Harmonization vs. Fragmentation: The Struggle to Govern Cross-Border Data in Trade Agreements

Miebaka Nabiebu[1], Amarachukwu Ijiomah[2], Mokutima Etido Ekpo[3], Ntamy Agube[4]

Abstract— In the modern global economy, digital trade rules—particularly those governing cross-border data flows—have become a pivotal arena for both international competition and cooperation. States have adopted markedly divergent regulatory approaches, reflecting their distinct economic, political, and social priorities. The United States champions a market-driven model, advocating for minimal restrictions on data mobility to maximize commercial freedom. In contrast, the European Union enforces stringent data protection standards under the General Data Protection Regulation (GDPR), prioritizing individual privacy over unconstrained data flows. Meanwhile, developing nations often retain regulatory flexibility to nurture domestic industries and safeguard digital sovereignty. China presents a unique case, navigating tensions between domestic industrial policy, national security imperatives, and global integration. Its cross-border data governance framework seeks to balance economic openness with state control, permitting data transfers while imposing strict localization requirements in sensitive sectors. This approach underscores the broader challenge: how to harmonize conflicting regulatory paradigms without fragmenting the global digital trade system. This article contends that a narrowly tailored WTO e-commerce agreement could offer a viable solution. By establishing clear yet adaptable rules on cross-border data flows, such an agreement could accommodate legitimate policy exceptions—including security, privacy, and developmental concerns—while preventing protectionist overreach. A flexible multilateral framework, rather than rigid uniformity, may be the most pragmatic path forward in governing the digital economy.

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

[1] Faculty of Law, university of calabar, Nigeria.
[2] Faculty of Law, university of calabar, Nigeria.
[3]Faculty of Law, university of calabar, Nigeria.
[4]Faculty of Law, university of calabar, Nigeria.

INTRODUCTION

The digital economy has fundamentally transformed global trade, with big data, cloud computing, and other information technologies becoming key strategic assets for businesses and governments alike. Data now serve a dual role—both as an economic resource that fuels competition and as an essential component in safeguarding personal privacy, human rights, and national security (Burri, 2017). These multidimensional characteristics of data have led to significant regulatory divergence across jurisdictions, as governments seek to balance economic gains with broader social and security concerns.

Currently, there is no comprehensive global framework governing cross-border data flows, leading to regulatory fragmentation (Duru, et al., 2023; Uto, et a., 2024). While multilateral efforts have been made, including within the WTO, progress has been slow. In response, nations have pursued regional and bilateral agreements to address the governance of digital trade. Key agreements such as the Regional Comprehensive Economic Partnership (RCEP) (effective January 1, 2022), the United States–Mexico–Canada Agreement (USMCA) (effective July 1, 2020), and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) (effective December 30, 2018) all recognize cross-border data flows as a core issue.

However, these agreements have introduced two critical challenges. First, major global players—the United States, China, and the European Union—maintain fundamentally different approaches to data governance. This divergence creates a new form of "digital divide" as nations define data ownership, privacy, and security in distinct ways. Second, while regional trade agreements are proliferating, they risk further fragmenting the global digital trade system rather than unifying it. The question, therefore, is whether these developments will exacerbate regulatory disparities or lay the groundwork for a future global framework.

This article seeks to address the central issue of interoperability in global digital trade. How can a middle ground be found among these divergent regulatory frameworks to ensure that cross-border data flows remain functional while respecting national policy preferences? The key challenge is balancing competing rights, interests, and values within the digital trade ecosystem. Norms that underpin data flow regulations include privacy protection, national security, local economic development, access to information, and the growth of global e-commerce. We argue that an effective regulatory approach must strike a balance among these principles, taking into account contextual, proportional, and tiered policy responses.

To examine this issue, this paper analyzes the governance models of the United States, the European Union, China, and developing nations, considering their respective positions in international trade agreements. By exploring the interests driving these models, we outline a potential path toward a global cross-border data flow governance framework.

THE MULTILATERAL DIGITAL TRADE SYSTEM AND CROSS-BORDER DATA FLOW

With the institutionalization of the World Trade Organization (WTO), the multilateral trade rule system has brought almost all trade-related matters under its jurisdiction. Consequently, trade disputes—including those concerning digital trade and cross-border data flows—can be submitted to WTO panels and the Appellate Body for adjudication and enforcement. This framework distinguishes the WTO from general international law, granting it a certain level of "hard law" characteristics (Burri, 2017).

Beyond its adjudicative function, the WTO serves as a platform for multilateral trade negotiations (Burri, 2017), positioning it theoretically as the most suitable forum for resolving issues related to digital trade and cross-border data flows. Recognizing the increasing significance of digital technologies, the WTO established a working group on electronic commerce (E-commerce) in 1998. This initiative aimed to address various dimensions of digital trade, including trade in services, trade in goods, intellectual property rights, and trade and development concerns (Burri, 2017; Duru¸et al., 2022). However, despite two decades of discussions, the expected results have not been realized (Usendok, et al., 2022).

