laws

MDPI

Article

Governing Cross-Border Data Flows: International Trade Agreements and Their Limits

Yik-Chan Chin [1,*] and Jingwu Zhao [2]

[1] School of Journalism and Communication, Beijing Normal University, Beijing 100875, China
[2] School of Law, Beihang University, Beijing 100191, China
* Correspondence: yik-chan.chin@bnu.edu.cn

Abstract: In modern international competition and cooperation, digital trade rules centered on the cross-border flow of data have become a competitive advantage for countries. Under the guidance of commercial freedom, the United States chooses to actively promote the free flow of data across borders. The European Union has placed the protection of personal data rights before the cross-border flow of data through the General Data Protection Regulation (GDPR), and developing countries generally reserve space for industry policy interpretation. As one of the world's largest economies, facing the needs of domestic industrial development and the pressure of international systems, China's cross-border data flows' policy is to ensure data flows under the premise of security, protection of personal information, seek international coordination of rules, and the freedom of transmission. The key question, therefore, is how to facilitate interoperability or find a middle ground among the divergent approaches in order to avoid the fragmentation of the digital trade system. The article suggests that a thin and narrowly scoped WTO agreement on e-commerce rules on cross-border data flows with sufficient policy space to accommodate different needs, policy preferences and priorities, and local contexts via legitimate exception provisions would be a welcome movement.

Keywords: cross-border data flows; national security; international digital trade rules; Chinese data rules; US data rules; EU data rules; WTO e-commerce

Citation: Chin, Yik-Chan, and Jingwu Zhao. 2022. Governing Cross-Border Data Flows: International Trade Agreements and Their Limits. *Laws* 11: 63. https://doi.org/10.3390/laws11040063

Academic Editor: Rolf H. Weber

Received: 3 May 2022
Accepted: 4 August 2022
Published: 16 August 2022

1. Introduction

Since the emergence of big data, cloud computing and other information technologies have been widely commercialized, and data have become key strategic assets in the economy and society. Data are not only an economic resource for[1] enterprises to compete in the market but also important production tools to expand personal and social values.[2] In addition to their commercial value; data are often involved in protecting personal privacy and human rights, shaping consensus on decision-making at the social level and maintaining important national security interests. These multi-dimensional characteristics of data have led to a divergence in regulatory and policy approaches of countries regarding data collection, storage, and transfer. The current rules on cross-border data flows are characterized by fragmentation; there is no coherent international framework addressing this situation. In order to develop the potential commercial value of big data, the governments of various

[1] An article in The Economist in 2017 likened data to the "new oil", sparking widespread discussion of the importance of data. See The World's most valuable resource is no longer oil, but data, The Economist (6 May 2017).

[2] See UN Secretary-General António Guterres' foreword to the United Nations Conference on Trade and Development's 2021 report on the digital economy. Digital Economy Report 2021, Cross-border Data Flows and Development: For Whom the Data Flow, https://unctad.org/webflyer/digital-economy-report-2021 (last viewed 30 January 2022).

countries[3] have launched regional or international digital trade dialogues for governing cross-border data flows.

When examining the important trade agreements reached in recent years[4], it is not difficult to find that the governance of cross-border data flows through trade agreements has become the mainstream trend. Whether it is the Regional Comprehensive Economic Partnership (RCEP), which came into effect on 1 January 2022, or the United States–Mexico–Canada Agreement (USMCA)[5], which took effect on 1 July 2020[6], or the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)[7], effective on 30 December 2018, cross-border data flows are obviously one of the core issues of these international digital trade agreements in the context of the digital economy.

The deployment of trade agreements has, however, raised two key problems. First, the data governance paradigms of major trading countries such as the United States, China, and those in the European Union are obviously divergent, forming a new "digital divide"; Such divergence is also reflected in defining the nature of data and various values attached to them by various countries. Secondly, may the continuous development of bilateral or regional trade agreements and the accelerated formation of special international rules for cross-border data flows further aggravate multilateral trade, or may the current fragmentation of the cross-border rule system also lay the foundation for a unified rule system in the future?

The key question, therefore, is how to facilitate interoperability or find a middle ground among the divergent approaches in order to avoid the fragmentation of the digital trade system. In other words, the key research question of the article is how to strike a balance between the various rights, interests, and values attached to the data flows by different state actors in the international digital trade system.

Norms underpinning rules governing cross-border data flows may include privacy protection, protecting public interests and national security, local economic development, the right to access information, and the development of global e-commerce. We argue that policies in this regard should be based on balancing various norms in a contextual, inclusive, proportional, and tiered manner.

To engage in these enquiries, we conducted a study on the US, EU, China, and developing countries' approaches to governing cross-border data flows and analyzed their positions in international trade agreements to observe the interests these approaches and

---

[3] Some scholars believe that digital trade is a new type of trade that accurately exchanges products and services that can be digitally or physically delivered, using data as the key production factor, using digital platforms as carriers, and using digital technologies such as big data, cloud computing, and artificial intelligence. See Tang (2021). Some scholars also believe that digital trade is an economic form based on the Internet, with data flow as the object of transmission or delivery. See Zhu (2021).

[4] Including the United States-Mexico-Canada Agreement (USMCA); Agreement between the US and Japan on digital trade; UK-Japan Comprehensive Economic Partnership Agreement; EU-Japan Economic Partnership Agreement; Digital Economy Partnership Agreement (DEPA) between Singapore, Chile, and New Zealand; Digital trade principles for G7 trade ministers, The Regional Comprehensive Economic Partnership (RCEP); and The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) is a Free Trade Agreement (FTA) between Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, Peru, New Zealand, Singapore, and Vietnam.

[5] RCEP was signed on 15 November 2020 by 15 countries, including China, Japan, South Korea, Australia, New Zealand, and ASEAN (ten countries), representing the core demands of digital trade development in 15 countries, including China. On 1 January 2022, RCEP officially came into effect. The first batch of countries to take effect included the six ASEAN countries, including Brunei, Cambodia, Laos, Singapore, Thailand, and Vietnam, and the four non-ASEAN countries, including China, Japan, New Zealand, and Australia. Among them, Article 15 of Chapter 12 Electronic Commerce deals with "cross-border transmission of information by electronic means". See http://fta.mofcom.gov.cn/rcep/rceppdf/d12z_cn.pdf (last viewed on 30 January 2022).

[6] The USMCA replaces the North America Free Trade Agreement (NAFTA), which adds new content such as Chapter 19 on digital trade. See https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement (last viewed 30 January 2022).

[7] In Chapter 14 Electronic Commerce, Article 14.11 provides for "cross-border transmission of information by electronic means". See http://www.mofcom.gov.cn/article/zwgk/bnjg/202101/20210103030014.shtml (accessed on 30 April 2022).

positions aimed to serve and suggest the possible way forward for a global cross-border data flows' regulatory framework.

The paper begins with a sketch of the drawback of the slow response of the WTO system to the cross-border data flows and three governing models: the United States' free trade system; China's model, aiming to balance data security and free flows of data; the European Union's model, balancing human rights and digital trade. It is followed by examining the sources of differences in the cross-border data flows negotiation, highlighting the developing countries' interests in protecting the right to development as well as the divergence in defining and applying the role of national security in digital trade. The paper then introduces the challenges of global standard-setting in data flows through international trade agreements, the ongoing regional interoperability mechanisms established by various trade blocks, and their limitations and proposes the possible role of the WTO. The paper concludes by pointing out that current trade agreements have regional characteristics and can only be used as a phased plan for governing cross-border flows, and further suggesting that the route for governing cross-border data flows needs to take a broader approach, link the trade with digital rights, and seek a delicate balance between the protection of privacy, legitimate public policy goals, national security, and free flows of data in a tiered, proportional and contextual manner in order to avoid fragmentation. A narrow and thin agreement in cross-border data flow established in the WTO system would be the right way to move such aims forward.

2. The Multilateral Digital Trade System and the Cross-Border Data Flow

Since the multilateral trade rule system has evolved into the institutionalized WTO system, almost all trade issues are within the jurisdiction of the WTO treaty system, and related trade disputes can be submitted to WTO panels and Appellate Body for adjudication and enforcement. In this sense, the WTO rule system is different from general international law and has a certain degree of a "hardlaw "nature.[8.] Not only that, but the WTO is also a multilateral trade negotiation venue[9], which should theoretically be the best venue for resolving disputes related to digital trade and cross-border data flows. In fact, the WTO recognized the importance of digital technology development as early as 1998 and set up a working group on electronic commerce (E-commerce)[10], covering trade in services, trade in goods, trade-related intellectual property rights, and trade and development issues and attempting to promote responsive changes in trade rules. However, the 20 years of efforts have not achieved the expected results.[11] More importantly, the WTO has not sufficiently adapted to the digital trade development because its incapability of addressing many of the contentious issues which block digital trade negotiations due to the fundamental cultural and policy divergency of countries (Burri 2017).

When the multilateral WTO mechanism governing cross-border data flows cannot respond to the real needs of digital trade or the digital economy in a timely and effective manner, countries circumvent the dilemmas through unilateral regulations, bilateral, or regional trade agreements to promote the fragmented legal framework for cross-border data flows due to different considerations such as personal information protection, the promotion of free trade, and the maintenance of national security. Moreover, global cross-border data flows digital trade agreements can be roughly divided into three categories, namely the "trade-first free flow model" of the United States, the EU's "balancing human

[8] See Shaffer and Pollack (2010).

