



The Role and Strategy of Multinational Enterprises in Global Data Governance: Challenges and Opportunities

Jun Wang

Central South University, Changsha, 410017, China

8101210112@csu.edu.cn

Abstract. In the current digital information age, data is increasingly becoming another major resource for world economic development and global cooperation in addition to goods and services. Cross-border flow of data is an important link in the realization of data value. This paper analyses the important roles and strategies played by multinational enterprises in cross-border flow of data as well as the challenges they encounter, such as legal obstacles and policy barriers, conflict between data sovereignty and globalization strategies, issues of trust and co-operation in the international business environment, etc., and some of the opportunities embedded in the challenges. The position and dilemmas of MNEs in global data governance are also discussed through instructive and exemplary case studies of three large multinational enterprises, Google, Amazon, and Alibaba, related to cross-border data flows. Finally, solutions are proposed for seeking a balance between multinational enterprises and global data governance in order to promote further data globalization.

Keywords: Global Data Governance, Cross-Border Data Flows, Multinational Enterprises, Globalization Strategies.

1 Introduction

Given how quickly information technology is developing, data has increasingly become one of the core production factors in the era of digital economy. Furthermore, as the process of globalization deepens, data are becoming more widely disseminated globally. Inevitably, some problems arise in the process of globalized sharing of data, which requires globalized governance of data. The United Nations and other international agencies have begun to work on global data governance. In addition to this, numerous regional and national initiatives are underway to control the gathering and application of digital data. It is worth mentioning that, the European Union's (EU) General Data Protection Regulation (GDPR) represents a major step forward for global data governance. In 2018, California enacted the California Consumer Protection Act (CCPA), following the momentum generated by the GDPR. While drawing inspiration from the GDPR, the CCPA also customizes regulations to suit California's unique legislative landscape as a state law. [1]. In these cross-border flows of data, personal data accounts for a large proportion. Multinational enterprises are an important carrier

© The Author(s) 2024

B. Siuta-Tokarska et al. (eds.), *Proceedings of the 2024 2nd International Conference on Management Innovation and Economy Development (MIED 2024)*, Advances in Economics, Business and Management Research 300, https://doi.org/10.2991/978-94-6463-542-3_42

and driving force for the cross-border flow of personal data. For instance, the operations of large multinational enterprises such as Google and Amazon in the United States and Alibaba and ByteDance in China are inseparable from the collection, flow and utilization of personal data.

Data is now a crucial cross-border and transnational resource. The international community does not have an efficient system for data governance, which makes complicates and hinders cross-border data transfers, presenting a myriad of challenges. Through its research, this paper aims to offer solutions to these challenges, proposing strategies for the efficient and secure management of global data flows. It seeks to facilitate the resolution of conflicts between multinational corporations and host countries regarding data control and the protection of personal information. By doing so, this paper aims to support the seamless operation and growth of transnational enterprises, contributing to the furtherance of international investment and the global economy. Furthermore, it endeavors to contribute to the establishment of a more stable and secure global economic order, thereby fostering the progression of economic globalization.

This paper unfolds across five sections, offering a structured journey through the complex landscape of global data governance and the role of multinational enterprises within it. The initial section provides an overview of the research background, objectives, and its significance, setting the stage for a comprehensive exploration of the subject matter. The second section examines the practical challenges encountered in global data governance, highlighting the legal, policy, and business hurdles that complicate cross-border data flows. In the third section, we conduct case studies on leading multinational enterprises, including Google, Amazon, and Alibaba, to illustrate the real-world implications of these challenges on their operations. The fourth section presents a suite of solutions and strategic approaches designed to address the identified dilemmas, proposing actionable pathways towards more effective data governance. A synopsis of the main conclusions and observations on the wider ramifications for the future of international data flows and economic globalization are included in the paper's conclusion.

2 Real-World Challenges: Multinational Companies in Global Data Governance

2.1 Legal and Policy Barriers to Cross-border Data Flows

The flow of data across borders is a very significant part of both for multinational companies, organizations, consumers and global economic development. However, many countries have erected a number of legal and policy barriers to the cross-border flow of global data on grounds of individual privacy, national security or economic mercantilism. In practice, these reasons are in most cases untenable or exaggerated. A prime example is "data localization," which confines data within a country's borders, severely limiting the outward flow and transmission of data. Data localization requirements can either be mandated by law or arise organically due to a combination of

other restrictive policies. These policies may include mandating businesses to store a copy of data locally, processing data within the local jurisdiction, or necessitating individual or governmental consent prior to any data transfer. These regulations provide a fresh impediment to international digital trade. Foreign companies suffer when data transfers are interrupted or made more difficult or costly. This is particularly relevant for smaller internet-based companies and platforms. They often lack the resources to navigate the stringent regulations of every country where they operate or have customers.