A key challenge for the WTO is its inability to sufficiently adapt to the rapid evolution of digital trade. The organization struggles to address many of the contentious issues obstructing digital trade negotiations, largely due to fundamental cultural and policy divergences among countries (Okoko & Ahamefule, 2023).

In response to the WTO's limitations in governing cross-border data flows, countries have sought alternative approaches. Many have bypassed the multilateral system in favor of unilateral regulations, bilateral agreements, or regional trade agreements. These fragmented legal frameworks reflect diverse national priorities, such as personal data protection, trade liberalization, and national security concerns. Broadly, global digital trade agreements on cross-border data flows can be categorized into three primary models:

1. **The Trade-First Free Flow Model (United States):** Prioritizing economic liberalization and minimizing restrictions on data flows.
2. **The Human Rights and Digital Trade Balance Model (European Union):** Emphasizing data privacy and personal rights protection while facilitating digital trade.
3. **The Security, Personal Data Protection, and Free Flow Balance Model (China):** Striving to balance national security concerns, personal data protection, and economic interests.

These distinct regulatory approaches highlight the challenges in establishing a unified multilateral framework for digital trade. As global digital commerce continues to grow, navigating these competing models will be essential for shaping the future of cross-border data governance.

THE UNITED STATES: STRENGTHENING THE FREE TRADE SYSTEM

The United States has long prioritized free trade over privacy concerns in its digital trade policies. Since the Clinton administration, the U.S. has championed the "maximum possible free flow of cross-border information" while ensuring that regulatory differences between countries do not become substantial trade barriers. This approach has been central to U.S. efforts in shaping international digital trade rules.

In 2002, the U.S. introduced the **Digital Agenda**, a framework promoting the free flow of cross-border data through **bilateral** and **regional free trade agreements**. Market access remains the **core principle** of U.S. trade agreements, reflecting the global dominance of U.S. tech firms. As a result, these agreements generally focus on two key aspects:

1. **Emphasizing individual consumer choice** in digital products and services.
2. **Restricting government control over data flows** to avoid creating trade barriers.

A landmark example is the **2012 U.S.-South Korea Free Trade Agreement**, which included a clause on the free flow of information. While non-binding, it set a precedent by stating that "parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."

The **2016 Trans-Pacific Partnership (TPP)** further advanced this agenda. Chapter 14 of the TPP was the first binding international agreement to ensure cross-border data flows while restricting data localization requirements. It stipulated that governments must allow data to flow freely unless **restrictions are necessary for a legitimate public policy objective**—but even then, the restrictions must be minimal. Despite the U.S. withdrawing from the TPP, these provisions were **fully retained in the 2018 CPTPP** and the **2020 USMCA**, reinforcing U.S. leadership in digital trade policy.

Beyond trade agreements, the U.S. has actively promoted its free trade stance within the **WTO**. In 2019, it submitted a proposal titled **"The Economic Benefit of Cross-Border Data Flow,"** emphasizing free data flow as a driver of global economic growth. The proposal urged WTO members to adopt privacy mechanisms that **minimize trade restrictions** and advocated for an **interoperable regulatory framework** rather than country-specific restrictions.

THE EUROPEAN UNION: BALANCING HUMAN RIGHTS AND DIGITAL TRADE

Unlike the U.S., the **European Union prioritizes data privacy and human rights** over unrestricted trade in its digital policies. This approach is anchored in the **General Data Protection Regulation (GDPR)**, which enforces strict data protection rules not just within the EU, but also **extraterritorially**.

The **GDPR's territorial scope** follows two principles:

1. **The Effects Principle** – If an entity outside the EU impacts the privacy of EU residents, GDPR applies.

2. **The Territoriality Principle** – If a business is established within the EU, it must comply with GDPR, regardless of where the data is processed.

For **intra-EU data flows**, GDPR ensures that **personal data can move freely between EU member states**, provided privacy rights are upheld. However, for **cross-border data flows with third-party countries**, the EU imposes strict conditions. A country must meet the **GDPR's adequacy standard** before its companies can process EU citizens' data freely. This **"adequacy decision"** grants the EU **significant leverage in global data negotiations**, effectively extending EU data sovereignty beyond its borders.

Historically, the EU has resisted trade rules that might weaken privacy protections. Even during the **Uruguay Round of GATS negotiations**, the EU insisted that trade agreements should not override national privacy laws (Article 14.C.ii, GATS).

The EU's cautious approach to digital trade agreements is evident in its **bilateral trade deals**:

- The **2002 EU-Chile Agreement** included **non-binding** e-commerce clauses.
- The **2016 EU-Canada CETA Agreement** introduced provisions for building mutual trust in digital trade.
- The **2018 EU-Japan Economic Partnership Agreement** was the first to mention **cross-border data flows**, but only in a tentative manner, stating that both parties would "reassess" the need for free data flow clauses within three years.

