https://doi.org/10.37420/j.mlr.2025.010

A Transnational Perspective and Systemic Review of Cross-Border Electronic Data Forensics

Huanyu Jiang
The Law School of Shandong University, Qingdao, China
***Corresponding author, E-mail: jianghuanyu2003@163.com**

Abstract

In an era marked by increasing cybercrime and global digital interdependence, cross-border electronic data forensics has become a vital yet highly contested legal issue. This paper offers a comprehensive and comparative review of the legal frameworks, practical challenges, and evolving models governing transnational electronic data forensics. It critically analyzes international and regional instruments, including the newly adopted United Nations Convention against Cybercrime, the Budapest Convention and its Second Additional Protocol, as well as national regimes such as the European Union's European Investigation Order and the CLOUD Act in the U.S. The study contrasts the emerging "data controller" model, which emphasizes jurisdiction over service providers regardless of data location, with the traditional "data storage place" model grounded in territorial sovereignty. Highlighting legal ambiguities, operational inconsistencies, and sovereignty conflicts, it underscores the limitations of both multilateral treaties and unilateral approaches. The paper also reflects on China's potential pathway, advocating a cautious, sovereignty-respecting engagement with the "data controller" framework while emphasizing data classification and reciprocity.

Keywords

Cross-Border Forensics; Electronic Data; Data Controller Model; Data Disclosure

1 Introduction

Against the background of rampant cybercrime, there is a growing demand in the international community for the formation of uniform rules of law to regulate Cross-Border Electronic Data Forensics. On December 24, 2024, the 79th United Nations General Assembly formally adopted the United Nations Convention against Cybercrime (hereinafter referred to as "the Convention"). The Convention is the first global normative document with international law effect in the cyber field promoted by China and other developing countries, and it is an important achievement for China to take the initiative to participate in the construction of a new order for the international governance of cyberspace, and to enhance China's international influence on the governance of cyberspace. The Convention not only consolidates and innovates the rules of uniform substantive law system for the international community to combat cybercrime in a coordinated manner, but also provides an important reference for China to improve the mechanism for cross-border electronic data forensics.

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

An important motivation for improving the rules on cross-border electronic data forensics is that the traditional method of international mutual legal assistance (hereinafter referred to as "MLA") in criminal matters has so far shown many problems. For example, requests are likely to be refused by the requested State due to political factors or because they do not comply with the "principle of double criminality" in international law. In addition, this system is no longer able to cope with the practical needs of electronic and computerized evidence collection. For instance, the European Union countries always need to request the United States Department of Justice to collect electronic data through the MLA procedure, but even if the process is carried out smoothly, it generally takes about 10 months to complete. By the time the MLA request is finally executed, it is highly likely that the corresponding evidence will have already been altered, destroyed or deleted. Consequently, the international community and state governments have begun to explore new paths for cross-border electronic data forensics to be in line with realistic needs.

Although both international and domestic regulations on cross-border electronic data forensics have shown a trend of continuous improvement, their practical problems have still not been completely solved. From the point of view of existing international conventions, such as the Budapest Convention on Cybercrime (hereinafter referred to as the "Budapest Convention") and other similar conventions, even though they own a large group of States parties, since most of these countries (or regions) are located in the same geographical area, the effectiveness of such treaties is merely limited in a specific geographic scope. As for the Convention as a truly international treaty, the nature of international law determines its rules concerning cross-border electronic data forensics lack of operational standards. Additionally, these rules also witness weak implementation and monitoring mechanisms and other shortcomings. At the level of domestic law, there are significant differences in the legal systems of various countries, and the emerging "data controller" forensic model and the traditional "data storage place" model are in fierce collision, resulting in frequent conflicts between a country's data sovereignty and the jurisdiction of other countries, which will pose a serious threat to one of the basic principles of international law—the principle of state sovereignty, and also lead to further difficulties in cross-border electronic data forensics.

This article will be based on three aspects—the international conventions, regional treaties, and foreign domestic law, to demonstrate the existing rules and legislative trends, and also combined with the relevant typical cases in order to present a comprehensive view on cross-border electronic data forensics from a perspective of transnational law. Though analyzing and evaluating with an angle of the comparative law, this article hopes to provide inspiration for China's cross-border electronic data forensics legal framework.

