Asian Social Science; Vol. 20, No. 2; 2024
ISSN 1911-2017 E-ISSN 1911-2025
Published by Canadian Center of Science and Education

Cross-Border Data Forensics: Challenges and Strategies in the Belt and Road Initiative Digital Era

Zhuan Zuo[1]

[1] School of Law and Politics, Lingnan Normal University, Zhanjiang, China

Correspondence: Zhuan Zuo, School of Law and Politics, Lingnan Normal University, 29 Cunjin Road, Zhanjiang, Guangdong Province, 524048, China. E-mail: zuozhuan@lingnan.edu.cn

Received: February 2, 2024 Accepted: February 18, 2024 Online Published: March 31, 2024

doi:10.5539/ass.v20n2p49 URL: https://doi.org/10.5539/ass.v20n2p49

Abstract

Cross-border data forensics in the era of the Belt and Road Initiative (BRI) are facing increased complexity. Multinational enterprises are encountering legal and technical challenges due to the fragmentation of global data regulations. The different data protection standards in major jurisdictions such as the European Union, China and the United States have created varying approaches to data privacy, national security, and cross-border data flow management. A study was conducted to explore the intricate framework of traditional Mutual Legal Assistance (MLA) in criminal cases. It highlights the inefficiency of cross-border data forensics and proposes reform proposals to strengthen international data-sharing cooperation. The study suggests that data localization is an effective alternative, but developing digital forensics standards in line with the goals of the Belt and Road Initiative would be a better option. To achieve this, a comprehensive regulatory framework needs to be established that balances national security, personal privacy and international cooperation in data exchange. The framework should emphasize that cross-border data management needs to coordinate and integrate technical, legal and business considerations.

Keywords: Cross-border data, Mutual Legal Assistance, Digital Evidence, Belt and Road Initiative

1. Introduction

The Internet marks a significant milestone in human society's advancement, symbolizing the transition into the information age (CHINA SCIO, 2022). Within this framework, the Belt and Road Initiative (BRI) emerges as a crucial component of the global trend towards digitalization. This initiative aims to enhance connectivity among nations along its route through infrastructure development, trade collaboration, and cultural exchange. In the era of the digital economy and the Internet, the BRI offers participating countries numerous opportunities for digital collaboration and entrepreneurial ventures.

Multinational enterprises operating in countries along the BRI route have the chance to implement their globalization strategies by leveraging digital technology and internet platforms. This enables them to expand their presence in international markets conveniently. Through digital channels, these enterprises can quickly penetrate the markets of BRI countries, facilitating immediate digital interactions with local consumers, suppliers, and partners. This phenomenon significantly boosts economic collaboration and information exchange among these nations. Furthermore, the BRI indicates that digital content will play a more substantial role in the industries of countries situated along the route.

The shift from traditional paper-based information to electronic data, and from traditional monetary transactions to digital currencies and electronic payments, are digitalization trends that will continue to be promoted and widely adopted in regions along the BRI. Additionally, the emergence of new technologies in the digital economy, such as blockchain, the Internet of Things (IoT), and cloud technology, will provide further opportunities for business model innovation and industrial advancement in countries along the BRI.

However, the process of digitization within the context of cross-border collaboration along the BRI also introduces various challenges. These challenges include the complex nature of digital evidence in forensic investigations, the need to consider privacy and data protection regulations, and the necessity to prevent and combat transnational crimes. Therefore, it is crucial for countries along the BRI to enhance collaboration in law, ethics, and standardization to foster the sustainable growth of the digital economy and effectively address the

associated challenges. The BRI serves not only as a platform for economic collaboration but also as a significant context for corporate compliance and advancement in the era of digital globalization. With these digital advancements under the BRI in mind, the discussion moves towards the fragmentation of global data regulations and its implications for multinational enterprises.

2. The Fragmentation of Global Data Regulations

Global data regulations' fragmentation refers to the diverse array of regulations and standards concerning data protection and privacy formulated and enforced by different countries. These regulations vary due to factors such as cultural norms, values, national security interests, and legal systems, presenting significant challenges for businesses engaged in cross-border operations, especially in relation to cross-border data flows, privacy protection, compliance, and international enforcement cooperation.

Enterprises must develop adaptable and comprehensive strategies to conform to the regulatory demands of diverse countries and regions. It is imperative for these enterprises to ensure that they operate within the confines of the law, maintain a high level of security, and adhere to global regulations. This necessity becomes particularly acute given the varied and sometimes conflicting nature of data protection laws across different jurisdictions, each influenced by its unique socio-political and legal context.

Navigating this complex regulatory landscape requires a nuanced understanding of local regulations in each country, as well as a robust compliance framework that can adapt to these varying requirements. This challenge is exacerbated by the dynamic nature of digital technology and the rapid evolution of data protection norms globally. For businesses operating in the digital economy, staying ahead of these regulatory changes and ensuring compliance is not just a legal necessity but also a strategic imperative to maintain trust, reputation, and competitive advantage.