A shift in EU policy emerged in **2018** with its proposal on **Cross-Border Data Flows and Personal Data Protection in Trade Agreements**. This proposal introduced **four prohibitions** aimed at removing unnecessary data flow restrictions:

1. **No mandatory use of domestic computing facilities** for data processing.
2. **No mandatory localized storage of data.**
3. **No prohibition on data processing in another country.**
4. **No forced data localization as a condition for trade.**

However, the proposal also reaffirmed that **personal data protection is a fundamental human right**, allowing states to impose privacy safeguards even if they restrict trade. This reflects the EU's continued insistence on balancing **human rights protection with economic interests**.

At the **WTO**, the EU has maintained this position, advocating for **higher privacy standards** in digital trade agreements. As GDPR enforcement grows stronger, future EU trade agreements may **further tighten data protection measures**, increasing the EU's influence in global digital markets (Gao, 2021).

KEY DIFFERENCES BETWEEN U.S. AND EU APPROACHES

Aspect	United States	European Union
Core Principle	Free trade and unrestricted data flow	Human rights and data protection
Legal Framework	Trade-first approach (Digital Agenda, CPTPP, USMCA)	Privacy-first approach (GDPR, adequacy decisions)

Aspect	United States	European Union
Government Control	Limits government interference in data flows	Allows restrictions to ensure privacy and security
Trade Agreements	Strong pro-free trade clauses in digital trade deals	Cautious approach, balancing trade with privacy
WTO Position	Advocates minimal trade barriers for data flow	Supports strict data protection in trade agreements

These differences highlight the **global divide in digital trade governance**. While the **U.S. prioritizes economic liberalization, the EU enforces stringent data protection laws,** often extending its influence beyond its borders. This divergence continues to shape international negotiations on cross-border data flows and digital trade rules.

THE SOURCES OF DIFFERENCES IN THE CROSS-BORDER FLOWS OF DATA NEGOTIATIONS: WHAT RIGHTS AND INTERESTS ARE PROTECTED?

The US, EU, and China

The diverging approaches of the US, EU, and China to cross-border data flows reflect their differing commercial interests and regulatory philosophies. The US prioritizes the protection of its digital service-oriented firms in the global e-commerce market, leveraging its dominance in digital services to advocate for minimal restrictions on data flows (Ota, et al., 2022). In contrast, China's e-commerce sector is more focused on traditional trade in goods facilitated by the internet, leading to a regulatory framework that emphasizes data sovereignty and national security. The EU, meanwhile, adopts stricter privacy regulations, which some view as a form of digital protectionism aimed at shielding its market from competition from both the US and China (Aaronson 2015; Chin and Li 2021).

Regulatory frameworks also differ significantly. The US operates under a "permissive legal framework," minimizing government intervention in the internet and relying heavily on corporate self-regulation. China, on the other hand, imposes extensive state-led regulations on its internet ecosystem, combining legal oversight with co- and self-regulatory mechanisms (Chin 2018, 2020; Chin et al. 2022). The EU, while prioritizing human rights and data protection, lacks dominant digital players in the global e-commerce market and does not have a centralized authority capable of overriding security concerns.

Developing Countries: Protecting the Right to Development and Maintaining Industrial Autonomy

Developing countries, particularly in Asia and Africa, approach cross-border data flows with a focus on protecting their digital industries and national security interests. Countries like India and members of ASEAN emphasize the importance of data localization and the need to safeguard national sovereignty and industrial autonomy. For instance, at the 2019 G20 Japan Summit, 24 countries, including the US, China, Russia, and the EU, signed the *Osaka Declaration on Digital Economy*, which promotes the free flow of data while addressing privacy, data protection, and security challenges. However, India, Egypt, Indonesia, and South Africa did not participate, reflecting their reservations about unrestricted data flows (Okon & Ahamefule, 2022).

India, in particular, has been vocal about its concerns. Commerce and Industry Minister Piyush Goyal argued that developing countries need time and policy space to build their legal and regulatory frameworks before engaging in e-commerce negotiations. India's policy favors data localization, viewing data as a national asset critical for development rather than primarily an individual right. Goyal emphasized that data is a "new form of wealth" and that digital trade negotiations must account for the needs of developing countries (Greenleaf 2019).

Similarly, the African Group has highlighted the persistent digital divide, warning that without addressing this gap, technological, income, and infrastructural disparities will widen. They argue that developing countries must use active policies, including data localization, internet filtering, and technology transfer requirements, to build infrastructure, manage digital flows, and foster domestic digital industries. The group opposes the introduction of a "digital trade agenda" in the WTO, arguing that it would constrain their ability to implement industrial policies and catch up with more advanced economies. They advocate for a focus on equity rather than efficiency to achieve inclusive and sustainable growth.

