
Liu, H-W, 'China Standard Time: The Boundaries of Techno-nationalism in Megaregionals' in S Peng et al (eds), *Governing Science and Technology under the International Economic Order* (Cheltenham, Edward Elgar, 2018) 114–42
Lynskey O, 'Article 20. Right to Data Portability' in C Kuner et al (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford, Oxford University Press, 2020) 497–507
Maurer, T et al, 'Technological Sovereignty: Missing the Point?' in M Maybaum et al (eds), *Architectures in Cyberspace* (Tallinn, NATO CCD COE Publications, 2015) 53–68
Mavroidis, PC and Neven, DJ, Competition Enforcement, 'Trade and Global Governance: A Few Comments' in D Gerard and I Lianos (eds), *Reconciling Efficiency and Equity: A Global Challenge for Competition Policy* (Cambridge, Cambridge University Press, 2019) 398–413

Mwangi, J, 'Contesting Digital Colonialism Narratives in Africa and Their Framing Effects' in PG Sampath and F Tregenna (eds), *Digital Sovereignty: African Perspectives* (Capetown, Zenodo, 2022) 72–79

Sampath, PG and Tregenna, F, 'Digital Sovereignty in Africa: An Introduction' in PG Sampath and F Tregenna (eds), *Digital Sovereignty: African Perspectives* (Capetown, Zenodo, 2022) 7–12

Shaffer, G and Halliday, T, 'With, Within, and Beyond the State: The Promise and Limits of Transnational Legal Ordering' in P Zumbansen (ed), *The Oxford Handbook of Transnational Law* (2021) 987–1006

Sokol DD, 'International Antitrust Institutions' in RD Blair and DD Sokol (eds), *The Oxford Handbook of International Antitrust Economics*, vol 1 (Oxford, Oxford University Press, 2014) 119–46

Solum, LB, 'Models of Internet Governance' in LA Bygrave and J Bing (eds), *Internet Governance: Infrastructure and Institutions* (Oxford, Oxford University Press, 2009) 48–91

Teubner, G and Korth, P, 'Two Kinds of Legal Pluralism: Collision of Transnational Regimes in the Double Fragmentation of World Society' in MA Young (ed), *Regime Interaction in International Law: Facing Fragmentation* (Oxford, Oxford University Press, 2012) 23–54

Trebilcock, MJ and Iacobucci, EM, 'National Treatment and Extraterritoriality: Defining the Domains of Trade and Antitrust Policy' in RA Epstein and MS Greve (eds), *Competition Laws in Conflict* (Washington, AEI, 2004) 152–76

Tuthill, LL, 'Cross-Border Data Flows: What Role for Trade Rules?' in P Sauvé and M Roy (eds), *Research Handbook on Trade in Services* (Cheltenham, Edward Elgar, 2016) 357–84

Wouters, J and Geraets, D, 'The G20 and Informal International Lawmaking' in A Berman et al (eds), *Informal International Lawmaking: Case Studies* (Torkel Opsahl Academic EPublisher, 2012) 19–54

JOURNAL ARTICLES

Aaronson, SA, 'What Are We Talking About When We Talk About Digital Protectionism?' (2018) 18(4) *World Trade Review* 541

Aaronson, SA, and Leblond, P, 'Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO' (2018) 21(2) *Journal of International Economic Law* 245

Abbott, FM, 'Under the Radar: Reflections on "Forced" Technology Transfer and the Erosion of Developmental Sovereignty' (2020) 69(3) *GRUR International* 260

Abelson, H, 'Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications' (2015) 1(1) *Journal of Cybersecurity* 69

Abraha, HH, 'Law Enforcement Access to Electronic Evidence across Borders: Mapping Policy Approaches and Emerging Reform Initiatives' (2021) 29(2) *International Journal of Law and Information Technology* 118

Ahmed, U, 'The Importance of Cross-Border Regulatory Cooperation in an Era of Digital Trade' (2019) 18(S1) *World Trade Law Review* s99

Arner, DW et al, 'The Transnational Data Governance Problem' (2021) 37 *Berkeley Technology Law Journal* 623

Azmeh, S et al, 'The International Trade Regime and the Quest for Free Digital Trade' (2019) 22(3) *International Studies Review* 671

Bartels, L, 'The Chapeau of the General Exceptions in the WTO GATT and GATS Agreements: A Reconstruction' (2015) 109(1) *American Journal of International Law* 95

Benvenisti, E, 'Upholding Democracy Amid the Challenges of New Technology: What Role for the Law of Global Governance?' (2018) 29(1) *European Journal of International Law* 9

Berman A, 'Industry, Regulatory Capture and Transnational Standard Setting' (2017) 111 *AJIL Unbound* 112

Bhala, R, 'National Security and International Trade Law: What the GATT Says, and What the United States Does' (1998) 19 *University of Pennsylvania Journal of International Economic Law* 263

Black, J, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (2008) 2(2) *Regulation & Governance* 137

Bollyky, TJ and Mavroidis, PC, 'Trade, Social Preferences and Regulatory Cooperation: The New WTO-Think' (2017) 20(1) *Journal of International Economic Law* 1

Borgogno, O and Colangelo, G, 'Data Sharing and Interoperability: Fostering Innovation and Competition Through APIs' (2019) 35(5) *Computer Law & Security Review* 1

Boshe, P et al, 'African Data Protection Laws: Current Regulatory Approaches, Policy Initiatives, and the Way Forward' (2022) 3(2) *Global Privacy Law Review* 56

Boylan, E, 'Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners' (2017) 50(1) *Vanderbilt Journal of Transnational Law* 217

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

Broeders, D et al, 'In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions' (2023) 61(4) *JCMS: Journal of Common Market Studies* 1

Burri, M and Chander, A, 'What Are Digital Trade and Digital Trade Law?' (2023) 117 *AJIL Unbound* 99

Burri, M and Polanco, R, 'Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset' (2020) 23(1) *Journal of International Economic Law* 187

Burri, M, 'New Legal Design for Digital Commerce in Free Trade Agreements' (2017) 107(3) *Digiworld Economic Journal* 1

Burri, M, 'The Regulation of Data Flows Through Trade Agreements' (2017) 48(1) *Georgetown Journal of International Law* 407

Callo-Müller, MV and Kugler, K, 'Digital Trade, Development, and Inequality' (2023) 117 *AJIL Unbound* 116

Cerf, V et al, 'Internet Governance Is Our Shared Responsibility' (2014) 10(1) *I/S: A Journal of Law and Policy for the Information Society* 1

Chaisse, J and Matushita, M, 'Maintaining the WTO's Supremacy in the International Trade Order: A Proposal to Refine the Role of the Trade Policy Review Mechanism' (2013) 16(1) *Journal of International Economic Law* 9

Chander A and Schwartz PM, 'Privacy and/or Trade' (2023) 90(1) *University of Chicago Law Review* 49

Chander A, 'Future-Proofing Law' (2017) 51(1) *UC Davis Law Review* 1

Chander A, 'International Trade and Internet Freedom' (2008) 102 *Proceedings of the ASIL Annual Meeting* 37