[9] Article 3 of the WTO Agreement stipulates that the WTO shall provide each member with a negotiating forum for dealing with multilateral trade relations in accordance with the agreements in the annexes to this Agreement. If the Ministerial Conference makes a decision, the WTO can also provide a venue for further negotiations among members on issues related to multilateral trade relations. See https://www.wto.org/english/docs_e/legal_e/04-wto_e.htm (accessed on 30 January 2022).

[10] WTO, Work Programme on Electronic Commerce, WT/L/274, 1998. See https://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm (accessed on 30 January 2022).

[11] Except for the Information Technology Agreement revised in 2015 and the Trade Promotion Agreement that came into effect in 2017, almost all WTO agreements remain in the pre-Internet era.

rights and digital trade model", and China's "balancing security, personal data protection and free flows of data model".

3. The United States: Strengthening the Free Trade System

The United States has adhered to the notion of free trade that prioritizes commercial interests over privacy in its digital trade policy. As early as during the Clinton administration, it advocated the "maximum possible free flow of cross-border information", and in the process of international rule-making, it ensured that "regulatory differences between countries will not become substantial trade barriers".[12] In 2002, the United States further proposed the "Digital Agenda"[13], which is a new way to promote the free flow of cross-border data through a series of bilateral[14] and regional free trade agreements.[15] Market access is the core norm of US's trade agreements. US Internet companies have significant and irreplaceable competitive advantages in the global market competition; therefore, the free flows of data or information has become a basic principle of US trade agreements. Specifically, US-led trade agreements generally focus on two issues: the emphasis is on the freedom of choice of individuals (consumers) in digital products and services and the restriction of the state's control over the flows of data.

The most typical example is the Free Trade Agreement between the United States and South Korea, which came into effect in 2012. Its Art 15.8, for the first time, clearly included the free flow of information clause. It "recognizes the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders". Of course, the expression in this article is not binding, and there are no strict definitions on what constitutes an "unnecessary" barrier, but it reflects the position of the United States on cross-border data flows.

Under the leadership and promotion of the United States, the 2016 Trans-Pacific Partnership (TPP) agreement, for the first time, made a binding commitment to free cross-border data flow in the e-commerce chapter. The TPP's chapter 14 on electronic commerce includes several novel commitments, including cross-border data transfers and the forced localization of computing facilities. It makes it clear that each TPP government shall allow the cross-border transfer of information, including personal information, by electronic means, "when this activity is for the conduct of the business of a covered person".[16] It allows a government to adopt or maintain a measure inconsistent with this obligation only "to achieve a legitimate public policy objective", provided that the measure "does not impose restrictions on transfers of information greater than are required to achieve the objective".

Although the United States later withdrew from the TPP agreement, the cross-border data flow rules proposed by it have become a model for more and more international digital trade agreements, not only fully preserved in the 2018 Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) agreement but also in the 2020's United States–Mexico–Canada Agreement (USMCA) digital trade chapter[17].

In addition, the United States submitted a proposal to the WTO's Work Programme on Electronic Commerce in 2019 entitled "The Economic Benefit of Cross-border Data Flow", which once again emphasized the importance of free data flow to global economic development and suggested that the Programme examine the mechanisms that both address

[12] See White House, A Framework For Global Electronic Commerce, 1 July 1997.

[13] U.S. Bipartisan Trade Promotion Authority Act of 2002. See Gao (2018).

[14] These include relationships with Singapore (2003), Chile (2003), Australia (2004), Peru (2006), South Korea (2007), Panama (2012), Colombia (2012), etc.

[15] Mainly the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the United States-Mexico-Canada Agreement (USMCA). Although the United States has withdrawn from the CPTPP, the CPTPP has fully followed the TPP agreement led by the United States.

[16] See TPP article 14.11 Cross-Border Transfer of Information by Electronic Means.

[17] See United States–Mexico–Canada Agreement article 19.11 Cross-Border Transfer of Information by Electronic Means.

privacy issues in a manner that is the least trade restrictive, allowing trade to flourish while preserving legitimate public policy objectives. It also advocated for an international dialogue on approaches that ensure the interoperability of different regulatory regimes.[18]

4. The European Union: An Extraterritorial Jurisdiction Model Balancing Human Rights and Digital Trade

Although the EU attaches great importance to the development of the digital economy and a "digital single market strategy",[19] the EU also considers human rights as the priority norm in dealing with cross-border data flows. The territorial scope of the EU's General Data Protection Regulation (GDPR) is based on two principles. They are the effects principle: the controller or processors are outside the EU but produce substantive effects within the EU territory, and the principle of territoriality: the controller or processor has an establishment on land. For data within the EU, the GDPR requires member states to allow the free flows of personal data between member states on the premise of protecting the right to privacy in relation to the processing of personal data. For data flows involving third-party countries, the EU requires the third-party country to provide an adequate level of protection to personal data equivalent to the GDPR.[20] In addition, the GDPR has a broad extraterritorial scope of application; it will apply to those data controllers or processors that are not established in the EU but provide goods or services to data subjects in the EU or monitor the activities of the data subject taking place within Europe (article 3(2)). Moreover, it shall also apply to processing taking place outside of EU territory if it is being carried out "in the context of activities of an establishment of the controller or processor' located within the EU.

In fact, as early as in the Uruguay Round of GATS negotiations in the last century, the EU insisted that the GATS agreement could not prevent member states from implementing and enforcing laws concerning "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" (Article 14.C.ii, GATS[21]), in order to prevent trade rules from affecting privacy protection. Based on the principle of prioritizing the right to privacy and personal data protection, the EU has adopted strict restrictions on cross-border data flows with third-party countries; that is, only when the third-party country meets the EU's data protection requirements is the cross-border flows of personal data allowed. In other words, the EU's cross-border data flow is conditional, and whether it meets the conditions for "adequate protection" is determined by the EU through the so-called "adequacy decision".[22] This allows the EU to have important legal power when negotiating data protection with third-party countries, international organizations or enterprises, and increase the legal influence of the EU in the data market, in essence, it is the extraterritorial extension of EU data sovereignty (Chin and Li 2021). The EU adopts a restrictive measure

[18] See WTO, The economic benefits of cross-border data flows, Communication from the United States, S /C/W/382, 17 June 2019.

[19] In 2015, the Council of the European Union adopted the "Digital Single Market" strategy, which unifies the digital markets of the 28 EU member states as a whole. Market access (e-trade tier online delivery of goods and services for consumers and businesses within the EU), enabling digital networks and services to thrive (providing high-speed, secure, and trustworthy network infrastructure and services under the right regulatory conditions), support digitalization for growth (building an inclusive digital economy). https://ec.europa.eu/eurostat/cache/infographs/ict/bloc-4.html (last viewed 30 January 2022).

[20] See Article 45 GDPR. 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), http://data.europa.eu/eli/reg/2016/679/oj (last viewed 30 January 2022).

[21] https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm (accessed on 30 April 2020).

[22] Regarding the adequacy decision of the European Commission, the European Parliament and the Council of the European Union may at any time request the European Commission to amend or withdraw the "adequacy decision" on the grounds that they have exceeded their authority to implement the GDPR. As of January 2022, Andorra, Argentina, Canada (limited to commercial establishments), Israel, Japan, New Zealand, South Korea, Switzerland, United Kingdom, Uruguay, Faroe Islands, Guernsey, Isle of Man, Jersey 14 countries and territories have been granted adequacy decisions. See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last viewed 30 January 2022).

of and prudent manner towards cross-border data flows in the name of human rights protection.

It was not until 2002 that the EU introduced non-binding e-commerce clauses in its agreement with Chile, the 2016 Comprehensive Economic and Trade Agreement with Canada included specific provisions for establishing mutual trust in e-commerce[23] and the 2018 Economic Partnership Agreement with Japan, for the first time, cross-border data flow is mentioned in the form of specific clauses, but it is only expressed as: "the two sides agree to 'reassess' the need to incorporate free data flow clauses into the agreement within three years of the agreement's entry into force.[24] " In the draft trade agreement between the EU and Australia, New Zealand, and Tunisia, it tries to prohibit data localization and promote the free flow of data, but it also limits the data flows on the premise of human rights protection. It reflects a certain shift in the attitudes of the EU towards cross-border data flows and trade rules.

In July 2018, in order to solve the compliance concerns of enterprises regarding the cross-border flows of data in digital trade, the European Union issued an *EU proposal for Provisions on Cross-border Data Flows and Protection of Personal Data and Privacy* in the EU trade agreement, clearly explaining the EU' positions on cross-border flows of data in digital trade. Among them, the "cross-border data flows" is a horizontal clause covering all sectors of the economy and covering both personal data and non-personal data. It proposes that contracting parties must be committed to facilitating cross-border data flows. The EU proposed the prohibition of four measures that restrict the free flow of data across borders in digital trade[25]: (1) requiring the use of computing facilities or networks within a member's territory to process data; (2) requiring the localized storage or processing of data within a member's territory; (3) prohibiting the storage or processing of data in another member's territory; and (4) placing the use of member state's computing facilities or data localization as a condition for allowing data to flow.

In the personal data and privacy protection clauses, all parties are clearly required to recognize personal data and privacy protection as a basic human right, and high protection standards can help build trust in the digital economy and promote trade development; the parties have the right to take and maintain such personal data protection measures as they deem appropriate, including formulating and adopting rules for the cross-border transfers of personal data.[26] In the copy submitted to the WTO Working Group on Electronic Commerce, the EU also maintained its consistent position.[27] It is predicted that given the intrusive rules in the GDPR, the EU's regional trade agreements in the future may adopt stronger language on personal data protection (Gao 2021).