Despite these reservations, developing countries recognize the need for international collaboration in the digital economy. The *Regional Comprehensive Economic Partnership (RCEP)*, signed by ASEAN in November 2020, includes provisions for cross-border data flows in its Chapter 12 on Electronic Commerce. The RCEP allows each member state to maintain its regulatory requirements for data transmission while prohibiting restrictions on cross-border data flows for business purposes. It also includes flexible exceptions for legitimate public policy and essential security interests, empowering member states to determine what constitutes a legitimate public policy (Hong 2021a). This flexibility is particularly important for underdeveloped countries like Cambodia and Laos, which are given a five-to-eight-year buffer period to comply with the agreement's provisions.

THE ROLE OF NATIONAL SECURITY IN DIGITAL TRADE

The role of national security in digital trade has become increasingly contentious. Two opposing views dominate the debate: (1) security considerations should be minimized in trade to avoid undermining globalization and trade interdependence, and (2) trade and security are inherently intertwined, as trade enables countries to accumulate wealth and project strategic interests globally (Olson 2022). Security exceptions in trade agreements are often used to justify restrictive measures, with the concept of national security expanding to include not only military and defense interests but also areas like food security, energy security, cybersecurity, and health security (Heath 2020; Mishra 2020).

Trade agreements like the *Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)* include broad security exceptions. Article 29.2 of the CPTPP allows parties to restrict data flows or access to information if they determine it is necessary to protect their essential security interests. This provision has been criticized for being overly expansive and self-judging, potentially allowing countries to justify arbitrary or protectionist measures under the guise of national security (Olson 2021). Critics warn that such exceptions could undermine the integrity of trade agreements and lead to conflicts between trade norms and security policies.

CYBERSECURITY MEASURES AND TRADE AGREEMENTS

Cybersecurity measures, such as data localization requirements, are often viewed as trade barriers because they can hinder the cross-border supply of services and disrupt global data operations. These measures may conflict with international trade obligations, including market access, non-discrimination, transparency, and domestic regulation (Meltzer 2019). However, developing countries argue that such measures are necessary to protect national security and promote domestic industries.

The debate over whether cybersecurity should be treated as a national security issue or a public policy issue remains unresolved. Some argue that cybersecurity measures should be subject to the general exception rules of trade agreements, which require a balancing of policy objectives, the impact of the measure, and its proportionality. Others contend that cybersecurity is an integral part of national security, given its implications for economic stability, social governance, and public safety (Heath 2020).

The Case of Nigeria

Nigeria, like many developing countries, faces challenges in balancing the benefits of cross-border data flows with the need to protect national security and promote domestic industries. The country has been working to develop its digital economy through initiatives like the *National Digital Economy Policy and Strategy (2020-2030)*, which aims to leverage digital technologies for economic growth. However, Nigeria

also recognizes the risks associated with unrestricted data flows, particularly in terms of data privacy, cybersecurity, and economic dependency.

In recent years, Nigeria has taken steps to regulate cross-border data flows, including the introduction of the *Nigeria Data Protection Regulation (NDPR)* in 2019. The NDPR requires data controllers and processors to ensure that personal data transferred outside Nigeria is subject to adequate protection. This aligns with the global trend of data localization and reflects Nigeria's commitment to safeguarding its citizens' data while promoting digital trade.

THE SELF-JUDGING NATURE OF SECURITY EXCEPTIONS

The question of whether security exceptions in trade agreements are self-judging remains contentious. While some argue that national security issues are political and should not be subject to judicial review, the WTO has ruled that security exceptions must be invoked in good faith and cannot be used to circumvent trade obligations. In the *Russia – Traffic in Transit* case, the WTO Panel held that "essential security interests" must be narrowly defined and that measures taken under this exception must be proportionate and necessary (Heath 2020). This ruling underscores the need for clarity and accountability in the use of security exceptions in trade agreements.

To address the growing intersection of security and trade, innovative approaches are needed. These include international policy coordination, transnational dialogues, and regulatory cooperation to reconcile differing national security priorities with global trade obligations. For instance, China's *Global Initiative on Security* proposes a comprehensive approach to addressing both traditional and non-traditional security challenges, emphasizing the need for international cooperation in areas like cybersecurity and climate change (Wang 2022). Such initiatives highlight the importance of adapting global governance frameworks to the evolving realities of the digital economy.

THE ESTABLISHMENT OF REGIONAL INTEROPERABILITY MECHANISMS

Developed countries, including the United States, the European Union, Japan, and South Korea, have sought new cooperative approaches to establish cross-border data flow interoperability mechanisms. First, the United States and the European Union have made multiple attempts to establish a cross-border data flow cooperation mechanism. On March 25, 2022, the European Commission and the United States announced an agreement in principle on a new Trans-Atlantic Data Privacy Framework, committing to finalizing legal texts (European Commission 2020, 2022).