Chander, A and Sun, H, 'Sovereignty 2.0' (2023) 55(2) *Vanderbilt Journal of International Law* 283

Chander, A and Le, UP, 'Data Nationalism' (2015) 64(3) *Emory Law Journal* 677

Chander, A, 'Is Data Localization a Solution for *Schrems II*?' (2020) 23(3) *Journal of International Economic Law* 771

Chang, Y, 'China Beyond China, a Digital Order with Chinese Characteristics? China's Discursive Power and Its Global Digital Vision' (2023) 51(2) *Politics & Policy* 283

Cho, S, 'Of the World Trade Court's Burden' (2009) 20(3) *European Journal of International Law* 675

Cochrane, T, 'Law Enforcement Cross-Border Data Sharing: A CLOUD Act Agreement for Aotearoa New Zealand?' (2021) 3 *New Zealand Law Review* 401

Colino, AM, 'The Case Against Alibaba in China and Its Wider Policy Repercussions' (2022) 10(1) *Journal of Antitrust Enforcement* 217

Cowhey, PF and Aronson, JD, 'Digital Trade and Regulation in an Age of Disruption' (2018) 22(1) *UCLA Journal of International Law and Foreign Affairs* 8

Curto, G et al, 'Are AI Systems Biased Against the Poor? A Machine Learning Analysis Using Word2Vec and GloVe Embeddings' (2022) *AI & Society* [online]
Daskal, J, 'Borders and Bits' (2019) 71(1) *Vanderbilt Law Review* 179
Daskal, J, 'The Un-Territoriality of Data' (2015) 125 *Yale Law Journal* 326
Delimatsis, P, 'Global Standard-Setting 2.0: How the WTO Spotlights ISO and Impacts the Transnational Standard-Setting Process' (2018) 28(2) *Duke Journal of Comparative & International Law* 273
DeNardis, L and Raymond, M, 'The Internet of Things as a Global Policy Frontier' (2017) 51(2) *UC Davis Law Review* 475
Du, M, 'How to Define 'Public Morals' in WTO Law? A Critique of Brazil – Taxation and Charges Panel Report' (2018) 13(2) *Global Trade and Customs Journal* 69
Du, M, 'Re-conceptualizing the Role of Science in International Trade Disputes' (2018) 52(5) *Journal of World Trade* 697
Du, M, 'The Necessity Test in World Trade Law: What Now?' (2016) 15(4) *Chinese Journal of International Law* 817, 835
Erie, MS and Streinz, T, 'The Beijing Effect: China's Digital Silk Road as Transnational Data Governance' (2021) 54(1) *Journal of International Law and Politics* 1
Evertsz, N et al, 'What Constitutes Equitable Data Sharing in Global Health Research? A Scoping Review of the Literature on Low-Income and Middle-Income Country Stakeholders' Perspectives' (2023) 8(e010157) *BMJ Global Health* 1
Farboodi, M et al, 'Big Data and Firm Dynamics' (2019) 109 *AEA Papers and Proceedings* 38
Farrell, H and Newman, AL, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion' (2019) 44(1) *International Security* 42
Farrell, H and Newman, AL, 'The Janus Face of the Liberal International Information Order: When Global Institutions are Self–Undermining (2021) 75 *International Organisation* 333
Finnemore, M and Hollis, DB, 'Constructing Norms for Global Cybersecurity' (2016) 110(3) *American Journal of International Law* 425
Fox, E, 'The End of Antitrust Isolationism: The Vision of One World' (1992) 1 *University of Chicago Legal Forum* 237
Fox, E, 'Toward World Antitrust and Market Access' (1997) 91 *American Journal of International Law* 1
Froese, MD, 'Digital Trade and Dispute Settlement in RTAs: An Evolving Standard?' (2019) 53(5) *Journal of World Trade* 783
Gal, MS and Rubinfeld, DL, 'Data Standardization' (2019) 94(4) *NYU Law Review* 737
Garcia, F, 'Beyond Special and Differential Treatment' (2004) 27(2) *Boston College International and Comparative Law Review* 291
Gasser, U and Almeida, V, 'Futures of Digital Governance' (2022) 65(3) *Communications of the ACM* 30
Gasser, U, 'Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy' (2016) 130 (2) *Harvard Law Review Forum* 61
Georgieva, I, 'The Unexpected Norm-Setters: Intelligence Agencies in Cyberspace' (2020) 41(1) *Contemporary Security Policy* 33
Gibson, CS, 'Globalization and the Technology Standards Game: Balancing Concerns of Protectionism and Intellectual Property in International Standards' (2007) 22(4) *Berkeley Technology Law Journal* 1403
Glen, C, 'Norm Entrepreneurship in Global Cybersecurity' (2021) 49(5) *Politics & Policy* 1121
Goldsmith, J, 'How Cyber Changes the Laws of War' (2013) 24 (1) *European Journal of International Law* 129
Greenleaf, G, 'APEC's Privacy Framework: A New Low Standard' (2005) 11(5) *Privacy Law and Policy Reporter* 121
Greenleaf, G, 'Pakistan and Sri Lanka's Data Privacy Bills Move Forward' (2021) 173 *Privacy Laws & Business International Report* 24

Guzman, A, 'Antitrust and International Regulatory Federalism' (2001) 76 *New York University Law Review* 1142

Guzman, A, 'Is International Antitrust Possible?' (1998) 73 *New York University Law Review* 1501

Hagemann, R, 'Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future' (2018) 17(1) *Colorado Technology Law Journal* 37

Heath, B, 'The New National Security Challenge to the Economic Order' (2020) 129(4) *Yale Law Journal* 924

Hegde, V and Wouters, J, 'Special and Differential Treatment Under the World Trade Organization: A Legal Typology' (2021) 24(3) *Journal of International Economic Law* 551

Heinemann, A and Choi, YS, 'Competition and Trade: The Rise of Competition Law in Trade Agreements and Its Implications for the World Trading System' (2020) 43(4) *World Competition* 521

Hilbert, M, 'Big Data for Development: A Review of Promises and Challenges' (2016) 34(1) *Development Policy Review* 135

Hoekman, B et al, 'Transfer of Technology to Developing Countries: Unilateral and Multilateral Policy Options' (2005) 33(10) *World Development* 1587

Hollis, DB, 'An e-SOS for Cyberspace' (2011) 52(2) *Harvard International Law Journal* 373

Hon, WK et al, 'Policy, Legal and Regulatory Implications of a Europe-only Cloud' (2016) 24(3) *International Journal of Law and Information Technology* 251

Horowitz, J, 'US International Trade Commission's Digital Trade Roundtable: Discussion Summary' (2015) 4 *Journal of International Commerce and Economics* 1

Hummel, P et al, 'Data Sovereignty: A Review' (2021) 8(1) *Big Data & Society* 1

Ikejiaku, B and Dayao, C, 'Competition Law as an Instrument of Protectionist Policy: Comparative Analysis of the EU and the US' (2021) 36(1) *Utrecht Journal of International and European Law* 75

Irion, K, 'Government Cloud Computing and National Data Sovereignty' (2012) 4(3–4) *Policy & Internet* 40

