Studies in Law and Justice
ISSN 2958-0382
www.paradigmpress.org/slj
Volume 4 Number 6 December 2025

International Regulation of Personal Information Protection in the Context of Cross-Border Data Flows

Bishan Zeng[1]

[1] School of Law and Politics, Guangzhou College of Applied Science and Technology, Guangdong, China
Correspondence: Bishan Zeng, School of Law and Politics, Guangzhou College of Applied Science and Technology, Guangdong, China.

doi:10.63593/SLJ.2025.12.04

Abstract

In the era of digital economy, the relationship between personal information protection and cross-border data flows is complementary and mutually constraining. There are two approaches to international regulation of personal information protection in the international community: geographic location-based and organization-based, but both are inadequate. The existing regional trade agreements such as CPTPP, USMCA, and RCEP provide for the protection of personal information by establishing a chapter on electronic commerce, but regional trade agreements can only play a short-term supplementary role, and ultimately the WTO is the multilateral platform for the protection of personal information regulation. GATS Article XIV(c)(ii) is regarded as a relevant provision on personal information protection, but it is not sufficient to meet the challenges faced by personal information protection in the context of cross-border data flows and needs to be improved. In the interim, the WTO should make full use of the necessity test in conjunction with the provisions of the GATS on transparency and recognition agreements. In the long term, a more comprehensive annex on personal information protection should be developed within the GATS.

Keywords: personal information protection, cross-border data flows, GATS Article XIV(c)(ii), regional trade agreements, international regulation

1. Introduction

Personal data has become an indispensable element in the development of the digital economy. In today's digital age, everyday internet users must input personal data to access the vast array of options offered by websites, smartphones, applications, social media, and new technologies. (Itzayana Tlacuilo Fuentes, 2020, p. 90) However, the free cross-border flow of personal data is highly prone to information leaks. During cross-border data transfers, if overseas recipients fail to provide adequate safeguards or misuse personal data, they may infringe upon individual information rights, thereby posing challenges to personal information protection. For instance, Facebook collected and stored sensitive data—including religious beliefs—from users in other countries. However, due to inadequate security measures, user data was leaked and subsequently misused for political election analysis. (China News

Service, 2018) To address the challenges of personal information protection amid the free flow of data, regional trade agreements such as the CPTPP, USMCA, and RCEP now specifically stipulate personal information safeguards. They also permit exceptions based on legitimate public policy objectives to regulate cross-border data flows. Additionally, the General Data Protection Regulation (GDPR) provides robust protections for personal data transfers. However, these frameworks remain confined to specific regions, limiting their global impact. The Cross-Border Privacy Rules (CBPR) developed by the Asia-Pacific Economic Cooperation (APEC) and the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data are merely non-binding international standards. Meanwhile, GATS Article XIV(c)(ii) serves as an international regulatory framework for personal information protection under the WTO. However, this provision has become outdated in the context of the digital economy and urgently requires refinement.

How should we understand the relationship between personal information protection and cross-border data flows? What are the international regulatory models for personal information protection within the global community? How does the WTO regulate personal data protection? How should the WTO reform to better regulate the relationship between cross-border data flows and personal information protection? This paper will explore these questions.

2. The Relationship Between Personal Information Protection and Cross-border Data Flows

Various online activities generally require cross-border data flows to be completed, but such data flows are not always orderly and secure, posing significant challenges to personal information protection. From the perspective of digital trade development, the liberalization of digital trade requires unrestricted data movement, which paradoxically becomes the root cause of personal information leaks. (Dai Long, 2020) Cases like Facebook's unauthorized use of user data, Uber's data breach and subsequent cover-up that compromised millions of customers' and drivers' information, and Amazon employees' data breaches for commercial gain have become all too common. These incidents collectively demonstrate how cross-border data flows now threaten personal data protection. Regarding the relationship between cross-border data flows and personal data protection, scholars argue that there exists an inverse correlation between unrestricted data movement and safeguarding citizens' rights. (NEERAJ RS., 2019) In short, the freer cross-border data flows become, the more vulnerable personal information becomes. However, daily online activities require personal data inputs for access, and many software applications demand personal information to provide services. Without such data, users cannot enjoy free service experiences. Undoubtedly, cross-border data flows have become an indispensable part of digital trade development. Therefore, the relationship between these two aspects is far more complex than simply being inversely proportional.