Second, the United States has actively used the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) framework to expand the scope of cross-border data flows. CBPR is a voluntary mechanism that requires participating businesses to comply with the personal data protection rules outlined in the APEC Privacy Framework, first adopted in 2005 and revised in 2015. While CBPR

does not alter domestic privacy laws, it requires participating economies to sign the "Cross-Border Privacy Enforcement Agreement" to facilitate cooperation on privacy enforcement. Eight APEC members—Australia, Canada, Japan, South Korea, Mexico, Singapore, the United States, and Chinese Taipei—have joined the mechanism. Substantial cooperation has already begun between the United States and Japan, and CBPR members such as Japan, South Korea, and Canada have passed the adequacy tests under the EU's GDPR. The United States has also worked to extend CBPR beyond APEC, aiming to enhance its interoperability with the GDPR. In the USMCA, provisions on "cross-border data flows" were complemented by a requirement to recognize CBPR as an effective mechanism for promoting data transfers under the "personal information protection" clause, effectively positioning CBPR as a uniform standard among the contracting states.

On April 21, 2022, the US, along with Canada, Japan, South Korea, the Philippines, Singapore, and Chinese Taipei, established the Global CBPR Forum to promote global adoption of the CBPR and Privacy Recognition for Processors (PRP) Systems. The goal is to enhance data protection while enabling free data flows and interoperability with other privacy frameworks. The forum aims to establish an international certification system based on the CBPR and PRP Systems, providing businesses with a mechanism to demonstrate compliance with internationally recognized privacy standards (US Department of Commerce 2022). However, a major criticism is that CBPR's privacy protections rely on the APEC Privacy Framework, which offers a limited level of personal data protection. The framework is built on outdated OECD Guidelines, making it a first-generation privacy protection model. This raises concerns that CBPR's low privacy standards may lead to the unrestricted flow of personal data to the US and US-based companies (Hong 2021b).

Third, the EU has also expanded its cross-border data flow mechanisms, prioritizing bilateral cooperation through the GDPR's adequacy decisions. As of April 2022, the European Commission had recognized 14 countries as providing an adequate level of personal data protection. Future negotiations will prioritize engagement with India, Indonesia, Latin American countries (such as Brazil and Chile), and Eastern and Southern European nations. The EU has also explored the possibility of multilateral data flows based on the Council of Europe's Convention 108+, a modernized version of the 1981 Convention on data protection. By 2022, 55 countries had joined the Convention (Council of Europe 2019; Wang 2018).

Fourth, other developed nations, such as Japan and South Korea, have actively joined US-EU data flow interoperability initiatives to strengthen their digital economies. Japan has played a key role in cross-border data flow initiatives, promoting the concept of "Data Free Flow with Trust" at the 2019 Davos Forum and pushing for its adoption in the G20 Osaka Declaration on Digital Economy. South Korea has also systematically revised its domestic personal data protection laws and passed the EU's adequacy decision in December 2021.

While these competing regional interoperability mechanisms have enhanced international regulatory cooperation, they remain closely aligned with existing geopolitical and trade blocs. As a result, they do not fully address the fundamental challenge of establishing a truly global regulatory framework for cross-border data flows. Achieving a more balanced and inclusive international mechanism remains a critical goal.

NIGERIA AND THE CHALLENGE OF GLOBAL DATA FLOW GOVERNANCE

Nigeria, as Africa's largest economy and a rising player in the digital space, faces unique challenges in navigating global data governance frameworks. While Nigeria has embraced digital trade and cross-border data flows as part of its economic growth strategy, it also faces regulatory constraints due to data protection concerns. The Nigerian Data Protection Regulation (NDPR), introduced in 2019, aligns with global best practices by emphasizing data privacy and user rights. However, unlike the EU's GDPR, the NDPR lacks explicit adequacy agreements with major trade partners, making cross-border data transfers subject to complex compliance requirements.

Nigeria's digital economy strategy aims to foster greater engagement with international frameworks, including the African Continental Free Trade Area (AfCFTA) digital trade initiatives. However, the absence of a comprehensive regional data protection framework in Africa creates uncertainty regarding data transfer mechanisms. While Nigeria has signed agreements with international tech companies to facilitate digital trade, the country must navigate tensions between open data flow policies championed by the United States and stricter data sovereignty principles promoted by the EU.

Furthermore, Nigeria's reliance on foreign digital infrastructure, including cloud computing services hosted outside the country, raises concerns about data security and local control. The government has signaled interest in developing a national data strategy that balances economic benefits with regulatory oversight. This includes exploring interoperability mechanisms that align Nigeria's data governance policies with global standards while ensuring local data sovereignty.

Ultimately, Nigeria's approach to cross-border data governance will depend on its ability to engage with global regulatory trends while safeguarding national interests. Given the country's growing digital economy and increasing participation in international trade agreements, Nigeria must proactively shape its policies to align with evolving global data governance standards.

CHALLENGES OF GLOBAL STANDARD SETTING

Governments must strike 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 other digital rights of citizens (Taheri et al. 2021). However, inconsistent, contradictory, or incompatible cross-border

data policies are among the biggest risks to the digital economy. Efforts are needed to consolidate these rules around similar frameworks, but there are currently limited arenas for managing these challenges (Elms 2021).