Irion, K et al, 'Privacy Peg, Trade Hole: Why We (Still) Shouldn't Put Data Privacy in Trade Law' (*University of Chicago Law Review Online*, 27 March 2023)

Jenny, F, 'Competition Law and Digital Ecosystems: Learning to Walk Before We Run' (2021) 30(5) *Industrial and Corporate Change* 1143

Kelsey, J, 'How a TPP-Style E-commerce Outcome in the WTO Would Endanger the Development Dimension of the GATS Acquis (and Potentially the WTO)' (2018) 21(2) *Journal of International Economic Law* 273

Knight, L and Voon, T, 'The Evolution of National Security at the Interface Between Domestic and International Investment Law and Policy: The Role of China' (2020) 21(1) *The Journal of World Investment & Trade* 104

Komaitis, K, 'The "Wicked Problem" of Data Localization' (2017) 3(2) *Journal of Cyber Policy* 355

Kuner, C et al, 'The Language of Data Privacy Law (and How It Differs from Reality)' (2016) 6(4) *International Data Privacy Law* 259

Lamp, N, 'At the Vanishing Point of Law: Rebalancing, Non-violation Claims, and the Role of the Multilateral Trade Regime in the Trade Wars' (2019) 22(4) *Journal of International Economic Law* 721

Lamp, N, 'How Some Countries Became "Special": Developing Countries and the Construction of Difference in Multilateral Trade Lawmaking' (2015) 18 *Journal of International Economic Law* 743

Lazo, RP and Sauvé, P, 'The Treatment of Regulatory Convergence in Preferential Trade Agreements' (2018) 17(4) *World Trade Review* 575

Lee, J, 'Hacking into China's Cybersecurity Law' (2017) 53(1) *Wake Forest Law Review* 57

Lee, JS, 'Towards a Development-Oriented Multilateral Framework on Competition Policy' (2006) 7 *San Diego International Law Journal* 293

Lester, S and Zhu, H, 'A Proposal for "Rebalancing" to Deal with "National Security" Trade Restrictions' (2019) 42(5) *Fordham International Law Journal* 1451

Loevinger, L, 'Antitrust Law in the Modern World' (1962) 6(2) *International and Comparative Law Bulletin* 20

Low, P, 'The WTO in Crisis: Closing the Gap between Conversation and Action or Shutting Down the Conversation?' (2022) 21(3) *World Trade Review* 274

Lydgate, E, 'Is It Rational and Consistent? The WTO's Surprising Role in Shaping Domestic Public Policy' (2017) 20(3) *Journal of International Economic Law* 561

MacDonald, DA and Streatfield, CM, 'Personal Data Privacy and the WTO' (2014) 36(3) *Houston Journal of International Law* 629

Maher, I, 'Competition Law in the International Domain: Networks as a New Form of Governance' (2002) 29(1) *Journal of Law and Society* 111

Mamir, V, 'Anchoring the Need to Revise Cross-Border Access to e-Evidence' (2020) 9(3) *Internet Policy Review* [online]

Mann, CL, 'International Internet Governance: Oh What a Tangled Web We Weave' (2001) 2(2) *Georgetown Journal of International Affairs* 79

Mansfield, ED and Rudra, N, 'Embedded Liberalism in the Digital Era' (2021) 75(2) *International Organization* 558

Marachel, N, 'Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy' (2017) 5(1) *Media & Communication* 29

Marguiles, P, 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility' (2013) 14 *Melbourne Journal of International Law* 496

Matsushita, M, 'A View on Future Roles of the WTO: Should There Be More Soft Law in the WTO?' (2014) 17(3) *Journal of International Economic Law* 701

Matsushita, M, 'Basic Principles of the WTO and the Role of Competition Policy' (2004) 3(2) *Washington University Global Studies Law Review* 363

Mattoo, A and Meltzer, JP, 'International Data Flows and Privacy: The Conflict and Its Resolution' (2018) 21(4) *Journal of International Economic Law* 769

Mavroidis, PC and Wolfe, R, 'Private Standards and the WTO: Reclusive No More' (2017) 16(1) *World Trade Review* 1

McGinnis, JO and Movsesian, ML, 'The World Trade Constitution' (2000) 114(2) *Harvard Law Review* 511

Meltzer, JP, 'Governing Digital Trade' (2018) 18(S1) *World Trade Review* s23

Meltzer, JP, 'The Internet, Cross-Border Data Flows and International Trade' (2014) 2 *Asia & the Pacific Policy Studies* 90

Mishra, N and Agrawal, B, 'Addressing the Global Data Divide through Digital Trade Law' (2022) 14(2) *Trade, Law & Development* 238

Mishra, N and Valencia, AMP, 'Digital Services and Digital Trade in the Asia Pacific: An Alternative Model for Digital Integration?' (2023) 31(2) *Asia Pacific Law Review* 489

Mishra, N, 'Breaking Down Digital Walls: The Interface of International Trade Law and Online Content Regulation through the Lens of the Chinese VPN Measure' (2022) 47(2) *Brooklyn Journal of International Law* 359

Mishra, N, 'Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows' (2019) 52(2) *Vanderbilt Journal of Transnational Law* 463

Mishra, N, 'International Trade Law Meets Data Ethics: A Brave New World' (2021) 53(2) *International Law and Politics* 303

Mishra, N, 'The Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance?' (2017) 20(1) *Journal of International Economic Law* 31

Mishra, N, 'The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance' (2020) 54(4) *Journal of World Trade* 567

Mitchell, AD and Hepburn, J, 'Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer' (2017) 19 *Yale Journal of Law and Technology* 182

Mitchell, AD and Mishra, N, 'Data at the Docks: Modernizing International Trade Law for the Digital Economy' (2020) 20(4) *Vanderbilt Journal of Entertainment and Technology Law* 1073

Mitchell, AD and Mishra, N, 'Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute' (2019) 22(3) *Journal of International Economic Law* 389

Mitchell, AD and Samlidis, T, 'Cloud Services and Government Digital Sovereignty in Australia and Beyond' (2021) 29(4) *International Journal of Law and Information Technology* 364

Molinuevo, M and Gaillard, S, 'Trade, Cross-Border Data, and the Next Regulatory Frontier: Law Enforcement and Data Localization Requirements' (2018) 3 *MTI Practice Notes* 2

Mubarak, F and Suomi, R, 'Elderly Forgotten? Digital Exclusion in the Information Age and the Rising Grey Digital Divide' (2022) 59(Dec–Jan) *Inquiry: The Journal of Health Care Organization, Provision, and Financing*

Mueller, ML and Grindal, K, 'Data Flows and the Digital Economy: Information as a Mobile Factor of Production' (2018) 21(1) *Digital Policy, Regulation and Governance* 71

Oddenino, A, 'Digital Standardization, Cybersecurity Issues and International Trade Law' (2018) 51 *Questions of International Law* 31

Ohm, P, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 *UCL Law Review* 1701

Pasquale, F, 'Privacy, Antitrust and Power' (2013) 20(4) *George Mason Law Review* 1009

Pauwelyn, J, 'Taking Stakeholder Engagement in International Policy-Making Seriously: Is the WTO Finally Opening Up?' (2023) 26(1) *Journal of International Economic Law* 51