In essence, these tactics amount to data protectionism, as they complicate or increase the costs of data transfers, particularly affecting companies in countries where they have customers [2]. By stifling the cross-border flow of data, these measures can hinder international digital trade, stifle innovation, and slow the pace of economic growth. Moreover, they contribute to a fragmented global digital marketplace, where the rules of engagement vary widely from one jurisdiction to another, increasing complexity and compliance costs for businesses of all sizes. Furthermore, these barriers do not only impact foreign enterprises but can also backfire on the economies that impose them. By restricting access to global digital services and markets, they can limit the opportunities for local businesses and consumers, potentially leading to higher costs and reduced choices. The long-term effect can be a slowdown in the host country's own economic development and a diminished role in the global economy.

2.2 The Conflict Between Data Sovereignty and Globalization Strategies

Globalization describes the growing interconnectedness among the economies, cultures, and populations worldwide, driven by advancements in technology, cross-border trade of goods and services, investment exchanges, and the movement of information and people. Global strategy fundamentals can support company executives in navigating a challenging situation. Globalization also has a significant impact in business, including increasing innovation, reducing costs, and better risk diversification. The cross-border flow of data is an important part of globalization and, at the same time, can contribute to the advancement of globalization strategies. Data can be used as an intermediate, a product, or for a variety of other purposes. Data has an impact on the economy on a personal, home, business, national, and worldwide scale. We can draw the conclusion that data drives the process of globalization.

However, the rise of data sovereignty challenges this narrative. This concept underscores the right of individuals and states to control data collection, storage, and utilization within their territories, asserting a form of digital self-determination [3]. After the Snowden's reveal, many states make efforts to reinforce their data sovereignty through technical and legal solutions. It's worth noting that the EU introduced the General Data Protection Regulation (GDPR) in May 2018. This regulation is designed to oversee the handling of users' data by third parties operating online.

While the protection of personal and national data is paramount, the stringent regulation of data flows can impede the essence of globalization, creating a tension between local data governance and global digital integration. The introduction of data security laws and other regulations may be seen as necessary for protecting sover-

eignty, but they can also restrict the free movement of data across borders, challenging the global strategies of businesses and potentially stifling economic growth and innovation.

2.3 Issues of Trust and Cooperation in the International Business Environment

In the realm of international business, trust and cooperation stand as foundational elements for successful relationships. The complexities of global operations, including communication hurdles, coordination difficulties, and the inherent uncertainties of cross-border interactions, underscore the critical importance of trust. These challenges are further compounded by cultural, legal, and regulatory differences between entities from various nations, making the establishment and maintenance of trust a daunting task [4]. Trust plays a crucial role in fostering cooperation. Positive expectations regarding the future actions of another organization are heavily influenced by perceptions of its reliability. Consequently, this encourages parties to be more open and vulnerable with each other, enabling a more precise anticipation of risk-taking decisions, behaviors, and other outcomes. However, achieving this level of trust in an international context is fraught with obstacles.

Firstly, cultural differences between home and host countries, as well as between multinational enterprises and host countries, may lead to mutual distrust. If a multinational enterprise and a host country can understand each other's cultural differences, then they can communicate effectively with their partners. Otherwise, if they cannot communicate effectively, both parties will lose the basis of trust in each other. Secondly, diverse legal and regulatory frameworks across countries can create uncertainties and complexities in business operations. Variations in legal systems, contract enforceability, and intellectual property protection can affect trust and cooperation between international business partners. Additionally, political instability, changes in government policies, economic crises, or trade disputes represent further challenges to establishing trust. Such unpredictable conditions can deter long-term investment and collaboration efforts, as they introduce significant risks and uncertainties into the business environment.

3 Case Analysis of Multinational Companies and Global Data Governance

3.1 Google and the EU GDPR Compliance Challenge

Cross-border compliance pertains to organizations' adherence to regulatory requirements and compliance obligations while operating across multiple jurisdictions. Google's challenge with the EU's GDPR shortly after its enactment in June 2018 exemplifies the intricacies of such compliance efforts. The French data protection authority, CNIL, initiated an investigation following complaints from ten thousand data subjects represented by La Quadrature du Net and NOYB. These complaints accused

Google of lacking a legitimate basis for processing personal data for behavioral analysis and ad personalization.