2.1 EU's Most Rigorous Data Regulation Law

To further explore the intricacies of data governance, this analysis focuses on the European Union's General Data Protection Regulation (GDPR), illustrating a prominent instance of stringent data privacy regulation. The European Union's GDPR is an extensive and all-encompassing regulatory framework that pertains to enterprises and data processors operating within the European Economic Area, affecting a total of 30 countries or regions, each characterized by its distinct cultures, objectives, and requirements (Hilliard, 2020). The GDPR enforces a set of rigorous regulations regarding the processing, transfer, and storage of personal data, covering various aspects such as the rights of data subjects, the principle of transparency, and specific provisions pertaining to cross-border data transfers.

The implementation of the GDPR is widely regarded as a significant milestone in safeguarding and governing personal data, offering an unparalleled degree of protection (Kong, 2019). This has had a considerable impact on multinational corporations, compelling them to adapt their initial privacy policies in order to adhere to the regulations set forth by the GDPR. Compliance with the GDPR is crucial not only for their operations within the European Economic Area but also as a benchmark for global data protection strategies. The GDPR's influence extends beyond Europe, setting a high standard for data privacy that may serve as a reference point for nations developing or revising their own data protection regulations. This interaction between the GDPR and global data governance frameworks exemplifies the complexities and interdependencies in global data regulation, underscoring the need for multinational corporations to maintain a versatile and informed approach to data privacy and compliance.

2.2 The Chinese Government Exercises Control Over the Exit of Data

In analyzing China's data protection legislation, particularly the Personal Information Protection Law (PIPL), it's crucial to contrast it with the European Union's regulatory framework. China's PIPL imposes stringent restrictions on the export of corporate data, especially for larger companies. This law necessitates retaining personal data collected within China, presenting unique challenges for multinational corporations. When transferring personal data to offshore organizations, enterprises are required to disclose pertinent information about the offshore entity. This includes revealing the identity of the recipient, the intended purpose and method of data utilization, and obtaining explicit consent from the individual concerned. This scenario underscores the importance of understanding the nuances of China's data protection framework, especially in comparison to that of the European Union, to navigate the complexities faced by multinational corporations operating in diverse legal environments.

2.3 The United States (U.S.) Expanding Extraterritorial Data Access Rights

Shifting the geographical focus to the United States, this section provides an analytical examination of the

CLOUD Act's influence on the jurisdictional reach concerning data access rights beyond national borders.

The CLOUD Act, also known as the Clarifying Lawful Extraterritorial Use of Data Act, was enacted and implemented in March 2018. The primary objective of this initiative is to facilitate law enforcement agencies in legally obtaining access to data that is stored in offshore locations. The Act provides U.S. law enforcement agencies with legal authority to obtain data from cloud service providers located outside the United States, irrespective of the identity or characteristics of the data owner. Nevertheless, this gives rise to apprehensions regarding the protection of data privacy for individuals who are not citizens of the United States.

The CLOUD Act introduces protocols and obligations concerning data storage and access in order to uphold legal, privacy, and compliance standards in the realm of data privacy and compliance. Cloud service providers may be required to comply with these regulations to ensure the protection of user data privacy and to adhere to the legal requirements of the United States and other jurisdictions. The objective of the bill is to strengthen collaboration in international law enforcement by enabling the United States government to establish bilateral agreements with partner nations, thereby enhancing the ability to obtain cross-border data. Although this process entails a certain level of international data exchange, it is imperative that it is executed in accordance with the legal framework.

Notably, companies based in the United States that are bound by the GDPR must adhere to both U.S. legislation and, potentially, the data protection regulations of other countries (Klar, 2020). What is evident is that the existing execution of the GDPR is hindered by the constraints of a truly cooperative European culture in the domain of safeguarding data. To this day, the GDPR has not completely accomplished the emancipation of data protection from the influence of national idiosyncrasies and policies (Gentile & Lynskey, 2022).

2.4 New Trends in Extraterritorial Data Sharing

In addition, it is noteworthy that the United States and the United Kingdom have made plans to implement the U.S.-U.K. Agreement on Access to Data, which was officially signed in 2019, on October 3, 2022 (Home Office, 2022). This bilateral CLOUD Act agreement, being the first of its kind, lays the groundwork for a departure from the conventional Mutual Legal Assistance (MLA) (Galbraith, 2020) and initiates the implementation of this departure. The impact of the agreement, however, exhibits a greater level of nuance. There exists a degree of ambiguity surrounding the enhancement of privileges for specific individuals, coupled with the simultaneous curtailment of rights for others, particularly in cases involving individuals from foreign nations.