5. China: A Territorial and Protective Jurisdiction Model Balancing Security, Personal Data Protection and Free Flows of Data

China's cross-border data flow policy is closely tied with data sovereignty, national security and increasingly personal data protection to maintain the "legal, secure and free flows" of transborder data. Data sovereignty originates from the traditional theory of national sovereignty, which means that a country has the power of jurisdiction and control over the data generated in the country, and enjoys the highest national power to exclude

[23] Comprehensive Economic and Trade Agreement, Canada-EU, Art.16.5, 30 October 2016, OJ(L.11)23.

[24] Agreement between the European Union and Japan for an Economic Partnership, Art.8.81, 27 December 2018, OJ(L.330).

[25] See European Commission, EU proposal for provisions on Cross-border data flows and protection of personal data and privacy, 9 February 2018.

[26] See European Commission, Factsheet-EU provisions on Cross-border dataflows and protection of personal data and privacy in the Digital Trade Title of EU trade agreements, 19 July 2018.

[27] Includes: (1) requiring the use of computing facilities or networks within a member's territory to process data; (2) requiring localized storage or processing of data within a member's territory; (3) prohibiting the storage or processing of data in another member's territory; and (4) placing the use of member state's computing facilities or data localization as a condition for allowing data to flow. See Joint Statement on Electronic Commerce, EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce, Communication from the European Union, INF /ECOM/22, 26 April 2019.

the interference of others, so as to demonstrate the independence and autonomy of the country in data management (Qi and Zhu 2016). Data sovereignty legally guarantees the country's autonomy in regulating domestic data storage, use, processing, and analysis, and ensures that the country's data industry policies and data security rules are in line with the country's national interests. External data sovereignty refers to a country's independence in performing data-related activities in external relations, such as the independent right to participate in the formulation of international rules related to cyberspace data or join relevant international treaties and agreements (He 2019).

China's current data sovereignty and cross-border data flow rules are mainly reflected in the "Cybersecurity Law", "Data Security Law", "Personal Information Protection Law", "Key Infrastructure Security Protection Regulations", "Cybersecurity Review Measures", and most recently in the "Measures for Data Export Security Assessment".

First, China's positions and claims on data sovereignty are reflected in its *Global Initiative on Data Security* (《全球数据安全倡议》), which promotes the proposition of data sovereignty from the aspects of respecting each country's sovereignty, jurisdiction, and data security rights (Ministry of Foreign Affairs of China 2020). It proposes that countries must not require domestic enterprises to store the data generated or acquired abroad in the country. Countries should respect the sovereignty, jurisdiction, and security management rights of the data of other countries and shall not directly obtain data located in other countries from enterprises or individuals without the permission of the laws of other countries. By March 2021, Russia, Pakistan, Cambodia, ASEAN, Arab League, and other countries and regional organizations have clearly expressed their support for the *Global Initiative on Data Security*. The United States and Europe questioned it on the grounds of lacking the consideration of human rights and privacy rights and believed that China intends to replace the existing international governance structure of cyberspace (Zhang and Peng 2022).

Secondly, China promotes the "legal, secure and free" cross-border flows of data.

It is worth noting that the *Data Security Law of China* is aimed at "regulating data processing activities", "guaranteeing data security", "protect the legitimate rights and interests of individuals and organizations, and safeguarding national sovereignty, security and development interests"[28]. This legislative principle expands the concept of data security from the perspective of "adhering to the holistic approach to national security and establishing a sound data security governance system" to improve the ability to ensure data security. Data security not only includes the traditional ability to effectively guarantee the integrity, confidentiality and availability of the data itself, but also links with national security and sovereignty, the rights and interests of individuals and organizations, and national economic development.

This and other expansions of the concept of data security as we shall see from the below Section 6.3 show that in the era of digital economy, the discussion of data security policies and regulations also expands from the security of data itself, and the data rights and interests of natural and legal persons, to include the impact of data on national sovereignty, national security and economic development.

The *Data Security Law of China* also requires the state to establish a data classification and grading system according to the importance of the data to economic and social development and the degree of harm caused to national security, public interests, or individuals' or organizations' legitimate rights and interests once that data are tampered with, destroyed, leaked, or illegally obtained or used.

Data are classified according to different types and applied different compliance requirements, including standard contracts, the security assessment of data export, and the restrictions or prohibitions of data export. They include:

(1) Requests for data from foreign judicial/law enforcement agencies;

[28] Article 1, Data Security Law of China, 10 June 2021, http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml (accessed on 20 April 2022).

(2) Requirements of international treaties or agreements;
(3) General data processors handle personal information;
(4) General data processors export important data overseas;
(5) Key information infrastructure operators process personal information and important data;
(6) Personal data processors process personal information that reaches one million people;
(7) Personal data processors accumulatively provide personal information of more than 100,000 people or sensitive personal information of more than 10,000 people abroad.

Data related to national security, the lifeline of the national economy, important to social livelihood, and major public interests are the important data and are subject to stricter regulation[29].

Newly enacted *Personal Information Protection Law* 《个人信息保护法》also stipulates regulations for cross-border personal information flows[30]. Article 38 states the compliance conditions for exporting personal data due to commercial needs; the data processor needs to fulfill one of the four conditions: (1) passing the security assessment in accordance with the provisions of Article 40 of this Law; (2) obtain personal information protection certification; (3) entering into a contract with the overseas recipient in accordance with the standard contract formulated by the national cyberspace administrative authority, stipulating the rights and obligations of both parties; (4) other conditions stipulated by laws, administrative regulations, or rules of authority.

China's *Cybersecurity Law* (《中华人民共和国网络安全法》) requires that critical information infrastructure operators that collect and generate personal information, and important data, shall be stored in the territory of China in general. For cross-border data flows due to their commercial needs, a security assessment is required.[31]

The new 2022 initiative of *Data Export Security Assessment Measures*《数据出境安全评估办法》clearly defines four types of cross-border data flows that require security assessment:

- Important data export by data processors;
- Personal information exported by key information infrastructure operators or data processors process personal information reaches one million people;
- Personal information exported by data processors accumulatively provides personal information of more than 100,000 people or sensitive personal information of more than 10,000 people abroad since the previous year;
- Other situations require by the national cyberspace administration department (Cyberspace Administration of China 2022).

The security assessment in the *Measures* focuses on the risks that data export may bring to national security, public interests, the legitimate rights and interests of individuals or organizations, and the legality, legitimacy, and necessity of the purpose, scope, and method of data export. Furthermore, it also assesses whether the safeguard measures meet the requirements of the laws, administrative regulations, and mandatory national standards of China.

Thirdly, the *Data Security Law* 《中华人民共和国数据安全法》adopts a jurisdiction model based on the "territorial plus protective" principles in response to the extraterritorial reach of other countries' data laws. The protective principle actually recognizes that a state can exercise extraterritorial jurisdiction over acts that do not occur within its territory. Article 2 of the *Data Security Law* stipulates that the law applies to data activities within the territory of China, i.e., the principle of territory. For organizations and individuals

[29] Article 21, Data Security Law of China, 10 June 2021, http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml (accessed on 20 April 2022).
[30] Personal Information Protection Law of China, 20 August 2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml (accessed on 20 April 2022).
[31] Cybersecurity Law of China, 7 November 2016, http://www.cac.gov.cn/2016-11/07/c_1119867116.htm (accessed on 20 April 2022).

outside China carrying out data activities that harm the national security, public interests, or the legitimate rights and interests of citizens or organizations of China, they shall be investigated for legal liability in accordance with the law, i.e., the protective principle.

China is the contracting state of the "Regional Comprehensive Economic Partnership" (RCEP). In 2021, China officially applied to join the CPTPP and DEPA. However, some CPTPP contracting states have doubts regarding China's current regulations on cross-border data flows and data localization. This is because the CPTPP has imposed strict restrictions on the issue of data localization. In terms of cross-border data flow, Article 14.11 of the CPTPP acknowledges that each contracting party may have its own regulatory requirements for cross-border data flows, but in principle, cross-border transfers of information by electronic means should be permitted. Except for special circumstances, such as to achieve legitimate public policy goals, each party may take exceptional measures for cross-border data flows, but these exceptional measures should not be arbitrary, discriminatory, or disguised and also need to pass the necessity test. On the other hand, it is also argued that China is entirely capable of managing the requirements of the CPTPP as ample exceptions and wide loopholes would ease China's compliance with the more challenging provisions, and China's accession would be a bold strategic gambit with important geopolitical ramifications[32].

Similar concerns are shown by members of DEPA; two modules—Article 4.3 on the cross-border transfer of information and Article 4.4 on the location of computing facilities—are flagged as the most problematic for China's accession. However, as SMU Professor Henry Gao has pointed out, Annex 14.A1 carves both provisions out of dispute settlement. Annex 1 goes further to say that both modules "do not create any rights or obligations between or among the Parties under this Agreement". Hence, it is certainly possible for China (or any other potential applicant) to join DEPA and restrict the cross-border flows of data or require local data hosting (Elms 2021).