Pauwelyn, P et al, 'When Structures Become Shackles: Stagnation and Dynamics in International Lawmaking' (2014) 25(3) *European Journal of International Law* 733

Peng, S, '"Private" Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime' (2018) 51(2) *Cornell International Law Journal* 445

Peng, S, 'Public–Private Interactions in Privacy Governance' (2022) 11(6) *Laws* 80

Peng, S, 'The Rule of Law in Times of Technological Uncertainty: Is International Economic Law Ready for Emerging Supervisory Trends?' (2019) 22(1) *Journal of International Economic Law* 1

Peng, S, 'The Uneasy Interplay Between Digital Inequality and International Economic Law' (2022) 33(1) *European Journal of International Law* 205

Pinchis-Paulsen, M, 'Let's Agree to Disagree: A Strategy for Trade-Security' (2022) 25(4) *Journal of International Economic Law* 527

Pohle, J and Thiel, T, 'Digital Sovereignty' (2020) 9(4) *Internet Policy Review*

Rachovitsa, A, 'Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue' (2016) 24(4) *International Journal of Law and Information Technology* 374

Reidenberg, JR, 'E-Commerce and Trans-Atlantic Privacy' (2001) 38 *Houston Law Review* 717

Roberts, A et al, 'Toward a Geoeconomic Order in International Trade and Investment' (2019) 22(4) *Journal of International Economic Law* 655

Rowley, J, 'The Wisdom Hierarchy: Representations of the DIKW Hierarchy' (2006) 33(2) *Journal of Information Science* 163

S Lester and I Manak, 'A Proposal for a Committee on National Security at the WTO' (2020) 30(2) *Duke Journal of Comparative & International Law* 267

Schloemann, HL and Ohlhoff, S, '"Constitutionalization" and Dispute Settlement in the WTO: National Security as an Issue of Competence' (1999) 93(2) *American Journal of International Law* 424

Schwartz, PM and Solove, DJ, 'Reconciling Personal Information in the United States and European Union' (2014) 102(4) *California Law Review* 877

Schwartz, PM, 'Legal Access to the Global Cloud' (2018) 118 *Columbia Law Review* 1681

Selby, J, 'Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?' (2017) 25(3) *International Journal of Law and Information Technology* 213

Sen, N, 'Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path' (2018) 21(2) *Journal of International Economic Law* 323

Shackleford, SJ et al, 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors' (2016) 17(1) *Chicago Journal of International Law* 1

Shackleford, SJ et al, 'When Toasters Attack: Enhancing the "Security of Things" Through Polycentric Governance' (2017) 2 *University of Illinois Law Review* 415

Shaffer, G, 'Trade Law in a Data-Driven Economy: The Need for Modesty and Resilience' (2021) 20(3) *World Trade Review* 259

Sheargold, E and Mitchell, AD, 'The TPP and Good Regulatory Practices: An Opportunity for Regulatory Coherence to Promote Regulatory Autonomy' (2016) 15(4) *World Trade Review* 587

Stucke, ME, 'Should We Be Concerned About Data-opolies?' (2018) 2(2) *Georgetown Law Technology Review* 275

Stucke, ME, 'The Relationship Between Privacy and Antitrust' (2022) 97(5) *Notre Dame Law Review Reflection* 400

Sun, H and Wat, P, 'Tech Wars and the Conflict of Public Interests' (2021) 5 *Georgetown Law and Technology Review* 62

Svantesson, JDB, 'The Regulation of Cross-Border Data Flows' (2011) 1(3) *International Data Privacy Law* 180

Sweeney, B, 'Globalisation of Competition Law and Policy: Some Aspects of the Interface Between Trade and Competition' (2004) 5(2) *Melbourne Journal of International Law* 375

Swire, P and Lagos, Y, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72(2) *Maryland Law Review* 335

Tarullo, D, 'Norms and Institutions in Global Competition Policy' (2000) 94(3) *American Journal of International Law* 478

Tene, O and Hughes, JT, 'The Promise and Shortcomings of Privacy Multistakeholder Policymaking: A Case Study' (2014) 66(2) *Maine Law Review* 437

Veisdal, J, 'The Dynamics of Entry for Digital Platforms in Two-Sided Markets: A Multi-Case Study' (2020) 30 *Electronic Markets* 539

Voon, T, 'Exploring the Meaning of Trade Restrictiveness in the WTO' (2015) 14(3) *World Trade Review* 451

Waller, SW, 'Book Review: Mario Marques Mendes, Antitrust in a World of Interrelated Economies' (1991) 17(3) *Brooklyn Journal of International Law* 609

Weber, RH, 'Regulatory Autonomy and Privacy Standards under the GATS' (2012) 7 *Asian Journal of WTO and International Health Law & Policy* 25

Weber, S, 'Data, Development, and Growth' (2017) 19(3) *Business and Politics* 397

Wells, CB, 'Platform Power and Privacy Protection: A Case for Policy Innovation' (2018) *CPI Antitrust Chronicle* 1

Whitman, JQ, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2014) 113(6) *Yale Law Journal* 1151

Widiatedja, IGNP and Mishra, N, 'Establishing an Independent Data Protection Authority in Indonesia: A Future–Forward Perspective' [2022, Advanced Access] *International Review of Law, Computers & Technology* 1

Wilkinson, M et al, 'The FAIR Guiding Principles for Scientific Data Management and Stewardship' (2016) 3(160018) *Scientific Data*

Willemyns, I, 'GATS Classification of Digital Services – Does "The Cloud" Have a Silver Lining?' (2019) 53(1) *Journal of World Trade* 59

Wolfe, R, 'Informal Learning and WTO Renewal: Using Thematic Sessions to Create More Opportunities for Dialogue' (2021) 12(S3) *Global Policy* 30

Wolfe, R, 'Learning About Digital Trade: Privacy and e-Commerce in CETA and TPP' (2019) 18(S1) *World Trade Review* s63

Wolff, J, 'What We Talk About When We Talk About Cybersecurity: Security in Internet Governance Debates' (2016) 5(3) *Internet Policy Review* 1

Wood, DP, 'The Impossible Dream: Real International Antitrust' (1992) 1992(1) *University of Chicago Legal Forum* 277

Woods, AK, 'Against Data Exceptionalism' (2016) 68 *Stanford Law Review* 729

Wu, M, 'The "China, Inc" Challenge to Global Trade Governance' (2016) 57(2) *Harvard International Law Journal* 261

Xavier, C et al, 'The Internet of Things and Its Impact on Individual Privacy: An Australian Perspective' (2016) 32(1) *Computer Law & Security Review* 4

Yakovleva, S, 'On Digital Sovereignty, New European Data Rules, and the Future of Free Data Flows' (2022) 49(4) *Legal Issues of Economic Integration* 339

Yoo JY, and Ahn, D, 'Security Exceptions in the WTO System: Bridge or Bottle-Neck for Trade and Security?' (2016) 19(2) *Journal of International Economic Law* 417

REPORTS, BRIEFS, WORKING PAPERS, THESIS AND CONFERENCE PROCEEDINGS

Aaronson, SA, 'Data Is Disruptive: How Data Sovereignty Is Challenging Data Governance' (Hinrich Foundation, 03 August 2022)