Legislatures in multiple countries have acknowledged the antiquated nature of the law, particularly the legislation pertaining to areas such as data protection. Under this prevailing trend, various countries and regions have exhibited distinctive legal attributes. The EU region, for instance, places significant emphasis on the respect and safeguarding of personal privacy through the implementation of more stringent regulations aimed at protecting personal data. China's data regulations prioritize national security and underscore the significance of data security. In addition, the United States places emphasis on asserting national jurisdiction in order to safeguard personal information. The organization has initiated active collaboration with allied nations to facilitate access to cross-border data and foster the advancement of international law enforcement cooperation. In the context of the BRI, multinational enterprises will face unprecedented challenges regarding data due to the diverse data regulations in different countries and regions.

3. Legal Framework for Cross-Border Data Sharing

Transitioning from an analysis of individual nation-state regulations, this section shifts focus to the intricate complexities and challenges inherent in MLA mechanisms, particularly within the sphere of transnational data forensics. Under the BRI, the issue of direct access to offshore data raises significant legal concerns that have the potential to impact the sovereignty of other nations and give rise to interstate disputes and conflicts. Therefore, it is imperative to thoroughly examine and address this matter from a legal standpoint. With the progress of the BRI and the presence of diverse legal systems and regulations among the participating nations, the acquisition of cross-border data has become subject to a more intricate legal landscape. This necessitates international legal negotiations and mediation to guarantee the legality and adherence of data access, while also preventing the occurrence of unwarranted legal liabilities.

On the contrary, the act of accessing personal data can potentially violate an individual's fundamental right to privacy and the safeguarding of their personal information. Given the variations in legal frameworks safeguarding personal privacy across different countries, it is imperative to conduct a thorough evaluation of compliance and regulatory measures when accessing data beyond national borders. This assessment is necessary to uphold individual rights, protect personal information, and mitigate potential legal liabilities associated with

data transfer. The task of achieving a balance between data flows and privacy safeguards is particularly significant, necessitating international collaboration to establish uniform privacy protection standards.

Legal and normative inconsistencies pose a significant challenge, as various countries have established distinct legal frameworks pertaining to data access and sharing. Addressing this issue necessitates engaging in cross-border consultations to establish shared norms for data access. This will ensure that data flows in BRI cooperation align with the fundamental principles of each country's legal framework, minimize regulatory conflicts and normative inconsistencies, and facilitate the smooth and regulated exchange of cross-border data.

3.1 Mutual Legal Assistance in the Context of Cross-Border Electronic Evidence

Given the increasing economic interdependence among nations participating in the BRI, it is possible for illicit activities to thrive unnoticed within this framework of cross-border cooperation. The acquisition of digital evidence in cross-border crimes involving enterprises presents new challenges and opportunities for international criminal mutual legal assistance, thanks to the BRI. Traditional international criminal mutual legal assistance continues to serve as the primary mechanism for cooperation, however, the context of the BRI has introduced increased complexity in terms of coordination and collaboration.

When it comes to acquiring evidence related to transnational criminal activities involving corporations, the primary method is through traditional international criminal mutual legal assistance. A formal request for MLA in criminal matters is typically initiated by judicial or law enforcement authorities and directed to the central agency of the requesting country, commonly the Ministry of Justice. The request is forwarded by the central agency of the country to the central agency of the designated country, as well as to the relevant law enforcement agencies, for review. This review process ensures compliance with the domestic law of the country and assesses the content of the request for mutual legal assistance. The specific enterprise is then required to cooperate and provide the corresponding evidence based on the outcome of this review.

3.2 Participant (Subject) Characteristics

Various countries and regions along the BRI possess distinct legal systems and judicial frameworks, necessitating increased consultation and coordination efforts when addressing international criminal mutual legal assistance requests. When addressing the evidentiary aspects of crimes perpetrated by multinational corporations, it is imperative to foster enhanced collaboration among nations in order to facilitate the seamless exchange of information and the effective prosecution of offenders. Furthermore, it is imperative to take into account the variations in the digital regulatory landscape among countries along the BRI. Various nations may employ distinct regulatory frameworks pertaining to digital information, thereby presenting potential legal obstacles in the realm of obtaining and analyzing digital evidence.

The advent of digital innovations has introduced innovative communication technologies that have significantly influenced the conventional domain of mutual legal assistance in criminal matters. These advancements have not only posed challenges in adapting the original methods of obtaining evidence for mutual legal assistance to the present circumstances but have also raised legal concerns regarding the allocation of jurisdictions to evidence, particularly in relation to cloud computing. It is a source of frustration to acknowledge that the predominant method for acquiring digital evidence in foreign jurisdictions remains the traditional and "outdated" mutual legal assistance in criminal matters. This is particularly concerning given the increasing prevalence of cloud technology, which has resulted in the storage of significant amounts of metadata in the cloud. The physical location of this data is often unknown or uncertain, making it difficult or even impossible to pursue a request for mutual legal assistance in criminal matters as a viable option (Maillart, 2019).