According to the report "How Barriers to Cross-border Data Flows Spread Globally, Costs and How to Solve These Problems", released by the ITIF, an American think tank, China's cross-border data policies are among the strictest in the world, and it questions China's "security assessment." However, in fact, based on considerations of national security and public interests, the number of countries/regions that require data localization has almost doubled to 144, which is a general trend; in fact, there are very few cases in China where the export of data is completely prohibited, the vast majority of data can be legally exported after meeting the requirements of security assessments, security certifications, standard contracts, etc. It has been criticized that the US has misinterpreted China's digital security proposition as data localization and ignored the fact that China is promoting cross-border data flows on the premise of security (Zhang and Peng 2022). In China's Joint Statement on Electronic Commerce to the WTO, it states that "trade-related aspects of data flow are of great importance to trade development. However, more importantly, the data flow should be subject to the precondition of security, which concerns each and every Member's core interests. To this end, it is necessary that the data flow orderly in compliance with Members' respective laws and regulations"[33].

[32] Members are allowed to impose restrictions on cross-border data in order to achieve a "legitimate public policy objective" (Article 14.11). The prohibition on required source code transfer is limited to mass-market software and does not apply at all when it is used in "critical infrastructure". Members are also permitted to require source code modification in order to comply with local law (Article 14.17). Furthermore, the prohibition of data localization requirements does not apply when there is (again) a "legitimate public policy objective" (Article 14.13). China has consistently demonstrated an expansive interpretation of what actions are justifiable under the pretext of public policy objectives (Olson 2021).

[33] Joint Statement on Electronic Commerce, Communication from China, 23 April 2019, INF/ECOM/19, Paragraph 4.3.

6. The Sources of Differences in the Cross-Border Flows of Data Negotiations: What Rights and Interests Are Protected?

6.1. The US, EU and China

The diverging approaches between the US, EU, and China reflect the differences in their commercial interests and regulatory approaches (Gao 2021). The US aims to protect its pure digital service-oriented firms in the global e-commerce market. As China's major e-commerce firms are trading physical goods, China focuses on traditional trade in goods enabled by the Internet. The EU's stricter privacy regulation is seen as a form of digital protectionist measures (Aaronson 2015) to fend off competition from both the US and China (Chin and Li 2021).

Regulatorily speaking, the US is characterized by its "permissive legal framework", which minimizes government regulation on the Internet and relies heavily on the self-regulation of companies. China's internet has been subjected to heavy state legal regulations and co-and self-regulations (Chin 2018, 2020; Chin et al. 2022). The European Union has a long tradition of human rights protection, but it has no major digital players dominant in the global e-commerce market and also lacks a strong central government to override security issues[34].

6.2. Developing Countries: Protect the Right to Development and Maintain Industrial Autonomy

Compared with the EU and other countries, developing Asian countries represented by ASEAN, India, etc., when formulating their own cross-border data flow rules and policies, consider the development of their own digital industries and national security interests more. Providing data export shall not damage the sovereignty and national interests of the country; they then clarify the conditions or scenarios for data export. For example, at the G20 Japan Summit held in 2019, 24 countries, including the US, China, Russia, the EU, Latin America, and East Asian countries, signed the "Osaka Declaration on Digital Economy", stressing that by continuing to respond to privacy, data protection, intellectual property, and security-related challenges can further facilitate the free flow of data and enhance the trust of consumers and businesses(i.e., "Data Free Flow with Trust")[35]. Furthermore, the declaration also urges us to respect "legal frameworks both domestic and international" and "cooperate to encourage the interoperability of different frameworks", and "the role of data for development". However, four significant developing countries, i.e., India, Egypt, Indonesia, and South Africa, did not participate.

Developing countries in Asia point to the right to development, questioning how they will improve the digital divide, enhance digital capacity building, and promote the development of the digital economy and digital trade to avoid squeezing the development space of their own industries and weakening their international voice in the field of digital trade. India refused to support this initiative; its Commerce and Industry Minister, Piyush Goyal, argued that 'developing countries need time and policy space to build deepest understanding of the subject and formulate their own legal and regulatory framework before meaningfully engaging in e-commerce negotiations'. Goyal reiterated India's policy favoring data localization and recognizing that data are a national asset, not primarily an individual right. Furthermore, data are a 'new form of wealth', which is important for development, and digital trade negotiations need to take into account the requirements of developing countries (Greenleaf 2019). In addition, the African Group also pointed out in the report submitted to the WTO e-commerce working group that "the world is confronted with the reality of a deep, persistent and widening digital divide". If this is not addressed, it will drive further technology, income and infrastructural divides". They observed "extremely high market concentration levels existing in the current global e-commerce space—evident both in terms of how e-commerce trade is distributed across

[34] n.43.

[35] See G20, Ministerial Statement on Trade and Digital Economy, Tsubuka, Ibaraki, Japan, 9 June 2019, https://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157920.pdf (accessed on 20 January 2022).

the global economy, and in terms of the number of firms that dominate this space, notably in terms of market capitalization". Developing countries need to use "active policies and deliberate efforts", including institutional tools such as data localization, Internet filtering, and technology transfer requirements (i.e., disclosure of source code) to develop the necessary infrastructure, manage digital flows to enable national digital catch up, and create, cultivate and develop their own digital industries through "smart industrial policy" or "powerful protectionist tools"[36]. The group stands against the attempt to introduce a "digital trade agenda" in the WTO multilateral framework as it will constrain the ability of governments to implement industrial policy and catch up, and argues that the asymmetrical nature of the global digital economy requires the policymakers to focus on equity but not only efficiency if inclusive and sustainable growth is to be achieved, and attempts to curtail developing countries' policy space would prevent them from building the capacities and skills to close the widening technological gap.

Although developing countries generally have a skeptical attitude towards cross-border data flow in international trade agreements, in the context of the transborder nature of the digital economy, it is in line with the interests of national economic development to seek international collaboration to resolve the issue. Therefore, in the RCEP signed by ASEAN in November 2020, its Chapter 12 "Electronic Commerce" section specifically provides for the "cross-border transmission of information by electronic means" clause. It considers and respects that "each contracting party may have its own regulatory requirements for the transmission of information by electronic means"[37]; on this basis, "a contracting party shall not prevent covered persons transmitting information electronically across borders for the conduct of business"[38]. Compared with the digital trade rules dominant in the US and the EU, the RCEP provides for a more flexible legitimate public policy and essential security interest exceptions[39], proposing that the need to implement legitimate public policies should be determined by the implementing party. It thus empowers the contracting party to decide what constitutes a "legitimate public policy" (Hong 2021a); at the same time, it also stipulates that any measures that the contracting party deem to be essential and necessary to protect its basic security interests shall not be prevented and that other contracting parties shall not object to such measures.[40] It can be seen that the RCEP's rules regarding cross-border flows of data have left room for policy adjustment for all parties to safeguard their own legitimate interests and ensure national data security. In addition, considering that the constitution of RCEP's contracting states is relatively complex, especially including the underdeveloped countries such as Cambodia and Laos, the RCEP has flexibly handled the terms of cross-border data transmission, providing some countries with a five-to-eight year buffer period.[41]

6.3. Divergency in the Role of National Security in the Digital Trade

The question of the role of security in digital trade has been subjected to mounting pressure that pushes to address it more deliberately in recent years. Two divergent schools of thought are presented (Olson 2022): (1) security considerations should be given little concern in trade, as linking trade and security will threaten globalization and trade interdependence. In addition, security exceptions in international trade agreements are used as

[36] See Work Programme on Electronic Commerce Report of Panel Discussion on "Digital Industrial Policy and Development", Communication from the African Group, JOB /GC/133, 21 July 2017.

[37] Chapter XII, Article 15(1) of the Regional Comprehensive Economic Partnership Agreement.

[38] Chapter XII, Article 15(2) of the Regional Comprehensive Economic Partnership Agreement.

[39] Article 15(3) of Chapter XII of the Regional Comprehensive Economic Partnership Agreement.

[40] Chapter XII, Article 15(3) of the Regional Comprehensive Economic Partnership Agreement.

[41] With regard to the obligation that "a Party shall not prevent covered persons from transmitting information by electronic means across borders for the conduct of business", the RCEP provides that Cambodia, the Lao People's Democratic Republic, and Myanmar, shall, on the date of entry into force of this Agreement, The application of this subsection shall not be required for a period of five years, and may be extended for a further three years if necessary. Vietnam shall not be required to apply this paragraph within five years from the date of entry into force of this Agreement.

tools to justify various restrictive trade and investment measures and to circumvent international communities by governments in FTAs. The notion of national security is expanded to cover not only military or defense interests but also other areas, such as food security, energy security, cyber-security, climate security, and recently, health security (Heath 2020; Mishra 2020); (2) the inevitable intertwining of trade and security as trade has become a means to pursue or protect technological preeminence and military capability. Moreover, trade also enables countries to accumulate the national wealth required to forcefully project strategic interests on the global stage.

At the same time, self-selected trade blocs take the lead in formulating regional e-commerce free trade agreements that also include national security exceptions. CPTPP's Article 29.2 provides security exceptions; it reads, "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". It is argued that this provision essentially permits any restrictive action taken to protect "essential security interests", countries implementing security assessment on the export of important data or data generated by critical infrastructure operators could invoke this "expansive, self-judging national security exception" if other exceptions in the e-commerce chapter cannot provide sufficient flexibility (Olson 2021). However, it has been warned that the invocation of this provision will have a significant impact on the role of national security in digital trade agreements, and countries must avoid the casual use of such security exceptions to resolve cybersecurity or economic issues (Heath 2020; Mishra 2020).