2 International Conventions and Their Evaluation

This section will focus on the design of the rules of the Convention on cross-border electronic data forensics, i.e. on the basis of data classification, specifying the scope of application of different evidentiary measures and the manner in which they are to be applied, and provide a holistic evaluation thereof. At the same time, it will also provide a basic summary and evaluation of the relevant regimes of both the United Nations Convention against Corruption (hereinafter referred to as the "UNCAC") and the United Nations Convention against Transnational Organized Crime (hereinafter referred to as the "UNCATOC").

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

2.1 Rules Regarding Cross-border Data Forensics in the Convention and Evaluation on them

The scope of the Convention is very broad, consisting of nine chapters in addition to the preamble, namely, general provisions (Arts. 1-6), criminalization (Arts. 7-21), jurisdiction (Art. 22), procedural measures and law enforcement (Arts. 23-34), international cooperation (Arts. 35-52), preventive measures (Art. 53), technical assistance and information exchange (Arts. 54-56), mechanism of implementation (Arts. 57-58) and final provisions (Arts. 59-68). Among them, "criminalization", "procedural measures and law enforcement" and "international cooperation" are the core components, Cross-border electronic data forensics is closely related to the latter two parts, i.e. chapters IV and V of the Convention.

The provisions of chapters IV and V of the Convention are aimed at strengthening international cooperation and promoting the sharing of electronic evidence, establishing procedures and law enforcement measures that are widely applied and in line with the principle of proportionality, and creating a new mechanism for comprehensive and efficient transnational cooperation based on a system of international mutual legal assistance in criminal matters:

On the one hand, Chapter IV of the Convention provides for six forensic measures for three different types of electronic data, categorizing electronic data into subscription user information, traffic data and content data, and setting out forensic measures i.e. expedited preservation and disclosure, production order, search and seizure, real-time collection and interception for the different data types, as shown in the table below:

Table 1 Classification and its Meaning of Electronic Data under the Convention

Categories of Electronic Data	Meaning
Traffic data	Any electronic data relating to a communication by means of an information and communications technology system, generated by an information and communications technology system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service
Content data	Any electronic data, other than subscriber information or traffic data, relating to the substance of the data transferred by an information and communications technology system, including, but not limited to, images, text messages, voice messages, audio recordings and video recordings
Subscriber information	Any information that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: (i) The type of communications service used, the technical provisions related thereto and the period of service; (ii) The subscriber's identity, postal or geographical address, telephone or other access number, billing or payment information, available on the basis of the service agreement or arrangement; (iii) Any other information on the site of the installation of communications equipment, available on the basis of the service agreement or arrangement
Personal data	Any information relating to an identified or identifiable natural person

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

Table 2 Different Forensic Measures and the Scope of Data Covered by them in the Convention

Forensic Measures	Categories of Electronic Data
Expedited preservation of stored electronic data	Traffic data, Content data, Subscriber information
Partial disclosure	Traffic data
Production order	A person in its territory to submit specified electronic data in that person's possession or control that are stored in an information and communications technology system or an electronic data storage medium
	A service provider offering its services in the territory of the State Party to submit subscriber information relating to such services in that service provider's possession or control
Search and seizure of stored electronic data	All kinds of electronic data
Real-time collection	Traffic data
Interception	content data

On the other hand, Chapters IV and V of the Convention specify the limitation in application of the forensic measures, as shown in the table below:

Table 3 The Limitation of Different Forensic Measures in the Convention

Forensic Measures	Limitation in Application
Expedited preservation of stored electronic data	Application limited to the territory of a State, with international cooperation methods under the Convention required for extraterritorial data
Partial disclosure	Application limited to the territory of a State, with international cooperation methods under the Convention required for extraterritorial data
Production order	**Application to extraterritorial data is permitted**, competent authority of a State may apply directly abroad
Search and seizure of stored electronic data	Application limited to the territory of a State, with international cooperation methods under the Convention required for extraterritorial data
Real-time collection	Application limited to the territory of a State, with international cooperation methods under the Convention required for extraterritorial data
Interception	Application limited to the territory of a State, with international cooperation methods under the Convention required for extraterritorial data