Aaronson, SA, 'What Does TPP Mean for the Open Internet?' (International Institute for Economic Policy Brief on Trade Agreements and Internet Governance, Prepared for the Global Commission on Internet Governance, 16 November 2015)

Aaronson, SA et al, 'DataGovHub Paradigm for a Comprehensive Approach to Data Governance – Year 1 Report' (Digital Trade & Data Governance Hub, 2021)

Ahrens, N, 'National Security and China's Information Security Standards' (CSIS Briefs, November 2012)

Anderson, RD et al, 'Competition Policy, Trade and the Global Economy: An Overview of Existing WTO Elements, Commitments in Regional Trade Agreements, Some Current Challenges and Issues for Reflection' (31 October 2018) WTO Staff Working Paper ERSD-2018–12

Andrenelli, A and González, JL, 'Electronic Transmissions and International Trade – Shedding New Light on the Moratorium Debate' (13 November 2019) OECD Trade Policy Working Paper No 233

Andreoni, A and Roberts, S, 'Governing Data and Digital Platforms in Middle Income Countries: Regulations, Competition and Industrial Policies, With Sectoral Case Studies from South Africa' (Digital Pathways Paper Series, Oxford University, November 2020)

APEC, 'Competition Law and Regulation in Digital Markets' (March 2022) APEC#222-EC-01.3

Arasasingham, A and Goodman, M, 'Operationalizing Data Free Flow with Trust (DFFT)' (CSIS, April 2023)

Bacchus, J, 'The Digital Decide – How to Agree on WTO Rules for Digital Trade' (CIGI, 2021)

Badiei, F et al, 'Markets versus Mandates: Solutions for Securing the Internet of Things' (R Street Institute, November 2017)

Banga, R, 'WTO Moratorium on Customs Duties on Electronic Transmissions: How Much Tariff Revenue Have Developing Countries Lost?' (3 June 2022) South Centre Research Paper No 157

Bauer, M et al, 'The Costs of Data Localisation: Friendly Fire on Economic Recovery' (2014) ECIPE Occasional Paper No 3

Beyleveld, A and Sucker, F, 'Cross-Border Data Flows in Africa: Policy Considerations for the AfCFTA Protocol on Digital Trade' (Mandela Institute, 21 October 2022)

Bhagwati, J, 'US Trade Policy: The Infatuation with FTAs' (1995) Columbia University Discussion Paper Series No 726

Brito, AC et al, 'The Contribution of Mutual Recognition to International Regulatory Cooperation' (2016) OECD Regulatory Policy Working Papers No 2

Brooymans-Quinn, J and Malinouski, A, 'Competition Policy and the International Trade Landscape: Assessing Recent Developments and Trends' (Trade Labs, 2020)
Budish, R et al, 'Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects' (2 March 2018) Hoover Institution, Aegis Series Paper No 1804
Bughin, J and Lund, S, 'The Ascendancy of International Data Flows' (McKinsey Global Institute, 9 January 2017)
Burri, M and Kugler, K, 'Digitization, Regulatory Barriers and Sustainable Development' (2023) Trade Law 4.0 Working Paper No 03/2023
Casalini, F, 'Cross-Border Data Flows – Taking Stock of Key Policies and Initiatives' (OECD, 2022)
Casalini, F et al, 'A "Digital" Convention to Protect Cyberspace?' (Trade Lab, 18 January 2018)
Casalini, F et al, 'Approaches to Market Openness in the Digital Age' (2019) OECD Trade Policy Papers No 219
Cernat, L, 'How Important Are Mutual Recognition Agreements for Trade Facilitation?' (December 2022) ECIPE Policy Brief No 10
Chander, A et al, 'World Development Report 2021 – Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation' (2021) World Bank Policy Research Working Paper 9594
Chen, L et al, 'The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies' (T20 Japan, 29 March 2019)
Chen, R, 'Mapping Data Governance Legal Frameworks Around the World – Findings from the Global Data Regulation Diagnostic' (2021) World Bank Policy Research Working Paper 9615
Christakis, T, 'European Digital Sovereignty: Successfully Navigating between the "Brussels Effect" and Europe's Quest for Strategic Autonomy' (2020)
CIGI and Chatham House, 'Global Commission on Internet Governance: One Internet' (2016)
Ciuriak, D and Fay, R, 'The Digital Economy Partnership Agreement: Should Canada Join?' (2022) CIGI Policy Brief No 171
Ciuriak, D, 'Rethinking Industrial Policy for the Data-driven Economy' (October 2018) CIGI Paper No 82, Centre for International Governance Innovation
Connolly, C et al, 'Privacy Self-Regulation in Crisis? TRUSTe's "Deceptive" Practices' (2014) UNSW Law Research Paper No 2015–08
Cory, N, 'Cross-Border Data Flows: Where Are the Barriers and What Do They Cost?' (ITIF, May 2017)
Cory, N and Dascoli, L, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them' (ITIF, July 2021)
Cybersecurity and Infrastructure Security Agency, 'Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default' (13 April 2023)
Datasphere Initiative, 'Datasphere Governance Atlas' (2022)
DeNardis, L et al, 'The Rising Geopolitics of Internet Governance: Cyber Sovereignty v Distributed Governance' (Paper Presented at Columbia SIPS Tech & Policy Initiative, Columbia SIPA, November 2016)
Department of Digital, Media, Culture & Sport (UK), 'Secure by Design: Improving the Cybersecurity of Consumer Internet of Things Report' (2018)
DFAT, 'Australia's International Cyber Engagement Strategy' (October 2017)
Digital Competition Expert Panel (UK), *Unlocking Digital Competition* (March 2019)
Drake, WJ et al, 'Internet Fragmentation: An Overview' (Future of the Internet Initiative White Paper, World Economic Forum, 2016)
Drake-Brockman, J et al, 'Digital trade and the WTO: Negotiation Priorities for Cross-Border Data Flows and Online Trade in Services' (2021) Jean Monnet TIISA Network Working Paper 2021/11
EIT Digital, 'European Digital Infrastructure and Data Sovereignty: A Policy Perspective' (2020)
Evenett, SJ and Fritz, J, 'Emergent Digital Fragmentation: The Perils of Unilateralism' (Hinrich Foundation, 28 June 2022)

Expert Group on Data Free Flow with Trust, 'Interim Report of the Expert Group on Data Free Flow with Trust' (METI, 28 February 2022)

Fazlioglu, M, 'How DPA Budget and Staffing Levels Mirror National Differences in GDP and Population' (IAPP, 2018)

Federal Ministry of Economic Affairs and Energy, 'Project GAIA-X: A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem' (2019)

Ferracane, MF and Marel, EVD, 'Regulating Personal Data: Data Models and Digital Services Trade' (World Bank, 2021)

Ferracane, MF et al, 'Digital Trade Restrictiveness Index' (ECIPE, 2018)

Friedman, AA, 'Cybersecurity and Trade: National Policies, Global and Local Consequences' (Centre for Technology Innovation at Brookings, September 2013)

FSB, 'Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships' (14 June 2021)