The aforementioned debates raised important questions in defining the role of national security in digital trade negotiations. What cybersecurity measures are deemed to be incompatible with digital trade agreements? Should cybersecurity be treated as a national security issue to qualify the national security exception, or should it be treated as a public policy issue to qualify for the public policy objective exception? Is the national security exception a self-judging provision?

First, it is argued that cybersecurity measures that restrict the cross-border flows of digital services and that require data localization are trade barriers since they hinder a foreign companies' cross-border supply of services, disrupt their global data and cybersecurity operations, and reduce their competitiveness. Thus, such measures may violate international trade agreement obligations, such as obligations on market access, non-discrimination, transparency, and domestic regulation (Meltzer 2019). However, as we argued in the previous section, developing countries have different opinions on these issues. Historically, many states have not supported US and EU efforts to facilitate the free flow of information in the 20th and 21st centuries because of the concerns that US domination in both the Internet economy and Internet governance could serve to fulfill its self-interests. Moreover, questions of when restrictions on data are necessary and when they are protectionist are also subject to disagreements amongst states (Aaronson 2015). It is argued that data security is an important integrated part of national security.

Recently, 55 submissions from 77 participants to the WTO's Joint Statement Initiatives by February 2020 showed that not all developing countries agree on the free cross-border data flow principle. Some developing countries are more reluctant due to either security or economic concerns. Even for countries that agree with this principle, they see such freedoms often reserved for the provision of covered services or investment only, and exceptions must be provided on grounds ranging from privacy protection to the special needs of specific sectors, such as financial services (Gao 2021).

Secondly, should data security and economic security be treated as a national security issue to qualify for the national security exception? In practice, countries have increasingly adopted a broad understanding of 'national security', one which potentially encompasses both military and economic security and includes both traditional, e.g., military threats, and

non-traditional, e.g., poverty, trade, economy, human rights, and environmental security domains. Data security is considered an integral part of national security since it is closely related to a nation's economic operation, social governance, public services, national defense, and security. Data leakage, loss, and abuse will threaten national security and social stability. Data security has become the focus of the strategic planning of major economies in the world, taking both national security and the development of the digital economy into account. The *Federal Data Strategy* and the *2020 Action Plan* and the *Department of Defense Data Strategy* of the United States stress "the development of data as a strategic resource" and taking strict measures to protect the security of important data and build a national security barrier. The *European Data Strategy*, *European Data Governance Act*, and *European Data Act* intend to ensure data security, improve data sharing mechanisms in the EU internal market, and the liquidity and accessibility of data in order to fully unleash the potential of the European digital economy (Dr2 Consultants 2022; Wei 2022). The collection of sensitive personal data by private or state-owned firms is increasingly being viewed as a national security issue.[42] China's *Cybersecurity Law* and *Data Security Law* also contain provisions to control domestic important data resources and to assess important data and a large amount of personal data's "risk of being stolen, leaked, damaged, illegally used and illegally export", and the risk of being subject to "foreign government influence, control, and malicious use"[43]. In June 2020, the Ministry of Information Electronics and Technology of India invoked Section 2009 of Part 69A of the *Information Technology Act* to prohibit users from accessing 59 Chinese mobile applications in India on the grounds that these mobile applications are stealing and surreptitiously transmitting user data in an unauthorized manner to overseas servers, which may damage India's sovereignty, national security, and public order.[44] National-security authority is used by states to regulate the collection, aggregation, and transfer of personal data (Heath 2020). For instance, in the United States, the interagency Committee on Foreign Investment in the United States (CFIUS) is mandated to review any foreign investment in any US business that "maintains or collects sensitive personal data" of US citizens.[45] In addition, domestic industrial policy that aims to protect emerging or declining industries is increasingly being used by governments for national security reasons (Heath 2020). The ban on the use of Huawei devices in 5G networks in the UK, Australia, New Zealand, and the US is based on security reasons. Furthermore, the Trump administration's declaration that "economic security is national security", and the recent invocation of Article XXI of the GATT also signals that the United States has shifted towards a version of national security that embrace a conception that equates security with economic self-sufficiency and competitiveness.[46] Thus, Heath argues that the securitization of industrial policy, i.e., a wide range of state interventions into the economy is justified on the grounds of security, could accelerate further clashes with trade rules. However, the open-ended and more flexible security exceptions in the CPTPP and the recent US–Mexico–Canada agreement, "seem to provide scope for justifying most, if not all, cybersecurity measures". Given the broad scope of the security exception, the range of measures that

[42] For instance, Carl O'Donnell, Liana B. Baker & Echo Wang, Exclusive: Told U.S. Security At Risk, Chinese Firm Seeks to Sell Grindr Dating App, Reuters, 27 March 2019 (accessed on 30 April 2022); And the European Commission connected its policies relating to data privacy "ultimately on the Commission's many concerns about EU Members' regional, national, and economic security." Desierto (2018).

[43] Cybersecurity Review Measures of China, Provision 10, article 5&6, 28 December 2021, http://www.cac.gov.cn/2022-01/04/c_1642894602182845.htm (accessed on 30 April 2022).

[44] Ministry of Electronics & IT, Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defense of India, security of state and public order, 29 June 2020, available at: https://pib.gov.in/PressReleasePage.aspx?PRID=1635206 (accessed on 20 January 2022).

[45] Foreign Investment Risk Review Modernization Act of 2018. Subsequent regulations explained that this provision covers, among other things, any business that maintains or collects certain types of data, including financial, health, email, and chat data, on more than one million persons or plans to do so. Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 85 Fed. Reg. 3112 (17 January 2020).

[46] White House, National Security Strategy of the United States, 17, 19, December 2017; White House, A Proclamation on Adjusting Imports of Steel into the United States, 8, 31 May 2022; U.S. Department of Commerce, the Effect of Imports of Steel on the National Security, 55–57, 11 January 2018.

could be justified in this way, and the much-underdeveloped relationship between trade norms and security exceptions, the current presentation of security and trade in the FTAs is problematic.

Neha Mishra stands against the position of assuming cybersecurity to be national security to qualify for the national security exception in trade agreements for several reasons, including the fact that cybersecurity-related laws do not draw a rational distinction between military and social/economic security and to distinguish legitimate security measure from other legitimate non-security measure is, however, necessary. The latter can be justified under the general exception rules, such as compliance with domestic data protection laws, or to achieve legitimate public policy objectives through a more demanding test, which requires to 'weigh and balance' different factors, such as the policy objective, the impact of the measure, and the proportionality of the trade-restrictive measure. She urges instead for greater international policy coordination and diplomatic dialogues to resolve their differences regarding cybersecurity governance, including transnational and multistakeholder dialogues that facilitate co-Cin cybersecurity.

Thirdly, is GATT art XXI/GATS art XIVbis, or a similar security exception, a self-judging provision and, thus, outside the purview of the judicial review of a trade-dispute settlement body? Although it is argued that no state in the international community seriously challenges the self-judging nature of the security exception in GATT Article XXI, especially the United States' use of the national security justification in its presidential proclamations on tariffs against steel and aluminum imports and claims that "national security issues are political and not appropriate for the WTO dispute system" (Desierto 2018). The GATT's tribunal did not seem to support this position. In an adopted report (US—Trade Measures Affecting Nicaragua), the GATT tribunal inferred that GATT art XXI would be redundant if it were entirely self-judging:

> *If it were accepted that the interpretation of Article XXI was reserved entirely to the contracting party invoking it, how could the CONTRACTING PARTIES ensure that this general exception to all obligations under the General Agreement is not invoked excessively or for purposes other than those set out in this provision?*[47]

In other words, the use of 'essential' in the security exception provision implies that the level of security interests should be higher than the usual security interests. The WTO Panel in Russia—Traffic in Transit—further reinforced this principle.[48] The report asserts that "Essential security interests" are evidently a narrower concept than "security interests"; it "may generally be understood to refer to those interests relating to the quintessential functions of the state, namely, the protection of its territory and its population from external threats, and the maintenance of law and public order internally"[49].

Importantly, the Panel held that the security exception must be invoked by the Members in 'good faith.' Meaning that Members cannot use the security exception to circumvent their obligations under WTO law.[50] This would mean that Members are required to articulate their essential security interests with sufficient specificity for Panels to determine the veracity of their claims.[51] This panel report of April 2019 is seen as a historic ruling for the WTO and for trade law generally, as it categorically rejected the proposition that the GATT security exception was self-judging (Heath 2020).

On the other hand, the WTO's experience, especially the responses from the developing and less developed countries, also shows that in order to provide the accepted certainty and clarity of the role of security in digital trade, it is first essential to understand how changing understandings of trade and security at the national level reflect or clash with the

47 United States—Trade Measures Affecting Nicaragua, 13 October 1986 (unadopted report), GATT Doc. L/6053 [5.17].
48 Panel Report, Russia –Traffic in Transit [7.72].
49 Panel Report, Russia –Traffic in Transit [7.130].
50 Panel Report, Russia –Traffic in Transit, [7.133].
51 Panel Report, Russia –Traffic in Transit, [7.134].

changing shape of global economic governance (Heath 2020). Secondly, the relationship between the varying notions of cybersecurity, data governance, and international trade law needs to be examined; For instance, China's recent "Global Initiative on Security" (Wang 2022). proposes that to maintain world peace effectively, the security of both traditional and non-traditional areas (such as climate change, cybersecurity, and biosecurity) needs to be maintained. With economic globalization, the connotations and extensions of the concept of security are more abundant than before and are characterized by connectivity, transnationality, and diversity, and require innovations in conceptualizations and international cooperation. Thirdly, innovative ways (Heath 2020) need to be created to reconcile the expanded security issues with trade obligations, whether through institutional mechanisms or through cyber-diplomacy and international regulatory cooperation mechanisms.