The CPTPP, RCEP, and DEPA, as recent international frameworks for cross-border data flows, have reserved public policy space for governments, but these agreements have regional characteristics and can only serve as phased plans for governing international data transfers. Negotiations on cross-border data flow rules are challenging due to conflicts of national interests between developing and developed countries, as well as geopolitical rivalries. Historically, developed countries have leveraged international trade rules to better serve their interests in negotiations with developing nations. Additionally, the US government has used international rules to pressure China, limiting its participation in global trade rule-making and excluding it from regional interoperability mechanisms for cross-border data flows (Liu and Gong 2013; Sun 2016). The Information Technology and Innovation Foundation has advocated for disqualifying China from global rule-setting activities for digital trade unless it makes binding commitments on data flows, arguing that data flows should be central to any WTO e-commerce outcomes (Cory 2019). However, China's cross-border data rules will inevitably influence the development of international standards, making engagement with China in crafting shared norms unavoidable.

One way to reconcile these divergences is through compatibility mechanisms. In privacy standards, these mechanisms could include mutual recognition of regulatory outcomes, reliance on international standards, recognition of comparable protections under domestic legal frameworks or certification systems, and other ways to secure data transfers between parties (Drake-Brockman et al. 2021). Interoperability mechanisms play a crucial role in this effort.

THE ESTABLISHMENT OF REGIONAL INTEROPERABILITY MECHANISMS

Developed countries, including the United States, the European Union, Japan, and South Korea, have pursued new ways of cooperation to establish cross-border data flow interoperability mechanisms. The United States and the European Union have attempted multiple times to create a framework for data flows. On March 25, 2022, the European Commission and the United States announced an agreement in principle on a new Trans-Atlantic Data Privacy Framework (European Commission 2020, 2022).

The United States also promotes the APEC Cross-Border Privacy Rules (CBPR) system, a voluntary framework adopted in 2005 and revised in 2015, allowing participating companies to comply with international privacy protection standards. The CBPR does not override domestic data legislation but requires participating economies to sign the "Cross-Border Privacy Enforcement Agreement" to facilitate law enforcement. Eight APEC economies, including Australia, Canada, Japan, South Korea, Mexico, Singapore, Chinese Taipei, and the United States, have joined the CBPR. Additionally, Japan, South Korea, and Canada—CBPR members—have also passed the EU's GDPR adequacy tests.

Beyond APEC, the United States seeks to expand CBPR's reach, particularly in promoting interoperability with GDPR. The USMCA recognizes CBPR as an effective mechanism for cross-border data transfers. On April 21, 2022, the United States, along with Canada, Japan, South Korea, the Philippines, Singapore, and Chinese Taipei, established the Global CBPR Forum to promote global adoption of CBPR and the Privacy Recognition for Processors (PRP) System. This initiative aims to facilitate data protection while ensuring free data flows (US Department of Commerce 2022). However, the CBPR's reliance on the APEC Privacy Framework has been criticized for offering a limited level of personal data protection. The APEC Privacy Framework, built on the OECD Guidelines, remains at a first-generation level of personal data protection legislation (Hong 2021b).

The European Union continues expanding its cross-border data framework by prioritizing bilateral cooperation and adequacy decisions under GDPR. As of April 2022, 14 countries have been recognized as having adequate levels of personal data protection. The EU is also exploring multilateral agreements under Convention 108+, which has been joined by 55 countries (Council of Europe 2019; Wang 2018).

Japan and South Korea actively participate in the US-EU data flows interoperability mechanisms to strengthen their digital economies. Japan seeks to act as a bridge between the US, EU, and other economies, promoting the "trusted data free flow with trust" concept at the 2019 Davos meeting, which was incorporated into the G20's Osaka Declaration on Digital Economy. South Korea has revised its data protection laws multiple times and passed the EU's adequacy decision in December 2021.

Despite these regional initiatives, global standard-setting remains fragmented, as regional agreements align closely with geopolitical power structures and existing trade blocs. A more inclusive international mechanism is necessary for regulating cross-border data flows.

THE NIGERIAN CONTEXT

Nigeria, as Africa's largest economy, faces unique challenges in cross-border data governance. The country's data protection landscape is primarily governed by the Nigeria Data Protection Regulation (NDPR) of 2019. While the NDPR provides a framework for personal data protection, it does not comprehensively address cross-border data flows. The Nigerian government has indicated its intention to establish a robust data governance framework, particularly through the proposed Nigeria Data Protection Bill.

Nigeria's digital economy strategy emphasizes the need for data sovereignty while promoting foreign investments in the tech sector. However, concerns about data localization and compliance with international data standards persist. Nigeria, like many developing countries, must navigate the balance between enabling global data flows and safeguarding national interests. Given its role as a regional economic leader, Nigeria has an opportunity to influence Africa's approach to cross-border data

governance, especially in alignment with the African Continental Free Trade Area (AfCFTA).

THE ROLE OF THE WTO IN DEFINING INTERNATIONAL RULES IN DATA FLOWS

International regulations for cross-border data flows should not enforce uniform standards but rather establish a global framework for data movement. The key challenge is achieving consensus on the model, scope, and pathways for data flow governance. While national security and data localization concerns are often cited as obstacles, the primary issue remains the lack of an international regulatory framework. Countries must balance the free flow of data with legitimate policy goals and digital rights (Burri 2021).