In fact, this paper argues that the relationship between cross-border data flows and personal information protection is one of mutual reinforcement and constraint. While cross-border data flows carry risks of personal information leaks, legal mechanisms can be employed to regulate and balance these two aspects. For instance, the GDPR also regulates cross-border data flows with the protection of personal data as its core objective. From a corporate perspective, in the long run, strengthening the personal information protection obligations of digital technology enterprises also aligns with their interests. Neglecting privacy safeguards risks eroding user trust, leading to customer attrition and the inability to sustainably access data. (Dai Long, 2020)

Meanwhile, as data becomes a production factor, it can now be traded as an object of exchange, with practices like personal data transactions emerging in real-world applications. For example, a new company called Wibson, founded in 2018, provides consumers with a blockchain-based decentralized marketplace that allows them to monetize their personal data. Wibson transforms an opaque, buyer-dominated ecosystem into a transparent and fair marketplace, enabling consumers to receive compensation for their data based on personal preferences and comfort levels. (Itzayana Tlacuilo Fuentes, 2020, p.111) For users, permitting enterprises to lawfully use personal data within the scope of their consent constitutes the consideration for accessing

services. Should users be barred from providing the requisite personal data for enterprise use, they would be unable to obtain the corresponding services they require, thereby hindering the continuous advancement of the digital economy. Therefore, from the perspective of dialectical materialism, the relationship between cross-border data flows and personal information protection should be viewed dialectically. These two elements are mutually reinforcing, mutually constraining, and interdependent.

3. International Regulatory Approaches to Personal Information Protection

Under the GDPR, 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (European Union, 2016) In the CPTPP Chapter on Electronic Commerce, personal information means any information, including data, about an identified or identifiable natural person. (CPTPP, 2018) In the USMCA chapter on digital trade, personal information means information, including data, about an identified or identifiable natural person. (USMCA, 2018) Given that academia has not made a clear distinction between personal information and personal data, the terms "personal information" and "personal data" used in this paper refer to the same meaning. Regarding international regulatory models for personal information protection in the context of cross-border data flows, scholars have proposed the most significant framework for evaluating privacy protection mechanisms addressing cross-border data transfers, distinguishing between "geographically-based" and "organizationally-based" approaches. (Kuner Christopher, 2013) The "geographically-based" approach is primarily led by the European Union, while the "organizationally-based" approach is predominantly championed by the United States.

3.1 Geographically-Based Approach

The geographically-based approach regulates data transfers based on the level of data protection in place in the receiving or importing country. (Julian Rotenberg, 2020, pp. 97-98) It is adopted by the European Union and several other jurisdictions. In May 2018, the European Union promulgated the General Data Protection Regulation (GDPR). Under the GDPR, personal data may be transferred from the EU to a third country that ensures an "adequate level of protection." The GDPR sets out three main criteria for assessing whether a third country provides such adequacy: (1) the establishment and enforcement of the rule of law; (2) the existence of an effectively functioning, specialized supervisory authority; and (3) accession to international treaties or multilateral agreements concerning the protection of personal data and the assumption of corresponding obligations under international law. (Yang, X., 2021) Moreover, the adequacy of a receiving country's data protection standards is typically determined by public authorities. Such determinations may take the form of unilateral recognition, whereby one country establishes the adequacy of another and permits data transfers to that destination, or mutual recognition between two or more countries. This mutual recognition may be formalized through free trade agreements, enabling the free flow of data among them. (Julian Rotenberg, 2020, p. 98) In practice, this approach is also known as the adequacy approach, meaning that a country's or jurisdiction's domestic data protection laws will establish the minimum standards for other countries or jurisdictions to become recipients of its data transfers. Thus, governments can employ this method to incentivize others to enact data protection laws with specific content to attract data exports. When the sovereign state establishing baseline protection levels possesses significant trade and political influence, this approach serves as an effective means to export its regulatory standard.