7. Challenges of Global Standard Setting

It is increasingly recognized that the right balance between capturing the immense economic value of data, which a light-touch regulatory mechanism may better facilitate, and safeguarding national security, data privacy, and the other digital rights of citizens needs to be struck by governments (Taheri et al. 2021). Meanwhile, it is argued that inconsistent, contradictory, or incompatible cross-border data policies are the sources of the biggest risks for the digital economy, and efforts are needed to consolidate the rules around similar frameworks; however, currently, there are limited arenas for managing these challenges (Elms 2021).

It is true that the CPTPP, RCEP, and DEPA, as the latest products of the international rules for the cross-border flow of data, have reserved public policy space for governments of various countries, but these agreements have regional characteristics and can only be used as a phased plan for governing international cross-border flows.

Moreover, the negotiations on the rules of the cross-border flows of data will be difficult as there are obvious conflicts in the national interests between developing countries and developed countries and also between geopolitical powerhouses. Historically, developed countries are much more experienced in using international economic and trade rules in the process of negotiating with developing countries to better serve their national interests. It is also argued that the US government attaches great importance to using international rules to put pressure on China and deliberately isolated and interfered with China's participation in the international economic community and trade-rule-making, excluding China from the formation of a regional interoperability mechanism for cross-border data flows (Liu and Gong 2013; Sun 2016). The Information Technology and Innovation Foundation advocates to disqualify China " from playing a role in global rule-setting activities for digital trade" if China cannot or does not propose clear, binding, and meaningful commitments on data flows as data flows should be central to any WTO ecommerce outcomes and China lacks of any sort of track record on making commitments supporting data flows (Cory 2019). This has been seen as another type of exclusion. However, China's cross-border data rules will inevitably affect the direction of international cross-border data rules, engaging with China to become part of a community crafting shared norm- and rule-creation for the future is inevitable too.

One of the solutions to reconcile such divergence is to establish compatibility mechanisms; for instance, for privacy standards, these mechanisms could include (1) the mutual recognition *of regulatory outcomes* agreements; (2) a reliance on international standards; (3) a recognition of comparable protection afforded by domestic legal frameworks or certification frameworks; (4) other ways of securing the transfer of data between the Parties (Drake-Brockman et al. 2021), the interoperability mechanism is one of them.

8. The Establishment of Regional Interoperability Mechanisms

The United States, the European Union, Japan, South Korea, and other developed countries have sought new ways of cooperation to establish cross-border data flow interoperability mechanisms that facilitate participation. First, the United States and European

Union have tried many times to establish a cooperation mechanism for cross-border data flows. On 25 March 2022, the European Commission and the United States announced that they have agreed in principle on a new Trans-Atlantic Data Privacy Framework and will finalize the details of this agreement in principle and translate it into legal texts (European Commission 2020, 2022).

Second, the United States uses the Asia-Pacific Cooperation (APEC) Cross-Border Privacy Rules (CBPR) as a framework to continuously expand the scope of data flows. CBPR is a voluntary cross-border privacy mechanism implemented between the APEC members. The participating companies abide by the personal data protection rules in the APEC Privacy Framework adopted by the APEC Leaders Meeting in 2005 and revised in 2015. In principle, businesses can demonstrate compliance with internationally recognized privacy protection standards by joining the CBPR. This mechanism does not change the domestic personal data legislation of each country but requires the participating economies to sign the "Cross-Border Privacy Enforcement Agreement" to facilitate law enforcement.[52] As of now, among the 21 economies of APEC, eight countries and regions, including Australia, Chinese Taipei, Canada, Japan, South Korea, Mexico, Singapore, and the United States, have joined the mechanism. Substantial cooperation through the CBPR has already begun between the United States and Japan. In addition, Japan, South Korea, and Canada, which are members of CBPR, have also passed the adequacy tests of the EU's GDPR.

The United States not only seeks to expand the scope of CBPR within APEC but also seeks to expand CBPR beyond APEC, especially to promote the interoperability between CBPR and GDPR. In the USMCA, in addition to the provisions concerning "cross-border data flows", the contracting parties also added the requirement to recognize CBPR as an effective mechanism for promoting cross-border information transfer in the "personal information protection" clause. This is equivalent to accepting the relevant principles of the CBPR as a uniform standard of protection among the contracting states in authorizing the export of personal data.[53]

On 21 April 2022, the US, together with Canada, Japan, the Republic of Korea, the Philippines, Singapore, and Chinese Taipei, established the Global CBPR Forum to promote the expansion and uptake of the Global CBPR and Privacy Recognition for Processors (PRP) Systems globally to facilitate data protection and the free flow of data, and pursuing interoperability with other data protection and privacy frameworks. The forum will "establish an international certification system based on the APEC CBPR and PRP Systems; "first-of-their-kind data privacy certifications that help companies demonstrate compliance with internationally recognized data privacy standards" (US Department of Commerce 2022). However, a criticism is that the CBPR's personal data protection depends on the APEC Privacy Framework. The level of personal information protection provided by the APEC Privacy Framework is very limited. The first APEC Privacy Framework was built on the basis of the OECD Guidelines from the very beginning, and the revision of the APEC Privacy Framework in 2016 was mainly aligned with the 2013 version of the OECD Guidelines. Therefore, the nine principles contained in the APEC privacy framework belong to the level of the first generation of personal data protection legislation. Through the establishment of a cross-border flow order of personal data based on low-level protection, the CBPR could ensure that countries will not restrict cross-border personal data flows on the grounds of a domestic country's high level of protection and ultimately facilitate the convergence of personal data to the US or US companies (Hong 2021b).

Third, the EU continues to expand the scope of its cross-border data flow. The EU promotes bilateral international cooperation by prioritizing the adoption of adequate decisions in the GDPR. As of April 2022, the European Commission has recognized 14 countries'

[52] See APEC, What is the Cross-Border Privacy Rules System? 15 April 2019. available at: https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System (accessed 20 January 2022).

[53] See United States–Mexico–Canada Agreement Article 19.8.2.

adequate level of personal data protection.[54] In the current and future negotiations, the European Commission has also prioritized negotiation and cooperation with India, Indonesia, some Latin American countries (such as Brazil and Chile), and neighboring countries in Eastern and Southern Europe. The EU has discussed with more countries the possibility of establishing a multilateral data flow on the basis of *The Council of Europe Convention for the Protection of Individuals with Regard to the Processing of Personal Data* ("Convention 108+"). In 1981, the member states of the Council of Europe signed Convention 108, which was modernized in 2018 ("Convention 108+"), and joining the Convention will be regarded as an important reference for meeting the EU's "adequate protection" standard for cross-border data flows. Overall, 55 countries have joined the Convention by 2022 (Council of Europe 2019; Wang 2018, No. 3).

Fourth, other developed countries such as Japan and South Korea have actively joined the US–Europe data flows' interoperability mechanism in order to pave the way for their digital economies. Japan is very active in the cross-border flows of data between the United States and Europe and hopes to act as a bridge connecting the United States, the European Union, and other economies. Japanese Prime Minister Abe proposed the concept of "trusted data free flow with Trust" at the Davos meeting in early 2019 and promoted it to become a consensus in the G20 "Osaka Declaration on Digital Economy".[55] In recent years, South Korea has systematically revised domestic laws and regulations on personal information protection many times and passed the adequacy decision of the EU in December 2021.

The competing regional interoperability mechanisms have strengthened greater international regulatory cooperation; however, they are still largely aligned with the composition of geopolitical power and existing trade blocks and are not able to resolve the fundamental problem of establishing an international regulatory framework for governing cross-border data flows to avoid fragmentation. Global standard-setting for cross-border data transfers must be built on another more balanced and inclusive international mechanism.

9. The Role of the WTO in Defining International Rules in Data Flows

It should be noted that having international data cross-border flow regulations does not require all countries to adopt the same level and the same cross-border data rules but emphasizes the institutional goal of achieving the global flows of data. The key factors hindering data flow are not the so-called "data localization" or vague "national security" exceptions because these are subject to sovereign states' policy choices; international regulatory, cross-border flow rules first need to solve the problem of consensus; that is, what model, what scope, and what path of cross-border data flow can be generally agreed upon by various countries. For the digital economy, countries have no reason to suppress the free flow of data as an economic resource, but how to find a delicate balance among the cross-border flows of data, the legitimate policy goals of various states, and individual digital rights in a contextual, inclusive, proportional, and tiered manner has become a practical problem that needs to be solved urgently. To achieve this, we argue that the WTO has an important role to play since it operates on the principles of non-discrimination, which can potentially address the international rules on data flows even better than new tailor-made regulations in the FTAs that may often be adopted as a reaction to strong vested interests (Burri 2021).

The negotiation of e-commerce in the WTO has made some, despite slow progress. The current negotiations are under the Joint Statement Initiative (JSI) on Electronic Commerce, which was embarked upon in 2019 by 76 WTO Members in order to move towards a digital trade agreement. The negotiations are co-convened by Australia, Japan, and Singapore. Currently, 86 WTO Members representing over 90% of global trade, all major geographical regions, and levels of development are participating in these negotiations. In May 2021, the

[54] See European Commission, Adequacy decisions How the EU determines if a non-EU country has an adequate level of data protection, available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed on 20 January 2022).