3.3 Sampling Mutual Legal Assistance Procedures

The availability of evidence pertaining to crimes that occurred within national boundaries just a few years ago has significantly increased due to the emergence of digital virtual carriers in cloud services and electronic data. The ubiquity and intangibility of cloud data pose significant challenges to the process of mutual legal assistance between jurisdictions. The metaphorical comparison of cloud data to clouds in the sky highlights the complex nature of this issue (Krishnamurthy, 2016). If justice officials lack knowledge regarding the storage location of the required data, they will inevitably face challenges in making a request for mutual legal assistance in criminal matters, as they will be unaware of the appropriate country to approach. Nevertheless, with the increasing migration of data to cloud service platforms, the inherent tension and conflict between the intricate and convoluted procedures of cross-border judicial co-operation and the pressing need to acquire digital evidence are becoming more evident. The Microsoft Ireland case has prominently highlighted the challenge of cross-jurisdictional law enforcement in global jurisprudence. However, underlying this case is the recognition

that cross-border electronic data forensics, which have not kept pace with rapid advancements in digital technology, are rendered ineffective and constrained by the traditional system of international judicial assistance in criminal matters.

4. Judicial Cases of Cross-Border Data Forensics in Different Jurisdictions

The significance of cross-border data access regulation on companies has gained prominence within the framework of the BRI. As the BRI cooperation continues to advance, companies are expected to engage in more frequent data exchange during cross-border collaborations. However, the implementation of stricter regulations may pose additional challenges to this process. In addition to the aforementioned factors, variations in data regulations across different participating countries can lead to companies facing more complex and diverse compliance requirements, thereby intensifying the challenges associated with regulatory compliance. Regulatory uncertainty can potentially exert a detrimental influence on the strategic planning and execution of BRI cooperation, thereby impeding companies' market entry and hindering their business expansion in the countries situated along the route. Certain multinational corporations have already acknowledged the significance of regulations pertaining to cross-border data access. The regulatory stances adopted by various countries or regions with regard to cross-border data will significantly shape the ultimate outcome of the situation.

4.1 Twist: Microsoft Ireland Data Case

One of the most significant cases that has had a profound influence on cross-border data forensics in recent years is Microsoft Corp. v. United States，829 F.3d 197 (2d Cir. 2016). This case arose from the recognition that the process of international criminal judicial assistance is excessively lengthy and inefficient, resulting in several months of waiting time. Consequently, the U.S. judiciary has been compelled to explore alternative means of obtaining the necessary evidence for the investigation of the case.

In 2013, the two parties engaged in their initial debate regarding the legitimacy of the authorization obtained under U.S. law. The Stored Communications Act pertains to the storage of data. The two parties initially engaged in a dispute in 2013 regarding the validity of the authorization acquired under the jurisdiction of the United States. The application of the Stored Communications Act extends to data that is stored on servers located in Ireland. The U.S. Department of Justice sought to circumvent direct access to the data via the MLA process, with the aim of saving a substantial amount of time. Microsoft, in response to the U.S. Department of Justice, rejected their claims by arguing that the Stored Communications Act was not applicable to data stored outside of the United States. Following the directives of a magistrate judge and district court, Microsoft was instructed to adhere to the request made by the Department of Justice. However, the U.S. Federal Second Circuit subsequently overturned this order. The rationale behind this decision was that the order was not meant to have jurisdiction beyond national borders. Additionally, the primary objective of the Stored Communications Act, which safeguards the confidentiality of users' electronic communications, does not allow for extraterritorial enforcement (Noonan, 2017). The focal point of the case under discussion revolved around the capacity of law enforcement officials in the United States to initiate a formal solicitation for criminal judicial assistance. This request was made with the intention of acquiring crucial evidence required for the ongoing investigation.

Microsoft's stance, which asserts that the United States government has a responsibility to seek the necessary data via the MLA in criminal matters treaty with Ireland, in order to avoid potential violation of international law, aligns with Ireland's position. The slow and inefficient process of obtaining relevant evidence through MLA in criminal matters has prompted the U.S. Department of Justice to seek alternative methods for obtaining the necessary data, bypassing the MLA process (Hill, 2015). The failure of the Second Circuit to overturn the order would potentially enable the United States government to infringe upon the sovereignty of other nations, disregarding their respective legal frameworks. More broadly, granting the government direct access to extraterritorial digital evidence would not only contradict the established legal precedent set by the Second Circuit, but it would also unilaterally undermine the effectiveness of the MLA in criminal matters treaties that have been ratified by the U.S. Senate. This action would have significant implications for the MLA system that has been carefully established. Despite the current challenges faced by Mutual Legal Assistance in criminal matters, numerous potential enhancements have been suggested, rendering the dismissal of its effectiveness entirely unwarranted.