FSB, 'Third-Party Dependencies in Cloud Services' (9 December 2019)

Girard, M, 'Big Data Analytics Need Standards to Thrive – What Standards Are and Why They Matter' (2019) CIGI Papers No 2091

Girard, M, 'Standards for Digital Cooperation' (2020) CIGI Papers No 237

Global Commission on Internet Governance, *A Universal Internet in a Bordered World – Research on Fragmentation, Openness and Interoperability*, vol 1 (2016)

González, JL and Ferencz, J, 'Digital Trade and Market Openness' (2018) OECD Trade Policy Papers No 217

Govt of UK, 'G7 Roadmap for Cooperation on Data Free Flow with Trust' (G7 UK, 2021)

Guglya, L and Maciel, M, 'Addressing the Digital Divide in the Joint Statement Initiative on E-Commerce' (IISD, 30 December 2020)

Halle, M and Wolfe, R, 'A New Approach to Transparency and Accountability at the WTO' (2010) IISD Entwined Issue Brief No 6

ICN, 'Report on ICN Members' Recent Experiences (2015–2018) in Conducting Competition Advocacy in Digital Markets' (2019)

IEEE, 'IEEE Position Statement – IEEE Adherence to the World Trade Organization Principles for International Standardization' (19 August 2020)

IJPN, 'Framing Brief: Categories of Electronic Evidences' (31 May 2022) Ref 22/102

ILO, *Small Goes Digital – How Digitalization Can Bring About Productive Growth for Micro and Small Enterprises* (2021)

International Working Group of Sovereign Wealth Funds, 'Sovereign Wealth Funds – Generally Accepted Principles and Practices – Santiago Principles' (October 2008)

Internet & Jurisdiction Policy Network, 'Framing Brief: Categories of Electronic Evidences' (31 May 2022) Ref 22/102

Irion, K, 'Algorithms Off-limits?: If Digital Trade Law Restricts Access to Source Code of Software then Accountability Will Suffer' (FAccT' 22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency, 2022)

Irion, K et al, 'Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements' (Bureau Européen des Unions de Consommateurs (BEUC) et al, 2016)

ITU, 'Connectivity in the Least Developed Countries – Status Report' (2021)

ITU, 'Final Report – World Telecommunication Development Conference' (Buenos Aires, 2017)

ITU, 'Measuring Digital Development – Facts and Figures' (2021)

Jütting, J and McDonnell, I, 'Overview: What Will It Take for Data to Enable Development?' in OECD, *Development Co-operation Report 2017 – Data for Development* (2017)

Karachalios, K and McCabe, K, 'Standards, Innovation, and Their Role in the Context of the World Trade Organization' (E15 Initiative, December 2013)

Kathuria, R et al, 'Economic Implications of Cross-Border Data Flows' (ICRIER and IAMAI, November 2019)

Kijirah, M and Thuo, EW, 'Data Protection and Data Localisation in Kenya: Potential Economic Impact and Effect – On Kenya's Commitments in Various Regional Treaty Frameworks' (2021) Mandela Institute Policy Brief 03

Kommerskollegium, 'No Transfer, No Production – a Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods' (2015:4)

Kuner, C, 'Regulation of Transborder Data Flows Under Data Protection and Privacy Law' (2011) OECD Digital Economy Papers No 187

L Brittan and K Van Miert, 'Towards an International Framework of Competition Rules – Communication to the Council' (18 October 1996) Commission of the European Communities Doc No COM(96)284

La Chapelle, BD and Fehlinger, P, 'Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation' (April 2016) Global Commission on Internet Governance Paper Series No 28

Lang, A and Scott, J, 'Regulatory Convergence – A Role for the WTO?' (Proceeding of Annual BIICL WTO Conference, Gray's Inn, 23–24 May 2006)

Leblond, P and Aaronson, SA, 'A Plurilateral "Single Data Area" is the Solution to Canada's Data Trilemma' (2019) CIGI Papers No 226

Lee-Makiyama, H and Gopalakrishnan, BN, 'The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions' (August 2019) ECIPE Policy Brief No 3

Lippoldt, D, 'Mitigating Global Fragmentation in Digital Trade Governance – A Case Study' (January 2023) CIGI Papers No 270

Manyika, J et al, 'Digital Globalization: The New Era of Global Flows' (MGI, March 2016)

Mapping Project, 'Draft Legal Instrument on Government-led Surveillance and Privacy – Including the Explanatory Memorandum' (OHCHR, Ver 0.6, 10 January 2018)

Matambo, E and Ugar, ET, 'South Africa's Data Sovereignty Regulations: Merits and Possible Limitations' (2022) University of Johannesburg Centre for Africa–China Studies Policy Brief No 2

Mckay, A et al, 'International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World' (Microsoft, 2015)

Meltzer, JP, 'Supporting the Internet as a Platform for International Trade Opportunities for Small and Medium-Sized Enterprises and Developing Countries' (February 2014) Brookings Global Economy and Development Working Paper 69

Ministry of Electronics and Information Technology, 'Report by the Committee of Experts on Non-Personal Data Governance Framework' (2020) 111972/2020/CL&ES

Mishra, N, 'Data Governance and Digital Trade in India: Losing Sight of the Forest for the Trees?' (2021) ANU College of Law Research Paper No 21.16

Mishra, N, 'International Trade, Internet Governance and the Shaping of the Digital Economy' (2017) UNESCAP ARTNeT Working Paper No 168

Nakanishi, T and Hori, S, 'Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows' (WEF, 2023)

National Institute of Standards and Technology, 'Framework for Improving Critical Infrastructure Cybersecurity' (v. 1.1, 16 April 2018)

Neeraj, RS, 'Trade Rules on Source Code – Deepening the Digital Inequities by Locking Up the Software Fortress' (28 April 2017) Centre for WTO Studies Working Paper CWS/WP/200/37

Nicholas, G and Weinber, M, 'Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors' (Engelberg Center on Innovation Law and Policy, November 2019)

Nugraha, Y et al, 'Towards Data Sovereignty in Cyberspace' 2015 (3rd International Conference on Information and Communication Technology, Nusa Dua, Bali, Indonesia, 2015)

Nye, JS, 'The Regime Complex for Managing Global Cyber Activities' (20 May 2014) Global Commission on Internet Governance Paper Series No 1

OECD, 'Algorithms and Collusion: Competition Policy in the Digital Age' (2017)

OECD, 'Bridging the Digital Gender Divide – Include, Upskill, Innovate' (2018)