[55] See G20 Ministerial Statement on Trade and Digital Economy, 9 June 2019.

JSI co-conveners revealed that a clean text on open government data, e-contracts, online consumer protection, and paperless trading was within reach and will seek expedited progress in the negotiations, including on the key issues of data flows and data localisation.

In a statement issued on 13 June during the 12th WTO Ministerial Conference, the JSI, together with Switzerland, launched the E-commerce Capacity Building Framework to strengthen digital inclusion and to help developing and least-developed countries harness the opportunities of digital trade, and the conveners also stressed that "provisions that enable and promote the flow of data are key to a high standard and commercially meaningful outcome for the negotiations. At the same time, members must be mindful of the development aspect, such as the digital divide and capacity building needs, to achieve an inclusive outcome through the negotiations"; therefore, an "appropriate policy space is needed to accommodate different circumstances of the participating members". For instance, China's position on trade-related aspects of data flow is that "data flow should be subject to the precondition of security, which concerns each and every Member's core interests. To this end, it is necessary that the data flow orderly in compliance with Members' respective laws and regulations".[56]

Therefore, international institutions such as the WTO would be a better venue to deliberate, cooperate, and negotiate a set of inclusive, proportional, and tier-oriented rules on global data flows; the outcome may have a thin agreement, which shall allow sufficient policy space to accommodate different needs, policy preferences and priorities, and local contexts while reaching a set of commonly accepted minimum standards. We agreed with Burri (2021) that given the fluid, complex data ecosystem, the need for collaborations at international and national levels, the need for modesty and humanity from the policy-makers, as well as the need for a fair balance of different values, individual rights, and national interests or policy priorities, even a thin and narrowly-scoped WTO agreement on e-commerce rules on cross-border data flows with sufficient policy space to accommodate different needs, policy preferences and priorities and local contexts via legitimate exception provisions would be a welcome movement.

10. Conclusions

Although the US, EU, and China have different models for regulating the cross-border flows of data, recent regional trade agreements have demonstrated a certain degree of overlap between the three modes. For example, the United States, as the home country of the world's major Internet giants and digital service providers, has always emphasized export orientation, advocated the opening of the digital market, and advocated the free flows of data. However, in some of the latest trade agreements, whether it is the Privacy Shield agreement with the European Union, the USMCA, or the CPTTP, data protection clauses have also been written. As one of the largest markets for digital products and digital services, the EU is mainly the recipient of digital trade, and the protection of its consumer rights is the first principle in the data issue, but in the draft trade agreements with Australia, New Zealand, and Tunisia, there are provisions that prohibit data localization measures and promote the free flows of data. China has also put forward initiatives such as the "*Global Initiative on Data Security*" and "*Global Security Initiative*" to promote connectivity in the digital era and supports the strengthening of international cooperation in the digital economy and security, including participating in or joining the negotiations on relevant regional trade rules. The RCEP it has joined also stipulates the prohibition of data localization and a commitment to the free flows of data with exceptions.

Its application to join the CPTPP and DEPA will also put pressure on its cross-border data policies. Furthermore, the new *Data Export Security Assessment Measures* have provided some legal certainty by defining four categories of personal and important data that are required for a prior security assessment to assess the risks that data exports may bring to national security, public interests, and the legitimate rights and interests of individuals

[56] WTO, Joint Statement on electronic commerce, Communication from China, 23 April 2019, INF/ECOM/19.

or organizations. This formulation is moderately referenced to the practices of general and national security exceptions provisions in many FTAs. The assessment of the legality, legitimacy, and necessity of the purpose, scope, and methods is also in line with article 5 of China's *Personal Information Protection Law* and should not be considered as being discriminatory.

Secondly, in theory, there is no complete incompatibility between cross-border data flows and data sovereignty (Xu 2020). Moreover, the introduction of exceptions to respond to diverse cross-border data flow regulations is a common practice amongst various international trade agreements. A treaty is concluded on the basis of consent; even if it limits the "sovereignty" of the contracting parties to take certain measures or controls, it is the result of the exercise of the sovereign rights of the contracting parties. From the perspective of international trade rules, the principle of sovereignty mainly reflects the autonomy of contracting parties or members to take regulatory or restrictive measures in related fields. For example, the EU-Australia draft trade agreement also includes data sovereignty provisions, "the contracting parties may adopt and retain such safeguards as they deem reasonable to protect personal data and privacy, including adopting or applying rules for cross-border movement of personal data". "The agreement shall not affect the respective protection mechanisms of the contracting parties for personal data and privacy protection".[57] In order to further strengthen the EU's autonomy in personal data protection, the EU has also set up a regular review mechanism specifically for cross-border data flows in the EU–Australia FTA draft to assess the impact of implementing FTAs on personal data protection.[58] Not only that, the EU–Australia FTA also includes very broad exceptions that cover almost all legitimate public policy objectives of the government,[59] thereby retaining the supervisory and domestic regulatory power of cross-border data flows.

In terms of national security exceptions, countries have increasingly adopted a broad understanding of 'national security' encompassing both traditional, e.g., military threats, and non-traditional, e.g., poverty, trade, economy, human rights, and environment security domains. Data security is increasingly considered to be an integrated part of national security. However, given that in practice, there are different understandings of the role and scope of national security in the digital trade, states should avoid the casual use of it to resolve cybersecurity or economic issues in electronic commerce. Policymakers need to find innovative ways for the conceptualization and international cooperation of data or national security and to reconcile expanded security concepts with trade obligations.

Thirdly, digital divide between countries at different levels of digital development needs to be addressed. We argue that the route for governing cross border data flows has to take a boarder approach, link the trade with digital rights and legitimate national interests, and seek a right balance between the protection of privacy, legitimate public policy goals, national security, and free flows of data in a tiered, proportional and contextual manner in order to avoid the fragmentation of and better facilitate the global flows of data.

It is worth noting that in the latest regional agreements, such as the RCEP, the standard issue of data protection has been handled flexibly, providing special and differential treatments for developing countries and least-developed countries, and the RCEP expands the exceptions for cross-border data flows for "different levels of development among contracting parties, and the need for appropriate forms of flexibility." Special and differential treatment is an important cornerstone of the international trade agreements. It is also the embodiment of the principle of promoting development, better reconciling the economic

[57] See Article 6(2) of the draft EU-Australia Free Trade Agreement. European Union's (EU) proposal for the EU-Australia FTA, https://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157570.pdf (accessed 2 May 2022).

[58] It provides for a review within three years of the entry into force of the treaty, and a contracting party may request a review at any time. See Article 5(2) of the draft EU-Australia Free Trade Agreement.

[59] Article 2 of the draft EU-Australia Free Trade Agreement states, "Parties re-emphasize regulatory powers in their fields to achieve legitimate policy objectives, including the protection of public health, social services, public education, safety, the environment and climate change, public ethics, social or consumer protection, privacy and data protection, or the promotion and protection of cultural diversity".

level gap between countries, and promoting the establishment of broader multilateral rules. In China's Join Statement on E-Commerce submitted to the WTO, it also emphasizes that it is necessary to help developing and less-developed countries integrate into global value chains, bridge the digital divide, seize development opportunities, and benefit from inclusive trade, and hence better participation in the economic globalization.[60]

On the other hand, current international trade agreements such as CPTPP, RCEP, and DEPA have regional characteristics and may only be used as a phased plan for governing international cross-border flows. The competing regional interoperability mechanisms are still largely aligned with geopolitical power and trade blocks and may not be able to resolve the fundamental problem of establishing an international regulatory framework in cross-border data flows. We argue that a thin and narrowly-scoped WTO agreement on e-commerce rules on cross-border data flows with sufficient policy space to accommodate different needs, policy preferences and priorities, and local contexts via legitimate exception provisions should be established in the WTO system given the complexity of the issue, which include not only commercial interests but also national security as well as values of public interests and digital rights that need to mobilize cooperation at both national and international regimes.

Finally, from the perspective of the inclusiveness of participation in the construction of international digital trade rules of cross-border data flows, China, developing, and LDCs need to engage vigorously in research on international standards in the fields of data security, data governance, international trade law, and new technologies, strengthening the cultivation of talents, research institutions, and enterprises, and systematically improve their inputs in international rulemaking.

Author Contributions: Conceptualization, Y.-C.C. and J.Z.; methodology, Y.-C.C. and J.Z.; formal analysis Y.-C.C. and J.Z.; investigation, Y.-C.C. and J.Z.; writing—original draft preparation, Y.-C.C. and J.Z.; writing—review and editing, Y.-C.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

Aaronson, Susan. 2015. Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security. *World Trade Review* 14: 671–700. [CrossRef]

Burri, Mira. 2017. The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation. *UC Davis Law Review* 5: 65–132.

Burri, Mira. 2021. A WTO Agreement on Electronic Commerce: An Enquiry into Its Legal Substance and Viability. Trade Law 4.0 Working Paper Series. Available online: https://ssrn.com/abstract=3976133 (accessed on 20 April 2022).

Chin, Yik-Chan. 2018. The Legitimation of Media Regulation in China. *Chinese Political Science Review* 3: 172–94. [CrossRef]

Chin, Yik-Chan. 2020. Internet Governance in China: The network governance approach. In *Social Relations and Political Development in China: Change and Continuty in the 'New Era'*. Edited by Zhenxu Wang and Dragan Pavlicevic. London: Routledge, pp. 134–53.