4.2 Reforming Mutual Legal Assistance in Criminal Matters: Balancing Privacy and Efficiency

The reform of the MLA in criminal matters system should prioritize the protection of due process, privacy rights of individuals, and the principles of international comity when collecting or providing extraterritorial evidence. Such reforms should also take into account the requirements of the executive and legislative branches of national governments, providing them with adequate time to deliberate on pertinent foreign and domestic policy matters

(InternetLab 2018). Nevertheless, the reform of the MLA in criminal matters system alone will not address the issues presented by the Microsoft case. The MLA in criminal matters system serves as a formal mechanism through which a government can request data that falls under the jurisdiction of another sovereign state. One must address a fundamental question: under what conditions and at what times can a sovereign state exercise legal authority over data, even if it is physically situated beyond its borders? If the sole purpose of consolidating data control is to facilitate MLA formatting, then the proposed MLA reform can be considered an inadequate solution that fails to effectively address the inherent mobility and manipulability of electronic data (Daskal, 2015). The issue at hand is being addressed through the enactment of The Clarifying Lawful Use of Overseas Data Act in the United States. The aforementioned provision offers a means for foreign governments to circumvent the MLA in criminal matters system when conducting investigations into severe criminal offenses. This is achieved by enabling them to directly request data from service providers based in the United States, under the terms of an administrative agreement between the foreign government and the United States. However, it is important to note that such requests are subject to various procedural and substantive conditions. The approval of the bill, however, elicited disappointment among numerous data privacy organizations (Daskal, 2018). The Clarifying Overseas Data Access Act was included in a comprehensive government spending bill consisting of 2,232 pages. Remarkably, Congress forwarded the legislation to committee without conducting a thorough review or organizing any hearings on its content (Edmonds, 2018). This behavior aligns with the common practice among U.S. politicians to seize any opportunity to increase their authority, which partially addresses the challenges faced by law enforcement agencies. Under the BRI led by China, it is inevitable that the United States' approach will not be replicated. China is willing to embrace an equal consultation and mutually beneficial approach in order to foster relevant cooperation.

4.3 The Intersection of Tradition and Radicalization

When courts are confronted with the task of applying existing laws to emerging technologies, they are presented with a dilemma. They can either treat these new technologies as they would any other subject matter, or they can acknowledge the distinctive characteristics of these technologies and contemplate modifying the application of current laws accordingly (Harvard Law Review Association, 2016). Confronted with the clash between the MLA system and emerging technologies, both the U.S. Federal Second Circuit and the Supreme Court of the U.K. opted for the former. In the legal matter of Kellogg Brown Root Inc. v. Serious Fraud Office (SFO), the SFO exercised its investigative authority as granted by the Criminal Justice Act 1987 to request the submission of pertinent evidentiary material from the parent company of KBR Inc. in the United States (Supreme Court UK, 2021）. It is important to note that KBR Inc. does not possess a physical establishment or engage in any relevant business activities within the United Kingdom. However, KBR Ltd., a subsidiary of KBR Inc., maintains significant business operations within the UK. The decision made by the UK Supreme Court to prohibit unilateral cross-border evidence collection serves as a clear demonstration of the UK's stance against extraterritoriality. It reflects the belief that law enforcement agencies should acquire overseas evidence through collaborative mechanisms, such as mutual legal assistance in criminal matters (Cochrane, 2022).

In Brazil, a country situated along the BRI, a comparable incident took place, albeit with a distinct outcome compared to the approach adopted by the UK and the US. In this instance, the Brazilian authorities apprehended the vice president of Facebook's Latin America division. Brazilian law enforcement authorities have reported that Diego Dzodan, an Argentinean citizen, persistently declined to adhere to judicial directives mandating the surrender of data pertinent to a criminal inquiry involving drug trafficking (BBC News, 2016). As evident from the aforementioned, variations in regulations pertaining to cross-border data access across different countries and cultures can result in divergent consequences. In order to ensure compliance with cross-border data flows and cooperation, companies operating within the BRI must possess a comprehensive understanding of and adhere to national data protection regulations. Furthermore, this phenomenon compels organizations to formulate comprehensive and flexible approaches towards data management and privacy safeguarding in order to comply with the diverse legal obligations imposed by various countries and regions.

5. Strategy for Cross-Border Data Response in the Belt and Road Initiative

While there are many administrative and procedural problems associated with cross-border access to digital evidence through mutual legal assistance in criminal matters, a complete abandonment of the entire mutual legal assistance system is highly undesirable and more tailored solutions or alternatives should be developed to address the root causes of its existence.

5.1 Enhancing International Law Enforcement Cooperation

Problems associated with the MLA system are frequently characterized as administrative procedural issues, often