As the first global normative instrument with international legal effect in the cyberspace, the Convention's practical effectiveness and institutional design are still subject to significant controversy. Firstly, as the Convention largely draws on the outdated system of the Budapest Convention, its protection of emerging digital rights and interests fails to fully reflect the complex rights and interests in today's digital economy; secondly, the Convention's exploration of simplifying international criminal judicial assistance procedures and innovating the mechanism for cross-border evidence collection is very limited, and it is still difficult to adapt to the urgent demand for rapid and efficient access to extraterritorial electronic evidence; In addition, there are significant differences between the procedural rules established by the Convention and the current legal system of China. Taking the classification standard of personal information as an example, the Convention adopts the trichotomy of subscriber information, traffic data and content data as the basis of the system, and

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

designs the corresponding framework of forensic rules accordingly. However, there are obvious differences between this classification method and the classification according to the degree of damage caused by information leakage and the importance of information established in Personal Information Protection Law of China and Data Security Technology—Rules for Data Classification and Grading, so the cross-border electronic data forensics system of the Convention may create an obstacle to convergence with China's relevant legal system.

2.2 Rules Regarding Cross-border Data Forensics in the UNCAC and UNCATOC with Evaluation on them

The United Nations Convention against Corruption (UNCAC) is the key legal framework for international cooperation against corruption, which entered into force in 2005. The United Nations Convention against Transnational Organized Crime (UNCATOC), on the other hand, entered into force in September 2003 as the first comprehensive international legal instrument adopted by the United Nations to address transnational organized crime. This part is intended to summarize and evaluate the provisions related to cross-border electronic data forensics in the two treaties.

As for the UNCAC, the term "cross-border electronic data forensics" is not directly mentioned by it, but its provisions on "mutual legal assistance", "law enforcement cooperation" and "special investigative techniques" can be used to infer the basic position of the UNCAC on cross-border electronic data forensics:

Table 4 Provisions of the UNCAC Relevant to Cross-border Electronic Data Forensics

Article	Topic	Specific Content
Article 46	Mutual legal assistance	Mutual legal assistance shall be afforded to the fullest extent possible under relevant laws in investigations, prosecutions and judicial proceedings relating to corruption offences, including the collection, search, seizure and transfer of electronic evidence
Article 48	Law enforcement cooperation	Encouraging States Parties to enhance law enforcement cooperation in cross-border investigations, including undercover operations and technical means (e.g., electronic surveillance, data tracing, etc.) to obtain electronic evidence
Article 50(1)	Special investigative techniques	Allowing States Parties to use special techniques such as electronic surveillance, informants and cross-border data access in anti-corruption cases, subject to domestic laws and the principles of international cooperation
Article 50(2)	Encouraging States Parties to conclude arrangements for using such special investigative techniques	For the purpose of investigating the offences covered by this Convention, States Parties are encouraged to conclude, when necessary, appropriate bilateral or multilateral agreements or arrangements for using such special investigative techniques in the context of cooperation at the international level

Similarly to the UNCAC, UNCATOC's content on cross-border electronic data forensics is mainly dispersed throughout this Convention's provisions, in particular in the sections dealing with extradition, mutual legal assistance, joint investigations, special investigative techniques:

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

Table 5 Provisions of the UNCATOC Relevant to Cross-border Electronic Data Forensics

Article	Topic	Specific Content
Article 16	Extradition	States Parties may cooperate on extradition on the basis of the Convention and allow electronic evidence to accompany extradition requests
Article 18	Mutual legal assistance	Mutual legal assistance shall be afforded to the fullest extent possible under relevant laws in investigations, prosecutions and judicial proceedings relating to transnational organized crimes, including the collection, search, seizure and transfer of electronic evidence, remote computer data access and extraction, and rapid preservation of electronic evidence
Article 19	Joint investigations	Encouraging States parties to establish joint investigation teams in complex cases and to share electronic evidence
Article 20	Special investigative techniques	Allowing the use of technical means such as electronic surveillance and undercover operations to obtain evidence in transnational crime investigations

As stated above, since the UNCAC and the UNCATOC are not specifically targeted at combating cybercrime, their provisions on cross-border electronic data forensics are relatively general, making it difficult to implement them in reality; at the same time, since the UNCATOC and the UNCAC were enacted more than 20 years ago, it was difficult to foresee today's distributed storage technologies (e.g., IPFS), privacy computing applications, and decentralized financial (DeFi) transaction tracking technologies. Therefore, neither of them can respond well to problems in reality.

