International Trade Law and Global Data Governance

Aligning Perspectives and Practices

Studies in International Trade and Investment Law

Neha Mishra

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 loving 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

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 govern ing data, at both the domestic and transnational levels, focusing on five polic 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 impor tant to global data governance. I conclude this chapter by explaining why th 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 materia produced by abstracting the world into categories, measures, and other represen tations 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-18a361fac3a5.

[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 when 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 routes 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).
[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 a George Washington University) defines data governance as any norms, princ ples and rules governing various types of data.[50] Another definition, offered b Aaronson, is 'principles, policies, standards, laws, regulations and agreement designed to control, manage, share, protect and extract value from various type of data'.[51] The Datasphere Initiative (a multistakeholder network discussing issues of data governance and its impact on human lives) defines data govern ance as the 'development and implementation of policies, standards, law regulations, and agreements that cover the management of data within cou tries and transfer of data across jurisdictional boundaries'.[52] This is similar t the definition offered by Erie and Streinz, who define data governance as 'rules norms, practices, and infrastructures governing the collection, storage, transfe use of, and access to digitalized information'.[53]

For this book, the term 'data governance' refers to different norms, best prac tices, 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, multistake holder 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 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 bind ing 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 digitally 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 ti
time, global data governance is fast evolving into a complex area of both dom
tic and transnational regulation. Thus, it is both timely and relevant to exp
these different interfaces of international trade law and global data governa

III. FREE FLOW OF DATA VERSUS DATA SOVEREIGNTY

The imbalance of economic and political power among countries (and sta
holder groups within those countries) in the global data governance framew
leads to a deep regulatory divide as to how cross-border data flows must
regulated.[71] This section first presents two competing visions for the governa
of cross-border data flows – data sovereignty versus free flow of data – and th
presents the DFFT framework, which can be arguably viewed as a negotia
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 t
need for an interconnected and open Internet lies at the heart of tensions
global data governance and, consequently, influences how different countr
perceive the role of international trade law in the regulation of cross-borde
data flows. The subsequent chapters provide more detail, through various exa
ples, as to how governments operationalise data sovereignty in practice throug
different kinds of data-restrictive measures. The main aim of this section is
highlight the high-level, philosophical conflict between the idea of a free a
open Internet (characterised by the free flow of data) and a regulated Interne
(characterised by state-driven ideas of data sovereignty). This tension can shap
how governments design and implement laws, as well as how they cooperat
among themselves to develop regional or global frameworks on digital trade.

Data sovereignty is a vague term.[72] As Chander and Sun argue, data sove
eignty can be a 'double-edged sword': while it can be used safeguard importa
public interests such as privacy and data security, it can equally be used to repres
and control citizens.[73] In the context of regulating data flows,[74] data sovereignt
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' i
PG Sampath and F Tregenna (eds), *Digital Sovereignty: African Perspectives* (Capetown, Zenod
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 La*
283, 311.

[74] Data sovereignty also applies in other contexts; for instance, it can relate to management an
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. 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 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 Concept' (*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/.