OECD, 'Consumer Data Rights and Competition – Background note' (5 June 2020) DAF/COMP/WD(2020)48
OECD, 'Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document' (1 October 2015)
OECD, 'Economic and Social Benefits of Internet Openness' (2016) OECD Digital Economy Papers No 257
OECD, 'Fostering Cross-Border Data Flows with Trust' (2022) OECD Digital Economy Papers No 343
OECD, 'Mapping Approaches to Data and Data Flows – Report for the G20 Digital Economy Task Force' (2020)
OECD, 'Recommendation on Internet Policy Making Principles' (2014)
OECD, 'Report on the Cross-Border Enforcement of Privacy Laws' (2006)
OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being* (2015)
OECD, *Development Co-operation Report 2021: Shaping a Just Digital Transformation* (2021)
OECD, *Development Co-operation Report 2021: Shaping a Just Digital Transformation* (2021)
OECD, *Enhancing Access to and Sharing of Data* (26 November 2019)
OECD, *Handbook on Competition Policy in the Digital Age* (2022)
OECD, *ICTs for Development – Improving Policy Coherence* (2009)
OECD, *International Regulatory Cooperation: Addressing Global Challenges* (2013)
OECD, *OECD/ICN Report on International Co-operation in Competition Enforcement* (2021)
OECD, *Rethinking Antitrust Tools for Multi-Sided Platforms* (2018)
Office of the Director of National Intelligence (US), 'A Guide to Cyber Attribution' (14 September 2018)
Pisa, M et al, 'Creating a Level Playing Field for Data Protection' in OECD, *Development Co-operation Report 2021: Shaping a Just Digital Transformation* (2021)
Porciuncula, L and La Chapelle, BD, 'We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty' (Internet and Jurisdiction Policy Network, 2021)
Portuese, A, 'The Digital Markets Act: European Precautionary Antitrust' (ITIF, May 2021)
S Wismer and A Rasek, 'Market Definition in Multi-sided Markets' (15 November 2017) OECD DAF/COMP/WD(2017)33/FINAL
Sacks, S and Li, MK, 'How Chinese Cybersecurity Standards Impact Doing Business in China' (CSIS Briefs, 2 August 2018)
Sacks, S and Sherman, J, 'Global Data Governance Concepts, Obstacles, and Prospects' (New America, 2019)
Sebastian, W and Rasek, A, 'Market Definition in Multi-sided Markets' (15 November 2017) OECD DAF/COMP/WD(2017)33/FINAL
Segal, A, 'Chinese Cyber Diplomacy in a New Era of Uncertainty' (June 2017) Aegis Paper Series No 1703, Hoover Institution
Shahbaz, A et al, 'User Privacy or Cyber Sovereignty?' (Freedom House, July 2020)
Shelanski, H et al, 'Network Effects and Efficiencies in Multisided Markets' (15 November 2017) OECD DAF/COMP/WD(2017)40
Subcommittee on Antitrust, Commercial and Administrative Law of the Committee of the Judiciary (US), *Investigation of Competition in Digital Markets* (2020)
Swire, P, and Kennedy-Mayo, D, 'The Effects of Data Localization on Cybersecurity – Organizational Effects' (15 June 2023) Georgia Tech Scheller College of Business Research Paper No 4030905
Thorstensen, V et al, 'Private Standards – Implications for Trade, Development, and Governance' (E15 Initiative, September 2015)
US Department of Commerce, 'Measuring the Value of Cross-Border Data Flows' (September 2016)
Ubaldi, B, 'Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives' (2013) OECD Working Papers on Public Governance No 22
UN DESA, 'Central Product Classification (CPC)' (2015) Statistical Paper Series M No 77, Ver.2.1

UN, 'The Age of Digital Interdependence: Report of the UN Secretary-General's High-Level Panel on Digital Cooperation' (New York, 2019)
UNCTAD, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' (2016) UNCTAD/DTL/STICT/2016/1
UNCTAD, *Competition and Consumer Protection Policies for Inclusive Development in the Digital Era* (UNCTAD/DITC/CPLP/2021/2, 2021)
UNCTAD, *Digital Economy Report 2021* (UNCTAD/DER/2021, 2021)
UNDP, 'Drafting Data Protection Legislation: A Study of Regional Frameworks' (2023)
UNESCO, 'Recommendation on the Ethics of Artificial Intelligence' (UNESCO's 41st General Conference, Paris, 9–24 November 2021)
United States International Trade Commission, *Digital Trade in the US and Global Economies, Part 2* (Publication No 4485, August 2014)
UNSC CTED, 'The State of International Cooperation for Lawful Access to Digital Evidence: Research Perspectives' (January 2022) CTED Trends Report
USTR, '2015 Report on the Implementation and Enforcement of Russia's WTO Commitments' (December 2015)
WEF, 'Competition Policy in a Globalized, Digitalized Economy' (11 December 2019)
WHO, 'Framework for Engagement with Non-State Actors' (28 May 2016) WHA69.10
WHO, 'Sharing and Reuse of Health-Related Data for Research Purposes: WHO Policy and Implementation Guidance' (2022)
Wijkström, E and McDaniels, D, 'International Standards and the WTO TBT Agreement: Improving Governance for Regulatory Alignment' (25 April 2013) WTO Staff Working Paper ERSD-2013–06
Woods, AK, 'Data Beyond Borders – Mutual Legal Assistance in the Internet Age' (Global Network Initiative, January 2015)
World Bank, *World Development Report – Digital Dividends* (2016)
World Bank, *World Development Report 2021: Data for Better Lives* (2021)
WTO, 'Synthesis Paper on the Relationship of Trade and Competition Policy to Development and Economic Growth' (18 September 1998) WTO Doc WT/WGTCP/W/80
WTO, *World Trade Report 2018* (2018)
Yakovleva, S, 'Governing Cross-border Data Flows: Reconciling EU Data Protection and International Trade Law' (PhD thesis, University of Amsterdam 2021)
Zhang, R, 'Covered or Not Covered: That Is the Question' (November 2015) WTO Working Paper ERSD-2015-11

OTHER PRIMARY MATERIALS

APEC, 'APEC Privacy Framework' (November 2004)
Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' (5 April 2017) WP 242 rev.01
Competition Authority of Kenya, 'Revised Guidelines on Relevant Market Definition' (2019)
Department for Promotion of Industry and Internal Trade (India), Consolidated FDI Policy (2017) PP F No 5(1)/2017-FC-1
Department for Promotion of Industry and Internal Trade, Draft National E-Commerce Policy: India's Data for India's Development (26 February 2019)
Department of Communications and Digital Technologies (South Africa), Invitation to Submit Written Submissions on the Proposed National Data and Cloud Policy, No 306 of 1 April 2021
Department of Science and Technology (India), National Data Sharing and Accessibility Policy (9 February 2014)
European Commission, 'Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World' COM/2017/07 final

European Commission, 'Recommendation for a Council Decision authorising the opening of negotiations for digital trade disciplines with the Republic of Korea and with Singapore' COM(2023) 230 final, SWD(2023) 85 final

G20, 'G20 Ministerial Statement on Trade and Digital Economy' (Tsukuba City, 8–9 June 2019)

G7 Digital and Tech Ministers' Meeting, 'G7 Digital and Tech Track Annex – 1: Annex on G7 Vision for Operationalising DFFT and Its Priorities' (Takasaki, 30 April 2023)

G7, 'Declaration on Responsible States Behaviour in Cyberspace' (Lucca, 11 April 2017)

Global Cross-Border Privacy Rules Declaration (21 April 2022)

GPA, 'Adopted Resolution on Government Access to Data, Privacy and the Rule of Law: Principles for Governmental Access to Personal Data held by the Private Sector for National Security and Public Safety Purposes' (43rd Closed Session of the Global Privacy Assembly, October 2021)