The WTO's negotiations on e-commerce have made progress through the Joint Statement Initiative (JSI), launched in 2019 by 76 WTO members. By 2021, 86 members, representing over 90% of global trade, had joined these negotiations. The JSI aims to establish provisions on open government data, e-contracts, online consumer protection, and paperless trading. On June 13, 2022, during the 12th WTO Ministerial Conference, the JSI, alongside Switzerland, introduced the E-commerce Capacity Building Framework to enhance digital inclusion for developing countries. The conveners emphasized the need to balance data flow provisions with considerations such as the digital divide and capacity-building needs.

China's position is that data flows must be regulated based on security considerations, ensuring compliance with national laws and international standards. Given the complexity of digital trade, a WTO agreement on e-commerce and cross-border data flows could offer a more balanced approach than regional trade agreements. A WTO framework could provide sufficient policy space for national priorities while ensuring globally accepted minimum standards (Burri 2021).

CONCLUSION

Despite differing regulatory models between the US, EU, and China, regional trade agreements indicate some convergence in cross-border data governance. The US, historically advocating for unrestricted data flows, has included data protection clauses in agreements like the USMCA and CPTPP. The EU prioritizes consumer data protection but has also promoted free data flows in trade agreements. China has advanced initiatives like the "Global Initiative on Data Security" and the RCEP's prohibition of data localization.

For developing nations like Nigeria, cross-border data governance must balance economic growth with regulatory compliance. The WTO could serve as a platform for an inclusive, proportional, and tiered approach to global data flow regulations. A narrowly scoped WTO agreement with legitimate exception provisions could help bridge the digital divide and establish a more unified framework for data governance.

REFERENCES

Aaronson, S. (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. https://doi.org/10.1017/S147474561500011X

Burri, M. (2017). The governance of data and data flows in trade agreements: The pitfalls of legal adaptation. *UC Davis Law Review, 51*(1), 65–132.

Burri, M. (2021). A WTO agreement on electronic commerce: An enquiry into its legal substance and viability. *Trade Law 4.0 Working Paper Series*. https://ssrn.com/abstract=3976133

Chin, Y.-C. (2018). The legitimation of media regulation in China. *Chinese Political Science Review, 3*(2), 172–194. https://doi.org/10.1007/s41111-018-0097-z

Chin, Y.-C. (2020). Internet governance in China: The network governance approach. In Z. Wang & D. Pavlicevic (Eds.), *Social relations and political development in China: Change and continuity in the 'new era'* (pp. 134–153). Routledge.

Chin, Y.-C., & Li, K. (2021). Sovereignty in cyberspace: EU and China compared. *Paper presented at TPRC49: The 49th Research Conference on Communication, Information and Internet Policy*. https://ssrn.com/abstract=3900752

Chin, Y.-C., Park, A., & Li, K. (2022). A comparative study on false information governance in Chinese and American social media platforms. *Policy and Internet, 14*(2), 263–283. https://doi.org/10.1002/poi3.297

Cory, N. (2019). Why China should be disqualified from participating in WTO negotiations on digital trade rules. *Information Technology & Innovation Foundation*. https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital

Council of Europe. (2019). *Data protection*. http://www.coe.int/dataprotection

Cyberspace Administration of China. (2022). *Measures for data export security assessment*. http://www.gov.cn/zhengce/zhengceku/2022-07/08/content_5699851.htm

Desierto, D. (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*. https://www.ejiltalk.org/national-security-defenses-in-trade-wars-and-investment-walls-us-v-china-and-eu-v-us/

Dr2 Consultants. (2022). *European Data Act: A harmonized framework for accessing and sharing data*. https://dr2consultants.eu/european-data-act/

Drake-Brockman, J., Gari, G., Harbinson, S., Hoekman, B., Nordås, H. K., & Stephenson, S. (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). https://iit.adelaide.edu.au/ua/media/1551/wp-2021-11-j.drake-brockman-et-al.pdf

Duru, I. U., Eze, M. A., Yusuf, A., Udo, A. A., & Saleh, A. S. (2023). Effect of reward systems on workers' performance at the university of Abuja. *Asian Journal of Social Sciences and Management Studies*, *10*(1), 9-18.

Duru, I. U., Eze, M. A., Yusuf, A., Udo, A. A., & Saleh, A. S. (2022). Influence of motivation on workers' performance at the University of Abuja. *International Journal of Social and Administrative Sciences*, *7*(2), 69-84.