3.2 Organizationally Based Approach

The organizational-based approach, also known as the "accountability" approach, regulates how companies and other organizations handle data transferred across borders. Regardless of where the data is processed, these organizations are "accountable" for processing personal data in accordance with specific privacy principles. The accountability approach does not restrict cross-border data flows but instead imposes responsibilities on all parties involved in data transfers. Under this model, protection is based

on specific legal obligations imposed on data controllers, and these obligations continue to apply after personal data cross national borders. (Kuner Christopher, 2013, p. 64) One of the most relevant examples of the accountability approach is the Cross-Border Privacy Rules (CBPR) system adopted to facilitate the transfer of personal data among Asia-Pacific Economic Cooperation (APEC) economies. Corporate policies and practices must be certified by APEC accountability agents as meeting the requirements of the CBPR, and these agents, together with national privacy enforcement authorities, are responsible for ensuring compliance.(Asia-Pacific Economic Cooperation, 2019) Any APEC economy may unilaterally join the system, and enterprises subject to the laws of that economy will be able to participate in it. Another notable example is the OECD's 2013 revision of its Privacy Guidelines, which adjusts the relationship between individuals and data controllers. Individuals have the right to obtain confirmation from data controllers as to whether data relating to them are held, and to request information on how such data are processed; In cases of refusal, individuals have the right to challenge such refusal and, if successful, to have the data erased, rectified, completed, or amended. (OECD, 2013) Finally, the data controller remains responsible for the personal data under its control, regardless of the data's location.

Simultaneously, in countries or regions lacking adequacy findings, the GDPR stipulates that both Binding Corporate Rules (BCR) and Standard Contractual Clauses (SCC) constitute accountability methods. Both impose data protection obligations on companies operating across different jurisdictions. The adoption and implementation of binding corporate rules permits multinational corporations to transfer data across borders, albeit limited to transfers between corporate subsidiaries in different countries. These instruments typically require prior approval from relevant national data protection authorities, which may involve lengthy procedures. Standard Contractual Clauses are rules used in transactions involving cross-border transfers of personal data to third parties. These clauses are usually drafted or approved by data protection authorities and, once incorporated into a contract, are deemed to provide adequate protection for the transferred data regardless of the destination country or region.

3.3 Critical Assessment

Both the "Geographically-Based" and the "Organizationally Based" approaches have their respective shortcomings. Under the GDPR model adopted by the European Union, developing countries face a dilemma: either they must enact national privacy legislation similar to that of the EU, or their companies must bear the transaction-specific costs associated with the use of BCR and SCC. On the one hand, it is difficult for developing countries to adopt EU-style national privacy regimes, because the EU's conception of personal data as a fundamental human right—reflected in the Charter of Fundamental Rights of the European Union—is a product of Europe's particular historical and cultural context. (Aaditya Mattoo & Joshua P Meltzer, 2018, p. 770) On the other hand, SCC have also been shown to be cumbersome, as they must be designed to address all possible data transfers ex post. (Aaditya Mattoo & Joshua P Meltzer, 2018, p. 777) Compared to the GDPR and similar frameworks, the CBPR adopted by APEC and the Privacy Guidelines adopted by the OECD are considered more lenient. (Andrew D Mitchell & Neha Mishra, 2019, p. 400) In other words, the APEC and OECD frameworks lack binding force. As a result, the APEC framework in particular may struggle to become a global standard, because it offers a voluntary scheme rather than a legally binding set of rules, and because it is oriented more toward facilitating e-commerce than toward ensuring robust personal data protection. (Christian Pauletto, 2021) For example, the United States has removed references to these principles in its submissions to the WTO.