After conducting a number of online inspections on Google's platform in response to the complaints, the CNIL concluded that Google had violated several key provisions of the GDPR. First, the CNIL discovered that Google had violated Article 12 of the GDPR by failing to provide users with easy access to the pertinent data protection notification. The notification was found to be "not always clear and comprehensive" and to require users to take a few steps before they could view it.

Second, they discovered that Google had violated Article 13 of the GDPR as its notice did not adhere to the need to give data subjects precise, required information. According to the CNIL, because the material was "too generic and vague," "users lack a complete understanding of the extent of processing operations conducted by Google." Given that Google collected personal data for numerous purposes, it was determined that the company's processing operations were "particularly massive and intrusive." Users were found to be practically unable to exercise their right to refuse to have their data processed for ad personalization. Instead of being explicitly asked to consent to ad targeting, users were prompted to accept Google's terms and privacy policy in bulk. Because users grant consent for all of Google's processing activities collectively, instead of providing individual consent for each processing purpose, it was determined that this does not fulfill the "specific" requirement for consent outlined in the GDPR.

This decision served as a warning to all businesses operating in the EU about the repercussions of not meeting the necessary requirements. This ruling underscores the importance for businesses and marketing teams to ensure that their data protection notices are accurate, up-to-date, and effectively brought to the attention of data subjects to ensure full compliance with the GDPR.

3.2 Amazon's Data Management Practices in Different Jurisdictions

In navigating the complexities of cross-border data flows, multinational corporations like Amazon have implemented robust data management practices tailored to comply with various jurisdictional regulations while maintaining operational efficiency and user trust. Amazon's data management practices are guided by a comprehensive data governance framework that governs the collection, use, and sharing of data across its diverse business units and services. This framework encompasses policies and procedures for data classification, access controls, retention, and sharing agreements with third parties, ensuring accountability and transparency in data processing activities.

To begin with, Amazon places a high priority on compliance with data protection regulations in different regions, such as the General Data Protection Regulation (GDPR) in the European Union (EU). By obtaining user consent for data collection and processing activities, implementing actions to protect the security and privacy of personal information, and providing mechanisms for users to access, rectify, or delete their data, Amazon strives to uphold the principles of data protection while delivering personalized services and experiences.

In regions where data sovereignty regulations mandate the storage of particular data within designated geographic limits, Amazon employs data localization strategies to

ensure compliance. Nations and territories globally have introduced and implemented numerous regulations concerning data privacy, protection, and localization. These regulations compel companies to shift away from their conventional uniform approach to data management. Organizations that previously thrived with a global mindset must now adapt to local considerations. Amazon's strategies involve establishing data centers or utilizing cloud services with local presence to store data locally, thereby addressing regulatory requirements while maintaining data availability and accessibility for global operations.

Additionally, to mitigate risks associated with data breaches and unauthorized access, Amazon implements robust data security measures. These actions include encrypting data during transmission and storage, enforcing stringent access controls, performing routine security evaluations, and setting up protocols for responding promptly and effectively to security breaches.

Furthermore, Amazon tackles challenges across multiple jurisdictions by utilizing mechanisms such as Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or relying on adequacy decisions made by data protection authorities. These measures ensure the lawful transfer of data across borders, uphold user privacy, and comply with regulatory mandates.

3.3 Alibaba's International Data Flow and Localization Strategy

Alibaba, as a leading global e-commerce and technology enterprise, has implemented various strategies to manage international data flow and localization effectively.

Alibaba facilitates cross-border data transfer while ensuring compliance with relevant regulations. This involves implementing secure data transfer protocols, encryption mechanisms, and obtaining necessary permissions or certifications to transfer data across international borders. It has established robust global data governance frameworks to ensure data protection, privacy, and security across its international operations. This involves the enactment of data protection policies, conducting routine audits, and investing in cutting-edge cybersecurity measures to protect user data.