Elms, D. (2021). *China applies to join DEPA*. Asian Trade Centre. http://asiantradecentre.org/talkingtrade/china-applies-to-join-depa

European Commission. (2020). *Joint press statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross*. 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

European Commission. (2022). *European Commission and United States joint statement on Trans-Atlantic Data Privacy Framework*. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087

Gao, H. (2018). Regulation of digital trade in US free trade agreements: From trade regulation to digital regulation. *Legal Issues of Economic Integration, 45*(1), 47–70. https://doi.org/10.54648/LEIE2018004

Gao, H. (2021). Data regulation in trade agreements: Different models and options ahead. In M. Smeets (Ed.), *Adapting to the digital trade era: Challenges and opportunities* (pp. 322–334). WTO Press.

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

He, B. (2019). The development challenges and countermeasures of data sovereignty. *Journal of Cyber and Information Law, 1*, 201–216.

Heath, J. B. (2020). Trade and security among the ruins. *Duke Journal of Comparative and International Law, 30*(2), 223–266.

Hong, Y. (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.

Hong, Y. (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.

Liu, J., & Gong, Y. (2013). An analysis of the Obama administration's "rules diplomacy" towards China. *Forum of World Economic and Political, 3*, 84–96.

Meltzer, J. (2019). Governing digital trade. *World Trade Review, 18*(S1), S23–S48. https://doi.org/10.1017/S1474745618000507

Ministry of Foreign Affairs of China. (2020). *Global Initiative on Data Security*. https://www.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/202010/t20201029_9869292.shtml

Mishra, N. (2020). The trade–(cyber)security dilemma and its impact on global cybersecurity governance. *Journal of World Trade, 54*(4), 567–590. https://doi.org/10.54648/TRAD2020023

Okoko, C. O., & Ahamefule, I. C. (2023). Historicizing Political Dichotomy Among the Double Unilineal but Prevalently Matrilineal Cross River Igbo. *British Journal of Multidisciplinary and Advanced Studies*, *4*(5), 1-26.

Okon, I. E., & Ahamefule, I. C. (2023). Indigenous Agrarian Institutions for Capital Formations among the Ibibio People, 1900-2000. *Akwa Ibom State University Journal of Arts*, *4*(1).

Olson, S. (2021). The conventional wisdom on China and the CPTPP is wrong. *Hinrich Foundation*. https://www.hinrichfoundation.com/research/article/ftas/china-and-cptpp/

Olson, S. (2022). Ukraine forces debate on WTO and national security. *Hinrich Foundation*. https://www.hinrichfoundation.com/research/article/wto/ukraine-debate-on-wto-national-security/

Ota, E. N., Okoko, C. O., & Ahamefule, I. C. (2022). Fiscal federalism and resource control in Nigeria: Deconstructing conundrum. *Global Journal of Arts, Humanities and Social Sciences*, *10*(1), 1-20.

Qi, A., & Zhu, G. (2016). On the establishment and improvement of the national data sovereignty system. *Journal of Soochow University (Philosophy and Social Sciences Edition), 1*, 83–88.

Shaffer, G. C., & Pollack, M. A. (2010). Hard vs. soft law: Alternatives, complements, and antagonists in international governance. *Minnesota Law Review, 94*(3), 706–799.

Sun, Y. (2016). International institutional pressure and China's free trade zone strategy. *Quarterly Journal of International Politics, 1*, 125–161.

Taheri, R., Adams, O., & Stern, P. (2021). *DEPA: The world's first digital-only trade agreement*. Asia Pacific Foundation of Canada. https://www.asiapacific.ca/publication/depa-worlds-first-digital-only-trade-agreement

Tang, X. (2021). Between data security and openness: A Chinese approach to international rulemaking for digital trade. *Political Science and Law, 12*, 26–38.

US Department of Commerce. (2022). *Global Cross-Border Privacy Rules Declaration*. https://www.commerce.gov/global-cross-border-privacy-rules-declaration

Usendok, I. G., Akpan, A., & Ekpe, A. N. (2022). Effect of Board Size and Board Composition on Organizational Performance of Selected Banks in Nigeria. *International Journal of Business and Management Review*, *10*(5), 1-25. AKSUJACOG, 1(3).

Uto, S. C., Uwa, K. L., & Akpan, A. (2024). Knowledge management and competitive advantage in selected manufacturing firms in Akwa Ibom State. *International Journal of Business and Management Review*, *12*(1), 1-20.

Wang, R. (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.

Wang, Y. (2022). Implement global security initiatives to safeguard world peace and tranquility. *Ministry of Foreign Affairs of China*. https://www.mfa.gov.cn/wjbzhd/202204/t20220424_10672812.shtml

Wei, L. (2022). Implement the overall national security concept and effectively build a data security barrier. *China Information Security*. https://mp.weixin.qq.com/s/9UaqliGKIM7FDTlrECoeOA

Xu, D. (2020). On the legal guarantee of two-way compliance of cross-border data flow regulating enterprises. *Eastern Law, 2*, 185–197.

Zhang, L., & Peng, Z. (2022). The influence of China's international rules on data security needs to be improved. *Information Security and Communication Privacy, 3*, 27–32.

Zhu, F. (2021). The international game of digital trade rules, "seeking for common" dilemma and China's strategy. *Economic Review Journal, 8*, 40–49.