4. Regulation of Personal Information Protection Under Existing Agreements

In recent years, in the absence of meaningful progress at the multilateral level, bilateral and plurilateral free trade agreements have developed new models to address emerging barriers to digital trade. (Susannah Hodson, 2019, p. 592) The CPTPP, USMCA, and RCEP each contain a dedicated chapter on e-commerce and include separate provisions on personal information protection. Compared with the international standards adopted by the OECD and APEC, these agreements incorporate personal information protection into binding legal rule systems, representing a certain degree

of progress. Within the multilateral trading system, Article XIV(c)(ii) of the General Agreement on GATS, which forms part of the general exceptions, provides for "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." (WTO, 1994) This provision offers a legal justification for a member to adopt restrictions on cross-border data flows on the basis of personal privacy protection and thus constitutes the principal legal regulation of personal information protection under the GATS. This paper examines the provisions on personal information protection in the CPTPP, USMCA, and RCEP regional trade agreements, as well as Article XIV(c)(ii) of the GATS.

4.1 Regulation of Personal Information Protection Under Existing Regional Trade Agreements

The innovative feature of the CPTPP, USMCA, and RCEP lies in the fact that they impose obligations on destination countries to prevent fraud and deception and to protect personal information. All three agreements explicitly require their parties to adopt or maintain a legal framework that ensures the protection of users' personal information. At the same time, taking into account differences in levels of information technology development and cultural traditions among the parties, none of these agreements mandates a uniform legal framework; instead, each party is required to take into consideration the principles and guidelines of relevant international bodies. This approach has several advantages: First, it does not prescribe a specific model of privacy regulation. (Joel R. Reidenberg, 2000) The provision also does not prevent members from undertaking institutional innovation beyond the baseline requirements to protect personal information (for example, in light of their particular circumstances), provided that such measures are not arbitrary or discriminatory. (David Hyman & William E. Kovacic, 2019) Third, unlike the USMCA, which specifically references APEC's Cross-Border Privacy Rules (CBPR) and the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the CPTPP and RCEP do not cite relevant international bodies, privacy principles, or guidelines. This approach acknowledges that other evolving privacy principles or guidelines may exist and that other relevant international bodies may also be addressing these issues. (Andrew D Mitchell & Neha Mishra, 2019, p. 410) In addition, all three agreements require their parties to make publicly available information on the protection of personal information provided to e-commerce users, including avenues through which individuals may seek remedies and the specific obligations that enterprises must comply with under the law.

On the other hand, both the CPTPP and USMCA recognize that contracting parties may adopt different legal approaches to protect personal information, and each contracting party should encourage the establishment of mechanisms to promote compatibility among these different systems. Such mechanisms may be implemented autonomously or through mutual agreements and may even be achieved through broader international frameworks. (CPTPP, 2018; USMCA, 2018) By contrast, the RCEP merely emphasizes cooperation among the parties in the protection of personal information and does not provide for autonomous arrangements of this kind. In practice, levels of information technology development vary significantly across countries. If the standards set by international bodies are applied rigidly, countries with lower technological capacity may be unable to meet the corresponding requirements, making it difficult to achieve convergence on personal information protection standards. This reality highlights the greater importance of promoting compatibility among different domestic legal regimes. From this perspective, the "standards and interoperability" model adopted by the CPTPP and the USMCA is of considerable significance for promoting the harmonization and coordination of personal information protection. Moreover, all three regional trade agreements—the CPTPP, USMCA, and RCEP—allow restrictions on cross-border data flows as exceptions for the pursuit of legitimate public policy objectives, including the protection of personal information. The existence of such cooperative obligations reduces the need for source countries to take unilateral action under exception clauses and thereby creates a more secure environment for exporters to obtain personal data. In this regard, the CPTPP, USMCA, and RCEP are likely to serve as paradigms of regulatory cooperation. Nevertheless, although these three regional trade agreements have introduced innovative

frameworks for the regulation of personal information protection and achieved a certain degree of progress, their impact remains limited, and they can only play a short-term supplementary role. The key function of regional trade agreements is ultimately to pave the way for broader multilateral agreements, leading to more enforceable and binding commitments grounded in core WTO principles such as non-discrimination, minimal trade restrictiveness, and transparency.