In addition, the two conventions also have different shortcomings. For example, the electronic data forensics provisions of the UNCAC suffer from an imbalance in the guarantee of rights, as evidenced by the lack of specific standards for the application of the principle of proportionality and the lack of remedial procedures for third-party data subjects, as in the Convention; whereas, according to the United Nations Office on Drugs and Crime Report 2022, the average assistance period under the UNCATOC is 9-14 months, and 40% of the States Parties have not established specialized electronic data forensics government agencies.

It can be seen that the cross-border electronic data forensics legal frameworks of the two conventions suffer from the disadvantage of being less operational and unable to meet the rapidly evolving demand for cross-border electronic data forensics.

3 Regional Convention and its Evaluation—"Budapest Convention"

The Budapest Convention is the first comprehensive international legal document dedicated to cybercrime, formulated by the Council of Europe in 2001 and entering into force in 2004. The Convention aims to harmonize national legislation and strengthen international cooperation to combat cybercrime. This section will analyze the three aspects of the Budapest Convention, namely, "cross-border electronic data forensics by unilateral means", "public-private cooperation in cross-border electronic data forensics", and "guarantees of expeditiousness in cross-border electronic data forensics", and the legal framework for cross-border electronic data forensics under the Budapest Convention will be evaluated.

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

3.1 Cross-border Electronic Data Forensics by Unilateral Means

Unilateral cross-border forensics is the direct collection of electronic data stored overseas by competent authorities via the public Internet, bypassing the MLA in criminal matters procedures. Within the scope of European Union, unilateral cross-border forensics in most Member States is mainly carried out through the two situations in which States parties may carry out cross-border forensics without the MLA and the authorization of the other party, as provided for in Article 32 of the Budapest Convention:

Table 6 Unilateral Cross-border Forensics Mechanism under Article 32 of the Budapest Convention

Article	Requirements	Data Permitted to be Collected
Article 32(a)	Regardless of where the data is located geographically, without the authorisation of another Party	Publicly available (open source) stored computer data
Article 32(b)	The Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system, without the authorisation of another Party	Stored computer data located in another Party

As can be seen in the table above, the terminology set forth in Article 32 of the Convention is not clear, and this may lead to further confusion in its application. For example, in the Interpretative Report on the Convention on Cybercrime, issued in 2001, the framers of the Convention acknowledged that it cannot be ruled out that some States Parties may resort to unlawful means such as bribery, threats, deception, etc., against data right holders in order to ostensibly satisfy the condition of "lawful and voluntary consent" as stipulated in Article 32. The lack of clarity in terminology will inevitably lead to inconsistencies in the understanding and the application of the rules between the country that aims to collect evidence and the country where the data is stored, which will easily lead to disputes in international law and even diplomacy.

3.2 Public-private Cooperation in Cross-border Electronic Data Forensics

The Budapest Convention establishes a private subject data disclosure regime based on public-private cooperation in cross-border data forensics, and the mandatory feature of this mechanism is further enhanced by the ongoing development of the Budapest Convention.

3.2.1 The System of public-Private Cooperation in Cross-Border Evidence Collection Constructed by the Budapest Convention

Article 32 of the Budapest Convention not only demonstrates the unilateral cross-border data forensics framework under this Convention, but also provides a legal basis for public-private cooperation in cross-border data forensics, while Article 18 creates a system of "production order", i.e., it further clarifies that the investigative authorities of each Contracting Parties may request specific private subjects to provide data that may be located outside their territory under two circumstances. That is to say, it further specifies that the investigative authorities of each State party may, subject to the adaptation of domestic law, request specific private subjects to provide data that may be located outside its territory under two circumstances:

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

Table 7 Targeted Subjects and Accessible Data under Article 18 of the Budapest Convention

Targeted Subjects	Accessible Data
A person in the territory of the Party	Specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium
A service provider offering its services in the territory of the Party	Subscriber information relating to such services in that service provider's possession or control