Alibaba closely monitors changes in data protection and localization regulations worldwide and adjusts its strategies and operations accordingly. This proactive approach helps Alibaba stay compliant with evolving legal requirements and maintain trust with its international user base. It collaborates with local partners, governments, and regulatory authorities to navigate complex regulatory landscapes and ensure smooth operations across borders. Alibaba's dual strategy capitalizes on its strong position in the vast Chinese market while also leveraging strategic international partnerships. On the one hand, Alibaba leverages the vast Chinese domestic market, providing a robust business foundation bolstered by the strong e-commerce inclination of the Chinese population [5]. On the other hand, by fostering strategic partnerships, Alibaba can leverage local expertise and resources to address localization challenges effectively [6].

4 Solution Strategy of Multinational Companies and Global Data Governance

4.1 Build a Globally Unified Data Governance Framework

As data remains a vital transnational and cross-border asset, the lack of a clearly defined global governance strategy presents considerable obstacles to fully leveraging its potential [7]. In the current global landscape, where globalization accelerates and nations become more interconnected, the importance of data sharing grows. However, the process of global data governance is impeded by a variety of factors, including diverse and fragmented regulatory frameworks, issues of private ownership, conflicting incentives, and rapid technological advancements driven by data.

To tackle these obstacles, there is a pressing demand for a cohesive worldwide framework for governing data that encompasses a range of disciplines including data management, ethics, and protection. This framework should bridge the gap between policy and practice, facilitating the seamless flow and sharing of information across borders. It should foster cooperation and coherence in global data interactions, thus enabling countries and organizations to navigate the complexities of international data exchange more effectively.

Achieving this requires collaboration among a broad spectrum of stakeholders, including governments, multinational corporations, multilateral organizations, and grassroots data initiatives. These groups must work together to agree on a common set of principles that guide the ethical and equitable use of data, ensuring that practices promote transparency, accountability, and inclusivity across different regions and cultures. They must also develop structured protocols for decision-making within the framework to enhance consistency and fairness in handling data. Furthermore, it is crucial to establish effective mechanisms to enforce these decisions and manage compliance with established guidelines and standards, ensuring the framework is actionable and impactful.

4.2 Strengthen Data Security and Privacy Protection

Enhancing the cross-border flow of data can generate significant economic value globally, but it also brings substantial security risks and potential privacy breaches. This requires governments, data operators, and data owners to implement regulations that ensure data flows are safe and orderly. After decades of building a system of data security regulatory rules, the EU has formed a relatively strict, perfect and multi-layered system of data security regulatory rules led by the GDPR, and has set up corresponding regulatory agencies within the framework of the rules, building up an operational mechanism of data protection agencies covering the whole territory and member states at both levels. The GDPR mandates that data must be "processed lawfully," initially prohibiting the processing of personal data unless a lawful condition is met. Article 6 of the GDPR delineates lawful conditions, encompassing individual consent, contractual necessity, adherence to legal obligations, protection of vital interests, tasks in the public interest, or the "legitimate interest" of the data controller.

Nevertheless, this legitimate interest should not supersede the interests or fundamental rights and freedoms of the data subject, particularly when the data subject is a minor [8].

The fundamental tenets of the GDPR are quickly becoming a universal benchmark for data protection. Embracing a unified GDPR-compliant standard enables companies to avoid the expense of maintaining multiple privacy policies. For instance, Microsoft is expanding GDPR safeguards to encompass all data subjects globally. Nations worldwide are revising their data privacy legislation to harmonize with the EU's robust data protection and privacy shield framework. On the one hand, countries and governments should make reference to the requirements of the GDPR or formulate data regulatory regimes that are in line with their own national circumstances to legally and reasonably regulate and control the data flows of multinational enterprises. On the other hand, multinational enterprises should comply with the relevant rules, strictly protect users' privacy and personal information, and realize the safe and effective flow of cross-border data.

4.3 Promote Cooperation and Exchange on Cross-border Data Flows

In the digital era, cross-border data transfers play a vital role in advancing national economies and raising living standards, especially in developing nations. The substantial surge in data exchange now exceeds the movement of physical goods or services. [9]. Given this context, it's crucial for governments to not only regulate these data flows within their jurisdictions but also to foster international cooperation and exchange to optimize the benefits of global data movements.

Unlike physical goods or services, data does not exhibit scarcity [10]. It is sharable, reusable, and non-depletable [11]. The value of data increases with its volume and diversity, as well as with the number of contributors and users accessing it. This characteristic, known as network effects, suggests that data becomes more valuable as it is accessed and used more frequently. The inherently low cost of data flow presents a theoretical possibility for any country to exchange data with others, facilitating economic cooperation and integration globally.