4.2 Personal Information Protection Under the WTO Framework

Within the GATS, principles governing cross-border data flows—or at least their fundamental trade objectives—can be identified. Some scholars have argued that the movement of capital may be analogized to the flow of data; if so, the GATS effectively recognizes data as an integral component of services themselves. (Itzayana Tlacuilo Fuentes, 2020, p.111) Therefore, in the context of digital trade, the GATS can still provide a legal regulatory framework for cross-border data flows. Consequently, personal information protection based on cross-border data flows should naturally be provided with a legal regulatory framework within the GATS. Article XIV(c)(ii) of the General Agreement on GATS, which forms part of the general exceptions, provides for "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." (World Trade Organization, 1994) This provision offers the most appropriate legal basis for a Member to justify restrictions on cross-border data flows adopted for the purpose of protecting personal information.

However, applying pre-internet era GATS rules to data-related issues presents challenges. First, due to the cross-sectoral nature of digital services, it is difficult to determine whether members' commitments on national treatment and market access in their GATS schedules cover cross-border data flows in certain sectors. Second, the proximity of service suppliers and consumers within digital supply chains leads to highly intrusive data restriction measures. This issue cannot be resolved by invoking GATS privacy exceptions to justify such restrictions in the absence of shared international norms on data regulation. For instance, panels lack the capacity to assess the non-trade-related aspects of domestic data regulations, including whether they undermine the open and interoperable architecture of the internet or restrict the realization of human rights. (Andrew D Mitchell & Neha Mishra, 2019, p. 399) Third, although the Services Sectoral Classification List ("W/120") provides guidance for WTO Members when making commitments under the GATS, it is nearly thirty years old and no longer adequately reflects the commercial realities of the digital economy. Many digital products are based on converged business models that increasingly combine telecommunications services with other services, including computer, audiovisual, banking, financial, and advertising services. These services are inherently multifunctional and rely on a variety of service inputs to deliver an integrated digital platform. For example, WeChat and Google combine multiple services, including communications, payments, and cloud computing. However, commitments to service sectors or subsectors in a member's schedule are exclusive; as a result, a particular digital service (such as Google's search engine) cannot simultaneously be classified under computer and related services (more specifically, data processing services), telecommunications services (online information and data processing services), and advertising services. (Andrew D. Mitchell & Neha Mishra, 2018, p. 1086) This means that where cross-border data flows associated with a particular service sector fall outside the scope of a member's commitments under a converged business model, regulatory measures affecting such data flows cannot be justified under the personal privacy exception, thereby limiting the effectiveness of GATS Article XIV(c)(ii) in addressing personal information protection in the digital economy.

In sum, the provisions on personal information protection under the GATS are overly rudimentary and general, and are therefore ill-suited to the realities of the digital trade era. Accordingly, reform of the GATS framework with respect to personal information protection has become both necessary and imperative.

5. Proposals for Improving the WTO Rules on Personal Information Protection

As analyzed above, the current WTO framework on personal information protection is no longer able to respond to the challenges of the digital trade era; however, the WTO is the best forum for developing rules to govern cross-border data flows for two reasons: first, it covers 85 percent

of all countries; and second, WTO rules are transparent and flexibly designed to evolve with changes in technology, markets, and political conditions. (Susan Ariel Aaronson & Patrick Leblond, 2018, p. 251) Therefore, regulation of cross-border data flows must ultimately rely on WTO rules, and personal information protection, which is closely related to cross-border data flows, also needs to be addressed within the WTO framework. Although WTO reform is necessary, such a complex task cannot be accomplished overnight; the author argues that it should be pursued in two stages: a transitional stage and a long-term stage.