ISO, 'Cybersecurity – Guidelines for Internet Security' (2023) ISO/IEC 27032:2023

ITU, 'Declaration of Principles – Building the Information Society: A Global Challenge in the New Millennium' (12 December 2003) WSIS03/GENEVA/DOC/4-E

Ministry of Commerce & Textile (Commerce Division), E-Commerce Policy Framework of Pakistan (August 2019)

Ministry of Electronics and Information Technology, 'Report by the Committee of Experts on Non-Personal Data Governance Framework' (2020) 111972/2020/CL&ES

Ministry of Youth and ICT, Data Revolution Policy (April 2017, Rwanda)

OECD Civil Society Information Society Advisory Council (CSISAC), 'Statement Regarding Trusted Government Access to Private Sector Data Ministerial Declaration' (Gran Canaria, 14 December 2022)

OECD, 'Declaration on Government Access to Personal Data Held by Private Sector Entities' (12 December 2022) OECD/LEGAL/0487

OECD, 'Recommendation of the Council Concerning Guidelines for Cryptography Policy' (27 March 1997) C(97)62/FINAL

OECD, 'Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data' (2013) C(80)58/FINAL, as amended by C(2013)79, 2013) ['OECD Privacy Guidelines']

OECD, 'Recommendation of the Council on the Protection of Critical Information Infrastructures' (30 April 2008) C(2008)35

OECD, 'Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy' (2007)

OECD, 'Resolution of the Council renewing and revising the Mandate of the Committee on Digital Economy Policy' (11 December 2018) OECD C/M(2018)24

OECD, 'Statement of the Committee on Digital Economy Policy' (22 December 2020) DSTI/CDEP(2020)22/FINAL

Reserve Bank of India (RBI), 'Storage of Payment System Data' (6 April 2018) DPSS.CO.OD. No 2785/06.08.005/2017-18

The White House, 'A Declaration for the Future of the Internet' (2022)

Tunis Agenda for The Information Society (Tunis, ITU, WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 November 2005)

UNGA, 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security – Note by the Secretary-General' (14 July 2021) UN Doc A/76/135

UNGA, 'Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General' (14 September 2011) UN Doc A/66/359

UNGA, 'Road Map for Digital Cooperation: Implementation of the Recommendations of the High-level Panel on Digital Cooperation – Report of the Secretary-General' (29 May 2020) UN Doc A/74/821

UNGA, 'The Right to Privacy in the Digital Age – Report of the United Nations High Commissioner for Human Rights (3 August 2018) UN Doc A/HRC/39/29

UNODC, 'Consolidated Negotiating Document on the General Provisions and the Provisions on Criminalization and on Procedural Measures and Law Enforcement of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes' (Vienna, 9–20 January 2023)

UNSC Res 2322 (12 December 2016) UN Doc S/Res/2322

WTO (Committee on Specific Commitments), 'Report of the Meeting Held on 18 September 2014 – Note by the Secretariat' (15 October 2014) S/CSC/M/71

WTO (Committee on Specific Commitments), 'Report of the Meeting Held on 15 March 2017' (1 May 2017) S/CSC/M/78

WTO (Council for Trade in Services), 'Communication from the US Measures Adopted and Under Development by China Relating to Its Cybersecurity Law' (26 September 2017) S/C/W/374

WTO (Council for Trade in Services), 'Guidelines for Recognition of Qualifications in the Accountancy' (28 May 1997) WT/S/L/38

WTO (Council for Trade in Services), 'Report of the Meeting Held on 2 March 2018' (5 April 2018) S/C/M/138

WTO (Work Programme on Electronic Commerce), 'The E-Commerce Moratorium and Implications for Developing Countries: Communication from India and South Africa' (4 June 2019) WT/GC/W/774

WTO Negotiating Group on Basic Telecommunications, 'Telecommunications Services: Reference Paper' (24 April 1996)

WTO Work Programme on Electronic Commerce, 'Ministerial Decision' (22 June 2022) WT/MIN(22)/32 – WT/L/1143

WTO Work Programme on Electronic Commerce, 'The E-Commerce Moratorium and Implications for Developing Countries: Communication from India and South Africa' (4 June 2019) WT/GC/W/774

WTO Work Programme on Electronic Commerce, 'The Moratorium on Customs Duties on Electronic Transmissions: Need for Clarity on Its Scope and Impact' (8 November 2021) WT/GC/W/833

WTO Working Group on Interaction Between Trade and Competition Policy, 'Communication from the European Community and Its Member States' (25 May 1999) WT/WGTCP/W/115

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

WTO, 'Electronic Commerce Negotiations – Consolidated Negotiating Text' (14 December 2020) INF/ECOM/62/Rev.1

WTO, 'Joint Initiative on Services Domestic Regulation – Reference Paper on Services Domestic Regulation' (26 November 2021) INF/SDR/2

WTO, 'Joint Statement on Electronic Commerce – Communication from Ukraine' (6 May 2019) INF/ECOM/28

WTO, 'Joint Statement on Electronic Commerce – Communication from Cote d'Ivoire' (14 November 2019) INF/ECOM/46

WTO, 'Joint Statement on Electronic Commerce- Submission by Canada' (19 October 2020) WTO Doc INF/ECOM/58

WTO, 'Reference Paper on Services Domestic Regulation – Note by the Chairperson' (27 September 2021) INF/SDR/1

WTO, 'Role of Digital Public Infrastructure in Promoting E-Commerce – Communication from India' (9 February 2023) WT/GC/W/853

WTO, 'Services Sectoral Classification List – Note by the Secretariat' (10 July 1991) WTO Doc MTN.GNS/W/120

WTO, 'The Role of Transfer of Technology in Resilience Building – Communication from Namibia' (3 July 2023) WT/WGTTT/W/34

WTO, 'Work Programme on Electronic Commerce – Progress Report to the General Council' (July 1999) S/L/74
WTO, 'Work Programme on Electronic Commerce' (27 July 1999) S/L/74
WTO, 'WTO Adopts Disciplines on Domestic Regulation for the Accountancy Sector' (14 December 1998) WTO Press Release No 118
WTO, Declaration on the Conclusion of Negotiations on Services Domestic Regulation (WT/L/1129, 02 December 2021)
WTO, Electronic Commerce Negotiations, 'Updated Consolidated Negotiating Text – September 2021' (8 September 2021) INF/ECOM/62/Rev.2
WTO, Exploratory Work on Electronic Commerce, 'Non-paper from Brazil' (25 March 2019) INF/ECOM/3
WTO, Joint Statement on Electronic Commerce, 'Communication from Brazil' (25 March 2019) INF/ECOM/17
WTO, Joint Statement on Electronic Commerce, 'Communication from China' (24 April 2019) INF/ECOM/19
WTO, Joint Statement on Electronic Commerce, 'Communication from Côte d'Ivoire' (25 November 2022) INF/ECOM/70
WTO, Joint Statement on Electronic Commerce, 'Communication from China' (9 May 2019) INF/ECOM/32
WTO, Joint Statement on Electronic Commerce, 'Communication from the European Union' (12 July 2018) INF/ECOM/13

Index