It can be seen that the competent authorities of State Parties are authorized to request data from Internet Service Providers (hereinafter referred to as the "ISP") in their territories only in respect of "subscriber information" in their possession or control. The emphasis on "subscriber information" is due to the fact that the Budapest Convention makes a clear distinction between three types of data: "traffic data", "content data" and "subscriber information":

Table 8 Different Types of Data and their Meaning in the Budapest Convention

Categories of Data/Information	Meaning
Subscriber information (i.e., subscriber data)	Any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data
Traffic data	Any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service
Content data	The content of the communication, e.g., the meaning or intent of the communication (other than "traffic data"), the purpose or message expressed by the communication

Nevertheless, although the Budapest Convention establishes "production order" regime, there is a limitation on the scope in which it can have a coercive effect. Such compulsion is limited to the territory of the requesting State. Generally, in practice, ISPs only disclose user information in compliance with their domestic laws and corporate policies, i.e., the provision of such information is largely dependent on the unilateral action of the service provider. In summary, in the absence of clear legal regulation under the Budapest Convention, different ISPs have shown significant differences in terms of certainty, transparency, accountability and sustainability while facing data disclosure requests.

3.2.2 Enhancements to the Mandatory Disclosure Mechanisms in the "Second Additional Protocol"

As mentioned above, since the coercive effects of the Budapest Convention's data disclosure regime is rather limited, the availability of the required electronic evidence is largely dependent on the will of the service provider and is highly randomized. In response to this shortcoming, the Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (hereinafter referred to as the "the Second Additional Protocol"), signed in 2022, reflects the EU's efforts to promote

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

the burden of mandatory disclosure obligations on the ISPs. In particular, there are two mechanisms for enhancing cooperation (mandatory data disclosure in fact) between the competent authorities of one State Parties and the ISPs in the territory of another Party:

The first regime takes the form of a direct request by the competent authorities of a State Party for some types of data from ISPs in another Party. Specifically, the types of data available include "domain name registration information" under Article 6 and "subscriber information" under Article 7. The cross-border forensics procedures applicable to "domain name registration information" and "subscriber information" are, most of the time, the same, but the cross-border data disclosure procedures applicable to both remain distinctly different:

Table 9 Similarities and Differences in the Cross-border Forensics and Disclosure Procedures between "Domain Name Registration Information" and "Subscriber Information"

Similarities between "Domain Name Registration Information" and "Subscriber Information" in Cross-border Forensic Procedures	**Special Provisions for Cross-border Data Disclosure Procedures of "Subscriber Information"**
Each Party is entitled to apply such a procedure and other Parties are required to cooperate by adapting their domestic law	According to Arts. 7(2)(b), 7(5)(a)–(c), 7(9), at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, a Party may:
	with respect to orders issued to service providers in its territory–make the following declaration: " The order regarding cross-border disclosure of 'subscriber data', must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision"
Data disclosure orders issued by the competent authorities of a Party to an ISP in the territory of the other State need to be accompanied by the required detailed information, and these orders in electronic form need to be at the appropriate security level and provide the necessary guarantees of authentication	(and at any other time,) notify the Secretary General of the Council of Europe that, when an order is issued to a service provider in its territory for cross-border subscriber information disclosure, the Party requires, in every case or in identified circumstances, simultaneous notification of the order, the supplemental information and a summary of the facts related to the investigation or proceeding; require the service provider to consult the Party's authorities in identified circumstances prior to disclosure; require ISPs not to disclose data to the competent authority of another country in two specific circumstances
In the event of non-co-operation by an ISP, a requesting Party may request that the entity give a reason why it is not disclosing the information sought. The requesting Party may seek consultation with the Party in which the entity is located, with a view to determining available measures to obtain the information	reserve the right to not apply the procedure whereby the competent authorities of another Party directly request the submission of "subscriber information" from ISPs in its territory

It can be seen that the Second Additional Protocol has designed a cross-border data disclosure regime for both "domain name registration information" and "subscriber information" applicable to ISPs in the territory of the other Contracting State, but the procedures applicable to them are different, which clearly reflects the differences in the level of protection afforded by the Second Additional Protocol to the two types of data. The greater legal value of "subscriber information" as compared to "domain name registration information" necessitates stronger procedural safeguards. In conjunction with the fact that the Second Additional Protocol allows States Parties to make legal reservations to the mandatory disclosure procedures for "subscriber information", it can be further analyzed that States may tend to make stronger sovereignty claims over "subscriber information" controlled by ISPs, and to impose stricter protection requirements on the security of such data.