5.1 Transitional Stage

During the transition period, first, the "necessity test" should be utilized to prevent abuse of GATS Article XIV(c)(ii). For instance, the United States previously banned transactions with Chinese software applications, including Alipay and WeChat Pay, on grounds of protecting the personal information of American citizens. At the WTO level, the U.S. is highly likely to invoke GATS Article XIV(c)(ii) as a defense. Therefore, the proper application of this provision becomes a key focus. If a member invokes this provision to restrict cross-border data flows, it must demonstrate that the measure is "necessary" to achieve the stated objective. The Appellate Body has determined that it falls closer to the level of "indispensable" than to merely "contributing to" the objective. (Diane A. MacDonald & Christine M. Streatfeild, 2014) This standard requires a strong connection between the measure and the interest protected, which must be established through the "necessity test," which is an overall assessment involving the "weighing and balancing of a series of factors". (WTO, 2005) Although WTO dispute settlement practice does not set out an exhaustive list of factors to be considered, the weighing and balancing process generally involves an assessment of the relative importance of the interests or objectives pursued by the measure, the contribution of the measure to the achievement of the objective, and the measure's restrictive impact on international trade. (WTO, 2005) The final part of the necessity test includes determining whether there are reasonably available, less trade-restrictive alternative measures. (WTO, 2005) This requires a comparison between the measure and possible alternative measures, with the burden of proof resting on the complaining Member proposing the latter. (WTO, 2005) If the alternative measure is merely theoretical—for example, if the member lacks the capacity to accept it, or if it imposes an undue burden on the member, such as excessive costs or significant technical difficulties—it shall not be considered reasonably available. (Susannah Hodson, 2019, p. 594)

Second, if the necessity test is satisfied, the final stage of the analysis is to determine whether the measure complies with the chapeau of Article XIV. The general exception clause in GATS Article XIV stipulates, "Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services." (WTO, 1994) This provision constitutes a further safeguard against measures adopted on the basis of personal information protection. In addition, the roles of on transparency and on recognition under the GATS should be brought into play. Article III on transparency and Article VII on recognition help ensure the transparency of newly emerging arrangements between different countries. More importantly, GATS Article VII facilitates greater international coordination among members regarding domestic regulations pertaining to the licensing, certification, or authorization of service providers, while ensuring that any such arrangements are non-discriminatory and permit participation by third countries. (Aaditya Mattoo & Joshua P Meltzer, 2018, p. 788) Moreover, pursuant to paragraph 5 of GATS Article VII, members shall work in cooperation with relevant intergovernmental and nongovernmental organizations towards the establishment and adoption of common international standards and criteria for recognition and common international standards for the practice of relevant services trades and professions. (WTO, 1994) This provision encourages cooperation between members and international organizations. Given the multi-stakeholder nature of the Internet governance system, and particularly considering that regulatory frameworks for cross-border data flows require more sophisticated approaches than traditional multilateral processes, the WTO should fully leverage the provisions of GATS Articles III and VII to

enhance international coordination among members regarding domestic personal information protection regulations. It should encourage cooperation between members and international organizations and promote the adoption of international standards on personal information protection by more countries.

5.2 Long-Term Stage

In the long term, members must engage in thorough negotiations to add an annex on electronic commerce to the GATS, establishing a binding e-commerce framework for all members. This framework should provide clearer and more specific elaboration on the privacy protection exception stipulated in GATS Article XIV, thereby safeguarding the regulatory autonomy of countries in overseeing the internet. The reason for adding an annex on electronic commerce to the GATS is twofold. On the one hand, GATS was formulated in the pre-Internet era and is unable to respond to the cross-sectoral nature of cross-border data flows. On the other hand, it does not provide for the adoption by members of domestic frameworks for the protection of personal information. Regarding how to develop an annex on electronic commerce within the GATS, this paper argues that provisions on personal information protection from regional trade agreements such as the CPTPP and RCEP should be referenced. The provisions in the e-commerce chapters of regional trade agreements like the CPTPP and RCEP break away from the traditional sectoral classification under GATS, aligning with the international trend of cross-border data flows. Particularly noteworthy is the "standards-plus-compatibility" approach adopted in agreements such as the CPTPP and USMCA for personal information protection. This model encourages countries to pursue mutual cooperation to enhance the compatibility of personal information protection legislation, offering valuable insights for reference.