synonymous with delays, complexity, bureaucratic inefficiency, and similar challenges that are inherent to the overall global framework of governmental operations. The reform of the MLA system can be more effectively accomplished through the implementation of simplification measures, digitization efforts, specialized training for staff members, and the allocation of additional resources (Abraha, 2021). The current state of the office responsible for handling MLA requests indicates a clear inadequacy in terms of staff and resources. To address this issue, it is recommended to either assign additional staff or allocate staff from the judiciary to fulfill the necessary duties. Furthermore, the MLA system has encountered significant challenges due to networking issues. To improve the efficiency of the process, it is suggested to implement online platforms, such as the development of a unified e-form and an online submission platform. These measures can greatly enhance the effectiveness of the system. In addition, optimizing the number of steps involved in the MLA request process (Woods, 2015) and reducing the required materials and procedures for simple MLA requests can streamline the overall process. Lastly, simplifying the process of providing information or evidence to the requesting State is crucial. In many cases, the MLA request has already been accepted and the relevant content has been provided by the judicial authorities. However, there are still numerous cumber-some procedures that need to be followed before the information or evidence is provided. The information is furnished to the State making the request, resulting in a significant reduction in the required processing time for said State. There exist numerous intricate procedures that significantly impede the expeditious nature of the MLA process. Simultaneously, the international MLA framework in criminal matters must also take into account the concept of extraterritoriality. The recent ruling by the UK Supreme Court on KBR Inc. serves as a testament to the prevailing support for the MLA process, particularly within the United Kingdom.

5.2 Self-Assessment Conducted by Multinational Enterprises

Problem Technological advancements, in conjunction with legal delays, particularly in the realm of cloud computing and encryption technologies, are poised to render the existing legal frameworks of numerous BRI countries outdated in the near future. Therefore, achieving a harmonious equilibrium between ensuring data security and protecting user privacy within a law enforcement context necessitates the prompt re-vision of oversight models and authorization systems in BRI countries. This revision aims to enhance the alignment of interests among governments, technology companies, and individual consumers (Shah, 2015). There exists a partial alternative to mutual legal assistance in criminal matters known as remote digital forensics. In this approach, companies have the autonomy to determine their response to international user data requests and decide whether or not to provide non-content information, even in the absence of an MLA request. The existence of loopholes in the definition of "governmental entity" allows companies to legally provide non-content information to foreign governments. Google, as an illustration, acknowledges the possibility of offering non-content to users outside of the United States. A request can be submitted to them without the necessity of depending on mutual legal assistance in criminal matters treaty, provided that it aligns with international norms, U.S. law, Google's policies, and the laws of the requesting country or territory (Westmoreland, 2015). This proposition may appear to be an optimal resolution; however, governments are likely to express unease with such conduct due to its pre-dominantly unregulated nature. Furthermore, the involvement of businesses in such activities would subject them to liabilities that are typically the purview of the Ministry of Justice or other public authorities, a situation that is highly undesirable (De Busser, 2018). On one hand, if the legislation is excessively stringent, this approach deviates from its initial intent. On the contrary, when companies are granted autonomy by the law, there is a possibility that they may eventually find themselves compelled to make concessions to other governments in order to obtain certain benefits. Consequently, this situation can lead to an increased vulnerability in terms of information security. Nevertheless, it is indisputable that this approach can effectively address certain challenges encountered in the field of criminal justice assistance, as it allows for the partial resolution of less significant data-related issues.

5.3 Localized Data Storage Is Feasible But Limited

The challenge of conducting cross-border forensics on electronic data necessitates enhancing the expertise in digital forensics. Additionally, it is crucial to foster ongoing collaboration among law enforcement agencies, justice officials, and policymakers. It is recommended to proactively take initiatives in order to accelerate these frequently time-consuming procedures (Berghs et al., 2018). Additionally, as a potential alternative, nations situated along the BRI are contemplating or have already enacted legislation pertaining to data localization. Providers who have the ability to offer their services within a specific country are required to retain the content and associated data (or duplicates thereof) of users who are residents of that country. This is necessary in order to facilitate the generation of information when presented with a legal request from the domestic authorities.

Data localization further exposes individuals residing in nations with insufficient human rights standards to

potential threats concerning the confidentiality and safeguarding of user data (Gidari, 2016). More broadly, the challenges presented by the existing criminal justice assistance system in facilitating the exchange of evidence between different jurisdictions can be seen as a justification for the localization of evidence. This approach could significantly influence the way globalized communications are conducted and have implications for the governance of the Internet (Cate & Dempsey, 2017). China's Cybersecurity Law and Russia's Personal Data Law, for instance, include provisions that manage offshore service providers to store domestic data within their respective borders. This approach effectively circumvents the challenge of extraterritorial requests for digital evidence and guarantees the protection of information security and privacy for their citizens. In cases where a criminal investigation involves a service provider that does not operate in China but is obligated to provide specific data information as evidence, or when data is stored using cloud technology, the option of data localization is not a viable solution. In such situations, obtaining the required content through the criminal judicial assistance process is both the most direct and the least indirect method.

5.4 The Development of Digital Forensics Standards Aligned with the Belt and Road Initiative is Essential

New data-sharing standards are being developed within the framework of the BRI cooperation initiative. Once these standards are met, the legal transfer of personal data between regions can take place. In order to guarantee the legality of data transmission, organizations may also choose to implement standardized contractual terms for the purpose of uniform data sharing. Simultaneously, to ensure the secure utilization of data, it is imperative to create a record indicating the country of origin when sharing the data. This practice enables subsequent verification and risk management. The filing for data sharing should encompass various elements, including but not limited to the use scenario, purpose of use, appropriate storage duration, and disposal procedures after utilization. These mechanisms and contractual terms establish compliance and legal frameworks that enable enterprises to conform to the data protection requirements of countries and regions along the BRI. They also ensure the lawful processing and secure transmission of data.