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

In the second regime, the competent authorities of a Party may request the authorities of another Party, which in turn directs ISPs in its territory to provide certain types of data. Specifically, such data include "subscriber information" and "traffic data". There is also a special provision, set out in Article 9, whereby the investigative authorities of a Party may, in an emergency, request the authorities of another State party to expeditiously disclose, through the 24/7 Network established by the Budapest Convention, "computer-stored data" in the possession of an ISP. The Second Additional Protocol regulates "subscriber information" and "traffic data" in a manner similar to "domain name registration information" and "subscriber information" in the first regime, i.e., the cross-border forensics procedures for subscriber information and traffic data designed by the Second Additional Protocol are mostly the same, but there are differences in the applicable procedures for cross-border data disclosure between them:

Table 10 Similarities and Differences in the Cross-border Forensics and Disclosure Procedures between "Subscriber Information" and "Traffic Data"

Similarities between "Subscriber Information" and "Traffic Data" in Cross-border Forensic Procedures	**Differences between "Subscriber Information" and "Traffic Data" in Cross-border Data Disclosure Procedures**
Each Party is entitled to apply such a procedure and other Parties are required to cooperate by adapting their domestic law	According to Article 8(6)(a)，the requested Party, from the date of receipt of all the specified information, shall make reasonable efforts to serve the service provider within forty-five days, if not sooner, and shall order a return of requested information or data no later than: (i) twenty days for subscriber information; and (ii) forty-five days for traffic data
In its request, the requesting Party shall submit the order for expedited production of subscriber information and traffic data, the supporting information and any special procedural instructions to the requested Party	According to Article 8(13), at the time of signature of the Second Additional Protocol or when depositing its instrument of ratification, acceptance, or approval, a Party may reserve the right not to apply this article to traffic data
A Party may declare at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, and at any other time, that additional supporting information is required to give effect to orders for expedited production of subscriber information and traffic data	
The requested Party shall accept requests in electronic form. It may require appropriate levels of security and authentication before accepting the request	

Although the Second Additional Protocol authorizes the competent authorities of a Party to request cross-border data disclosure from ISPs located in another party through a facilitation mechanism, it still provides different institutional designs for procedural requirements and reservation clauses that can be made for the two different types of data, namely, subscriber information and traffic data. Thus, it can be seen that the Second Additional Protocol allows a Party to provide a greater degree of protection for traffic data, thereby denying another Party's cross-border expedited data disclosure under Article 8.

Taking into account the provisions aiming to reinforce the mandatory disclosure mechanism, it can be concluded that, considering the possible claims from the Parties in terms of data sovereignty and security protection, the Second Additional Protocol builds a regulatory mechanism for cross-border data disclosure that progressively tightens from leniency to stringency based on the classification of "domain name registration information", "subscriber information" and "traffic data".

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

3.3 Guarantees of Expeditiousness in Cross-border Electronic Data Forensics

In addition to designing a data disclosure regime based on the nature and characteristics of different data and protection requirements, the Budapest Convention also formulates a series of measures to further respond to the need for expeditiousness in cross-border electronic data forensics:

Table 11 Means to Guarantee Expeditiousness in Cross-border Electronic Data Forensics in the Budapest Convention

Article	Content
Article 25	It not only emphasizes the Parties shall afford one another mutual assistance to the widest extent possible expedited means of communication in criminal cases generally, but also regulates the means of expedited communication among Parties in urgent circumstances, refusals of international cooperation, and the conditions under which bilateral assistance may be requested
Article 29	It specifies the conditions under which a Party may request the other Party to initiate expedited preservation of stored computer data, the refusal of the requested Party, and a number of corresponding procedures
Article 30	Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted
Article 31	It authorizes that a Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. In addition, it also stipulates two circumstances under which the request shall be responded to on an expedited basis