6. Conclusion

The relationship between cross-border data flows and personal information protection is one of mutual reinforcement and constraint, requiring a dialectical perspective to understand their interplay. The CPTPP, USMCA, and RCEP regional trade agreements regulate personal information protection, but they can only serve as short-term supplements. Ultimately, the WTO—the most comprehensive multilateral platform—must play its role. GATS Article XIV(c)(ii) is no longer adequate for today's era of cross-border data flows and urgently requires improvement. Enhancing GATS can be approached in two phases: a transitional phase and a long-term phase. During the transitional phase, the necessity test should be fully leveraged, alongside the provisions on transparency under Article III and recognition under Article VII of GATS. Long-term efforts should focus on developing an annex on e-commerce within GATS to establish more robust regulations for personal information protection.

References

Aaditya Mattoo, & Joshua P Meltzer. (2018). International data flows and privacy: The conflict and its resolution. *Journal of International Economic Law, 21*, 770, 777, 788.

Andrew D Mitchell, & Neha Mishra. (2019). Regulating cross-border data flows in a data-driven world: How WTO law can contribute. *Journal of International Economic Law, 22*, 399, 400, 410.

Andrew D. Mitchell, & Neha Mishra. (2018). Data at the docks: Modernizing international trade law for the digital economy. *Vanderbilt Journal of Entertainment & Technology Law, 20*, 1086.

Asia-Pacific Economic Cooperation. (2019). APEC Cross-Border Privacy Rules System. http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf (Accessed May 15, 2022).

China News Service. (2018, March 30). https://m.chinanews.com/wap/detail/zw/fortune/2018/03-30/8494277.shtml (Accessed March 1, 2022).

Christian Pauletto. (2021). Options towards a global standard for the protection of individuals with regard to the processing of personal data. *Computer Law & Security Review, 40*, 105433.

CPTPP. (2018). Article 14.8.5; CPTPP. (2018). Chapter 14, Article 14.1.

Dai Long. (2020). On the protection of personal privacy rights in the context of digital trade. *Contemporary Law Review*, (1), 158.

David Hyman, & William E. Kovacic. (2019).

Implementing privacy policy: Who should do what? *Fordham Intellectual Property, Media & Entertainment Law Journal, 29*, 1121.

Diane A. MacDonald, & Christine M. Streatfeild. (2014). Personal data privacy and the WTO. *Houston Journal of International Law, 36*, 639–640.

European Union. (2016). *General Data Protection Regulation* (Article 4).

Itzayana Tlacuilo Fuentes. (2020). Legal recognition of the digital trade in personal data. *Mexican Law Review*, *12*, 90, 111.

Joel R. Reidenberg. (2000). Resolving conflicting international data privacy rules in cyberspace. *Stanford Law Review, 52*, 1359.

Julian Rotenberg. (2020). Privacy before trade: Assessing the WTO-consistency of privacy-based cross-border data flow restrictions. *University of Miami International & Comparative Law Review, 28*, 97–98.

Kuner Christopher. (2013). *Transborder data flows and data privacy law*. Oxford University Press, 64.

NEERAJ RS. (2019). Trade rules for the digital economy: Charting new waters at the WTO. *World Trade Review, 18*, 17.

OECD. (2013). OECD privacy guidelines (Article 13).

Susan Ariel Aaronson, & Patrick Leblond. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law, 21*, 251.

Susannah Hodson. (2019). Applying WTO and FTA disciplines to data localization measures. *World Trade Review, 18*, 592, 594.

USMCA. (2018). Article 19.8.6.; Chapter 19, Article 19.1.

WTO. (1994). GATS. (Article VII:5; Article XIV; Article XIV (c) (ii)).

WTO. (2005). *United States: Measures affecting the cross-border supply of gambling and betting services—Report of the Appellate Body* (WT/DS285/AB/R, paras. 304–307, 309).

Yang, X. (2021, April). Regulatory approaches of cross-border data flow in the big data era: China's choice. *Journal of Physics: Conference Series, 1848*(1), 012026. IOP Publishing.