Chin, Yik-Chan, Ahran Park, and Ke Li. 2022. A Comparative Study on False Information Governance in Chinese and American Social Media Platforms. *Policy and Internet* 14: 263–83. [CrossRef]

Chin, Yik-Chan, and Ke Li. 2021. Sovereignty in Cyberspace: EU and China Compared. Paper presented in TPRC49: The 49th Research Conference on Communication, Information and Internet Policy, Virtual, September 22–24. Available online: https://ssrn.com/abstract=3900752 (accessed on 20 April 2022).

Cory, Nigel. 2019. Why China Should Be Disqualified From Participating in WTO Negotiations on Digital Trade Rules, Information Technology & Innovation Foundation. Available online: https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital (accessed on 20 January 2022).

Council of Europe. 2019. Data Protection. Available online: http:www.coe.int/dataprotection (accessed on 30 April 2022).

[60] Joint Statement on Electronic Commerce, Communication from China, 23 April 2019, INF/ECOM/19, Paragraph 3.15.

Cyberspace Administration of China. 2022. Measures for Data Export Security Assessment. 7 July 2022. Available online: http://www.gov.cn/zhengce/zhengceku/2022-07/08/content_5699851.htm (accessed on 30 July 2022).

Desierto, Diane. 2018. Protean 'National Security' in Global Trade Wars, Investment Walls, and Regulatory Controls: Can 'National Security' Ever Be Unreviewable in International Economic Law? *Blog of the European Journal of International Law*. Available online: https://www.ejiltalk.org/national-security-defenses-in-trade-wars-and-investment-walls-us-v-china-and-eu-v-us/ (accessed on 30 April 2022).

Dr2 Consultants. 2022. European Data Act: A Harmonized Framework for Accessing and Sharing Data. Available online: https://dr2consultants.eu/european-data-act/ (accessed on 30 April 2022).

Drake-Brockman, Jane, Gabriel Gari, Stuart Harbinson, Bernard Hoekman, Hildegunn Kyvik Nordås, and Sherry Stephenson. 2021. Digital Trade and the WTO: Top Trade Negotiation Priorities for Cross-Border Data Flows and Online Trade in Services, Jean Monnet TIISA Network Working Paper no.11-2021. Available online: https://iit.adelaide.edu.au/ua/media/1551/wp-2021-11-j.drake-brockman-et-al.pdf (accessed on 20 April 2022).

Elms, Deborah. 2021. *China Applies to Join DEPA*. Singapore: Asian Trade Centre. Available online: http://asiantradecentre.org/talkingtrade/china-applies-to-join-depa (accessed on 22 April 2022).

European Commission. 2020. Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross. 10 August 2020. Available online: https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en (accessed on 30 April 2022).

European Commission. 2022. European Commission and United States Joint Statement on TransAtlantic Data Privacy Frame work Brussels. 25 March 2022. Available online: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087 (accessed on 30 April 2022).

Gao, Henry. 2018. Regulation of Digital Trade in US Free Trade Agreements: From Trade Regulation to Digital Regulation. *Legal Issues of Economic Integration* 45: 47–70. [CrossRef]

Gao, Henry. 2021. Data regulation in trade agreements: Different models and options ahead. In *Adapting to the Digital Trade Era: Challenges and Opportunities*. Edited by Maarten Smeets. Geneva: WTO Press, pp. 322–34.

Greenleaf, Graham. 2019. G20 makes declaration of 'Data Free Flow With Trust': Support and dissent. *Privacy Laws & Business International Report* 160: 18–19.

He, Bo. 2019. The Development Challenges and Countermeasures of Data Sovereignty. *Journal of Cyber and Information Law* 1: 201–16. Translated from 何波. 2019. 数据主权的发展挑战与对策. 网络信息法学研究 1: 201–16.

Heath, J. Benton. 2020. Trade and Security Among the Runis. *Duke Journal of Comparative and International Law* 30: 223–66.

Hong, Yanqing. 2021a. The Strategic Position of the US and Europe in Data Competition and China's Response: From the Dual Perspectives of Domestic Legislation and Negotiation of Economic and Trade Agreements. *International Law Studies* 6: 69–81. Translated from 洪延青. 2021a. 数据竞争的美欧战略立场及中国因应——基于国内立法与经贸协定谈判双重视角. 国际法研究 6: 69–81.

Hong, Yanqing. 2021b. China's plan to promote the cross-border flows of data along the "One Belt, One Road"—Development in the context of the U.S. and European paradigms. *China Law Review* 2: 30–42. Translated from 洪延青. 2021b. 推进"一带一路"数据跨境流动的 中国方案—以美欧范式为背景的展开. 中国法律评论 2: 30–42..

Liu, Jianhua, and Yabing Gong. 2013. An Analysis of the Obama Administration's "Rules Diplomacy" towards China. *Forum of World Economic and Political* 3: 84–96. Translated from 刘建华, & 龚雅冰. 2013. 试析奥巴马政府对华"规则外交. 世界经济与政治论坛 3: 84–96.

Meltzer, Joshua. 2019. Governing Digital Trade. *World Trade Review* 18: S23–S48. [CrossRef]

Ministry of Foreign Affairs of China. 2020. Global Initiative on Data Security, 29 October 2020. Available online: https://www.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/202010/t20201029_9869292.shtml (accessed on 28 April 2022).

Mishra, Neha. 2020. The Trade–(Cyber)security Dilemma and its Impact on Global Cybersecurity Governance. *Journal of World Trade* 54: 567–90. [CrossRef]

Olson, Stephen. 2021. The Conventional Wisdom on China and the CPTPP Is Wrong. Available online: https://www.hinrichfoundation.com/research/article/ftas/china-and-cptpp/ (accessed on 23 April 2022).

Olson, Stephen. 2022. Ukraine Forces Debate on WTO and National Security. Available online: https://www.hinrichfoundation.com/research/article/wto/ukraine-debate-on-wto-national-security/ (accessed on 23 April 2022).

Qi, Aimin, and Gaofeng Zhu. 2016. On the Establishment and Improvement of the National Data Sovereignty System. *Journal of Soochow University (Philosophy and Social Sciences Edition)* 1: 83–88. Translated from 齐爱民, & 祝高峰. 2016. 论国家数据主权制度的确立与完善. 苏州大学学报（哲学社会科学版） 1: 83–88.

Shaffer, Gregory C., and Mark A. Pollack. 2010. Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance. *Minnesota Law Review* 94: 706–99.

Sun, Yi. 2016. International Institutional Pressure and China's Free Trade Zone Strategy. *Quarterly Journal of International Politics* 1: 125–61. Translated from 孙忆. 2016. 国际制度压力与中国自贸区战略. 国际政治科学 1: 125–61.

Taheri, Rachelle, Olivia Adams, and Pauline Stern. 2021. DEPA: The World's First Digital-only Trade Agreement. Asia Pacific Foundation of China. Available online: https://www.asiapacific.ca/publication/depa-worlds-first-digital-only-trade-agreement (accessed on 20 April 2022).

Tang, Xia. 2021. Between Data Security and Openness: A Chinese approach to International Rulemaking for digital trade. Political Science and Law, 12: 26–38. Translated from 汤霞. 2021. 数据安全与开放之间：数字贸易国际规则构建的中国方案*. 政治与法律 12: 26–38.

US Department of Commerce. 2022. Global Cross-Border Privacy Rules Declaration. Available online: https://www.commerce.gov/global-cross-border-privacy-rules-declaration (accessed on 22 April 2022).

Wang, Rong. 2018. Policy Perceptions and Suggestions on Data Cross-Border Flows: From the Perspective of Comparison and Reflection on U.S. and European Policies. *Information Security and Communication Privacy* 3: 41–53. Translated from 王融. 2018. 数据跨境流动政策认知与建议: 从美欧政策比较及反思视角. 信息安全与通信保密 3: 41–53.

Wang, Yi. 2022. Implement Global Security Initiatives to Safeguard World Peace and Tranquility. Ministry of Foreign Affairs of China. Translated from 王毅. 2022. 落实全球安全倡议，守护世界和平安宁. 中华人民共和国外交部. Available online: https://www.mfa.gov.cn/wjbzhd/202204/t20220424_10672812.shtml (accessed on 2 May 2022).

Wei, Liang. 2022. Implement the Overall National Security Concept and Effectively Build a Data Security Barrier. China Information Security. Translated from 魏亮. 2022. 贯彻总体国家安全观 切实筑牢数据安全屏障. 中国信息安全. Available online: https://mp.weixin.qq.com/s/9UaqliGKIM7FDTlrECoeOA (accessed on 30 April 2022).

Xu, Duoqi. 2020. On the Legal Guarantee of Two-way Compliance of Cross-border Data Flow Regulating Enterprises. *Eastern Law* 2: 185–97. Translated from 许多奇. 2020. 论跨境数据流动规制企业双向合规的法治保障. 东方法学 2: 185–97.

Zhang, Linlin, and Zhiyi Peng. 2022. The Influence of China's International Rules on Data Security Needs to Be Improved. *Information Security and Communication Privacy* 3: 27–32. Translated from 张琳琳, & 彭志艺. 2022. 我国亟需提升数据安全国际规则影响力. 信息安全与通信保密 3: 27–32.

Zhu, Fulin. 2021. The International Game of Digital Trade Rules, "Seeking for Common" Dilemma and China's Strategy. *Economic Review Journal* 8: 40–49. Translated from 朱福林. 2021. 数字贸易规则国际博弈、"求同"困境 与中国之策. 经济纵横 8: 40–49.