Transparency and cooperation issues also require attention through legal mechanisms. Lack of transparency and cooperation can potentially result in a lack of trust and challenges in fostering collaboration among nations. The implementation of transparent legal procedures and international cooperation mechanisms can contribute to enhancing predictability and fostering trust in the process of accessing data.

6. Conclusion

Considering the array of challenges and viewpoints discussed, this conclusion aims to integrate these various insights and delineate prospective pathways for further exploration and action. Under the BRI, the issue of cross-border data access presents significant technical challenges and necessitates comprehensive analysis from a jurisprudential standpoint. The clarification of the offshore data's location and the means of accessing it may encounter technical obstacles. Therefore, legal norms should establish specific procedures and standards to tackle potential technical challenges and guarantee the fairness and legality of the access process. Such regulations can play a crucial role in achieving a harmonious equilibrium among the diverse interests of national security, individual privacy, and international cooperation in the realm of data access.

In the examination of the significance of specializing in digital forensics and the necessity to enhance collaboration among law enforcement agencies, judicial bodies, and policymakers, it was underscored that the involvement of technical proficiency and the alignment of legal adherence is particularly crucial in data forensics related to BRI cooperation. Specializing in digital forensics can play a crucial role in guaranteeing the integrity and authenticity of data. Additionally, fostering strong collaboration among law enforcement agencies, judicial bodies, and policymakers is essential to ensure the accurate utilization of data in legal proceedings. Simultaneously, it is important to consider the implications that data localization laws and evidence localization may have. In the context of the multi-country cooperation encompassed by the BRI, it is imperative to establish well-defined regulations in order to prevent data localization provisions from impeding project collaboration and hindering the exchange of information. When presenting alternatives for enterprises to independently determine whether to disclose non-content information, it is important to highlight the trade-offs that enterprises encounter when balancing regulatory obligations and users' right to information. Ensuring that enterprises recognize the importance of transparent data processing in order to comply with regulations, respect users' right to privacy, and meet national regulatory requirements. Additionally, providing clear guiding principles for data flows in BRI cooperation.

In the context of the BRI, the implementation of a comprehensive regulatory framework and collaborative mechanism, which considers the technical, legal, and business aspects, will effectively facilitate the movement of cross-border data. This approach will also ensure a harmonious balance between national security, individual

privacy, and international cooperation.

References

Abraha, H. H. (2021). Law enforcement access to electronic evidence across borders: Mapping policy approaches and emerging reform initiatives. *International Journal of Law and Information Technology, 29*(2), 118-153. https://doi.org/10.1093/ijlit/eaab001

BBC News. (2016, March 1). *Brazil Facebook head arrested for refusing to share WhatsApp data.* Retrieved from https://www.bbc.com/news/world-latin-america-35690488

Berghs, S., Morrison, G. S., & Goemans-Dorny, C. (2018). Electronic Evidence: Challenges and Opportunities for Law Enforcement. In *Handling and Exchanging Electronic Evidence Across Europe* (pp. 75-123). Springer, Cham. https://doi.org/10.1007/978-3-319-74872-6_6

Cate, F. H., & Dempsey, J. X. (2017). *Bulk collection: Systematic government access to private-sector data.* Oxford University Press. https://doi.org/10.1093/oso/9780190685515.001.0001

Cochrane, T. (2020). Digital Privacy Rights and CLOUD Act Agreements. *Brooklyn Journal of International Law, 47,* 1. Retrieved from https://brooklynworks.brooklaw.edu/bjil/vol47/iss1/1

Cochrane, T. (2022). The Presumption Against Extraterritoriality, Mutual Legal Assistance, and the Future of Law Enforcement Cross-Border Evidence Collection. *The Modern Law Review, 85*(2), 526-538. https://doi.org/10.1111/1468-2230.12675

Daskal, J. (2015). The Un-Territoriality of Data. *Yale Law Journal, 125,* 326. Retrieved from https://www.yalelawjournal.org/article/the-un-territoriality-of-data

Daskal, J. (2019). Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. *Stanford Law Review, 71,* 9-11. Retrieved from https://www.stanfordlawreview.org/online/microsoft-ireland-CLOUD-act-international-lawmaking-2-0/

De Busser, E. (2018). The Digital Unfitness of Mutual Legal Assistance. *Security and Human Rights, 28*(1-4), 161-179. https://doi.org/10.1163/18750230-02801008

Edmonds, N. (2018). CLOUD Act Opens Up User Data to Foreign Governments. *Harvard Journal of Law & Technology*. Retrieved from https://jolt.law.harvard.edu/digest/cloud-act-opens-up-user-data-to-foreign-governments#:~:text=The%20Clarifying%20Lawful%20Use%20of%20Overseas%20Data%20Act,government%20will%20procure%20this%20information%20from%20private%20companies.