International data transfers offer the potential to greatly enhance national economies and elevate living standards in developing countries by leveraging global expertise and incorporating these nations into the global economic system [12]. According to research conducted by the OECD in 2020, the involvement of emerging economies in the global value chain, facilitated by cross-border data transfers, has led to higher local wages and stimulated investment in local infrastructure, machinery, and equipment. This trend persisted despite a decrease in the contribution of local intangible assets [13]. Therefore, cooperation and exchange of data flows should be promoted among countries, among enterprises and between countries and enterprises on the premise of guaranteeing data security and personal information security, so as to promote world economic exchange and development as well as diversity.

5 Conclusion

In this current digital information age, the growth of cross-border data flows has outpaced the growth of the movement of goods, services and people, and has become a very significant driver of world economic growth. As economic exchanges between countries increase, so does the flow of data. However, in this process, a number of problems have arisen, such as legal and policy constraints on the flow of data, threats to the security of data and privacy breaches, conflicts between data sovereignty and globalization strategies, and issues of trust and cooperation in the international business environment. By studying some typical cases of multinational enterprises, we propose strategies to address these problems and promote healthier cross-border data flows: first, to build a globally unified data governance framework, second, to strengthen data security and privacy protection, and third, to promote cooperation and exchange in cross-border flows.

The significance of cross-border data in bolstering international trade, fostering transnational scientific and technological collaboration, and facilitating the exchange of data resources is increasingly evident. Promoting cross-border data transfers has emerged as a crucial approach to enhancing the quality of digital economic growth and ensuring global connectivity. Concurrently, cross-border data flows serve as a pivotal factor for nations seeking to capitalize on the opportunities presented by the global digital economic landscape. Studying cross-border data flows can facilitate both data and economic exchanges among countries, thereby advancing the evolution of globalization strategies.

References

1. Jacqueline Kuzio¹, Mohammad Ahmadi, Kyoung-Cheol Kim, Michael R. Migaud, Yi-Fan Wang and Justin Bullock.: Building better global data governance. *Data & Policy* (2022), 4: e25.
2. Nigel Cory.: Cross-border data flows:Where Are the Barriers, and what do they cost?. *Information technology & Innovation foundation* (2017), 5.
3. Diane E Smith.: Governing data and data for governance: the everyday practice of Indigenous sovereignty. *Indigenous Data Sovereignty* (2016).
4. Tengjian Zou¹, Gokhan Ertug², Ilya R. P. Cuypers³, Donald L. Ferrin.: Trust across borders: a review of the research on interorganizational trust in international business. *Journal of International Business Studies* (2023) 54:1379–1401.
5. Mario Glowik.: Case study Alibaba Group: A successful Chinese and international digital business giant?. *Global Strategy in the Service Industries* (pp.96-105) (2017), 4.
6. Sara Marcucci¹, Natalia González Alarcón¹, Stefaan G. Verhulst^{1,2,3,4,5}, Elena Wüllhorst.: Informing the Global Data Future: Benchmarking Data Governance Frameworks. *Data & Policy* (2023), 5: e30.
7. Nigel Cory.: Cross-border data flows:Where Are the Barriers, and what do they cost?. *Information technology & Innovation foundation* (2017), 5.
8. A. Michael Fromkin, Phillip J. Arencibia, P. Zak Colangelo-Trenner.: ARTICLE: SAFETY AS PRIVACY, 64 *Ariz. L. Rev.* 921, 923

9. Macmillan Keck, Seharish Gillani, Ahmed Dermish, Jeremiah Grossman, Friederike Rühmann.: The role of cross-border data flows in the digital economy. UNCDF(2022),7.
10. James Heskett. What Happens When the Economics of Scarcity Meets the Economics of Abundance?. Working Knowledge (Harvard Business School, 4 Aug 2006).
11. United Nations Conference on Trade and Development (UNCTAD), Cross-border data flows and development: For whom the data flow, Digital Economy Report 2021, Box 1.1 (2021),6.
12. Joshua Meltzer & Peter Lovelock, Regulating for a digital economy:Understanding the importance of cross-border data flows in Asia, Global Economy & Development Working Paper 113 (2018),5.
13. Ali Alsamawi et al., Returns to intangible capital in global value chains: New evidence on trends and policy determinants, supra, §4.2 at 24-26.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