Gidari, A. (2016). *MLAT Reform And The 80% Solution–What's Good For Users? The Center for Internet and Society at Stanford Law School.* Retrieved from https://cyberlaw.stanford.edu/blog/2016/02/mlat-reform-and-80-solution-whats-good-users.

Galbraith, J. (2020). United States and United Kingdom sign the first bilateral agreement pursuant to the CLOUD Act, facil-itating Cross-Border Access to data. *American Journal of International Law, 114*(1), 124-128. Retrieved from https://www.jstor.org/stable/26891035

Gentile, G., & Lynskey, O. (2022). Deficient by Design? The Transnational Enforcement of the GDPR. *International & Comparative Law Quarterly, 71*(4), 799-830. https://doi.org/10.1017/S0020589322000355

Harvard Law Review Association. (2016). Privacy - Stored Communications Act — Second Circuit holds that the government cannot compel an internet service provider to produce information stored overseas. — Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016). *Harvard Law Review, 130,* 769-776. Retrieved from https://harvardlawreview.org/wp-content/uploads/2016/12/769-776-Online-Rev.pdf

Hill, J. F. (2015). Problematic alternatives: MLAT reform for the digital age. *Harvard Law School: National Security Journal,* Jan 28, Online Edition. Retrieved from https://harvardnsj.org/2015/01/28/problematic-alternatives-mlat-reform-for-the-digital-age/

Hilliard, E. (2020). The GDPR: A retrospective and prospective look at the first two years. *Berkeley Technology Law Journal, 35,* 1245. https://doi.org/10.15779/Z384J09Z3K

Home Office. (2022, July 21). *Data Access Agreement: joint statement by the United States and the UK.* Retrieved from https://www.gov.uk/government/publications/data-access-agreement-joint-statement-by-the-united-states-and-the-uk

InternetLab Law and Technology Center. (2018, January 18). Brief amicus curiae of InternetLab Law and Technology Center in support of respondent, United States v. Microsoft Corporation, No. 17–2, Supreme

Court of the United States. Retrieved from [20180118203851162_17-2 bsac Internetlab Law and Technology Center.pdf (supremecourt.gov)].

Kong, G. (2019, August 14). *Why Stricter Data Privacy Laws Would Benefit The Data Industry.* Forbes. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2019/08/14/why-stricter-data-privacy-laws-would-benefit-the-data-industry/

Klar, M. (2020). Binding effects of the European General Data Protection Regulation (GDPR) on US companies. *Hastings Science and Technology Law Journal, 11,* 101. Retrieved from https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1095&context=hastings_science_technology_law_journal

Krishnamurthy, V. (2016). Cloudy with a Conflict of Laws. *Berkman Center Research Publication, 2016*(3). Retrieved from https://cyber.harvard.edu/research/cloudywithaconflictoflaws

Maillart, J. B. (2019, March). The limits of subjective territorial jurisdiction in the context of cybercrime. *In Era Forum, 19*(3), 375-390. https://doi.org/10.1007/s12027-018-0527-2

Noonan, A. (2017, July 1). Microsoft v. United States: DOJ Petitions for Certiorari in Microsoft Ireland, Argues that Probable–Cause Warrants Require Service Providers to Supply Data Stored Overseas. *Harvard Journal of Law & Technology.* Retrieved from https://jolt.law.harvard.edu/digest/doj-petitions-for-certiorari-in-microsoft-ireland-argues-that-probable-cause-warrants-require-service-providers-to-supply-data-stored-overseas

Shah, R. (2015). Law enforcement and data privacy-a forward-looking approach. *Yale Law Journal, 125,* 543. Retrieved from https://www.yalelawjournal.org/article/law-enforcement-and-data-privacy-a-forward-looking-approach

State Council Information Office of the People's Republic of China (CHINA SCIO). (2022, November 7). *Jointly Build a Community with a Shared Future in Cyberspace.* Retrieved from https://www.chinadaily.com.cn/a/202211/07/WS63687246a3105ca1f2274748.html

Supreme Court of the United Kingdom. (2021). R (KBR, Inc) v. Director of the Serious Fraud Office ([2021] UKSC 2). *Weekly Law Reports, 2,* 335.

Woods, A. K. (2015). Data beyond borders: Mutual legal assistance in the internet era. *Global Network Initiative,* January 27, 2015. https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf

Westmoreland, K. (2015, August 12). The Global Corporate Citizen: Responding to International Law Enforcement Requests for Online User Data. *Harvard Journal of Law & Technology.* Retrieved from http://jolt.law.harvard.edu/digest/the-global-corporate-citizen-responding-to-international-law-enforcement-requests-for-online-user-data

Acknowledgments

Not applicable.

Authors contributions

Not applicable.

Funding

This research is supported by China and Belarus Philosophy and Cultural Research Center, Lingnan Normal University.

Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Canadian Center of Science and Education.

The journal's policies adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.