The Budapest Convention has constructed a relatively mature mechanism for expeditious cross-border electronic data forensics through a number of articles, but there are still some problems in the process of implementation: for example, the term of "refusal of international cooperation" in Article 25 may be abused, affecting the efficiency of implementation, and in the future, it may be necessary to further clarify the reasonable criteria for refusal; the same applies to the "right of the requested Party to refuse" under Article 29. Additionally, although Article 30 requires the requested party to quickly disclose traffic data when an ISP in a third country is found to be involved, and this reflects the adaptation to data mobility, the actual operation may be limited by jurisdictional conflicts or technical obstacles, and there may be a need to strengthen technical assistance and cooperation among States Parties. Moreover, Article 31 distinguishes between general and expedited response mechanisms, which is conducive to striking a balance between efficiency and procedural justice, but the response period for a "rapid response" has not been clarified, which may lead to implementation discrepancies.

3.4 Evaluation on the Budapest Convention from a Holistic Perspective

The Budapest Convention, as the first international comprehensive legal document dedicated to cybercrime, is of great significance for the harmonization of the definition and legislative framework of cybercrime and the improvement of the design of regional cross-border electronic data forensic systems. However, the deficiencies and shortcomings of the Convention should not be overlooked:

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

On the one hand, in addition to the above two situations stipulated in Article 32 of the Budapest Convention, there is no clear answer to the question of whether States Parties can carry out cross-border data forensics in other ways, such as cross-border remote searches that may be adopted by the Parties in practice, as well as the seizure, real-time monitoring and other technical investigation measures that contain potential risks of infringement in nature. In fact, the Budapest Convention neither authorizes nor explicitly excludes other types of cross-border data forensic methods.

On the other hand, the Budapest Convention may bring the hidden concern of infringing on the sovereignty of other countries. "Communiqué of the Ministerial Meeting of G8 on Combating Transnational Organized Crime" in 1999, as a prelude to the Budapest Convention, stated declaratively that "[t]he State conducting a data search should consider informing the target State accordingly, if such informing of the State in which the data are located is permitted under the domestic law of the target State, and if the content of the data reflects a violation of the criminal law of the target State or appears to be in the interest of the target State." However, it is clear that Article 32 of the Budapest Convention does not impose an "obligation to inform" on States Parties. Part 3.1 of the Guidance Notes on Article 32 of the Convention only suggests that, based on the protection of rights, the State performing cross-border data forensics "may consider" informing the relevant authorities of the place where the data are stored. From the strong territorial feature of criminal jurisdiction, an investigative measure, whether mandatory or arbitrary, cannot in principle be applied directly outside the country. Therefore, in accordance with the principle of State sovereignty, cross-border forensics should be granted a consent by the government of the country where the data are located, rather than merely by the ISPs or even the individuals. Otherwise, by accepting such a provision, a State would be exposed to the risk of the collection of information by the authorities of other States under the guise of criminal investigations, which would undoubtedly pose a threat of infringement of State sovereignty.

4 Overview and Evaluation of the EU's Regime for Cross-Border Data Forensics

This section will introduce the existing typical system of EU law on cross-border data forensics— "European Investigation Order" (hereinafter referred to as the "EIO") and its shortcomings, and analyze and evaluate the development trend of the EU legislation, i.e., to promote the voluntary cooperation between ISPs and authorities while focusing on the construction of mandatory disclosure mechanism for cross-border data.

4.1 The Introduction of European Investigation Orders

In order to create a "single, efficient and flexible" cross-border forensics mechanism within the EU, Belgium and other countries jointly initiated the construction of the EIO system on May 21, 2010, aiming at authorizing the competent authorities of the Parties to conduct cross-border evidence investigations on the basis of valid warrants. On April 3, 2014, the European Parliament and the European Council jointly adopted the "Directive Regarding the European Investigation Order in Criminal Matters". Eventually, on May

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

22, 2017, the European Investigation Order system came into force, applying to all EU countries except Denmark and Ireland (which did not participate). As a result, the vast majority of EU Member States will be able to use the EIOs to carry out mutual assistance work more easily without the need to apply outdated conventions and documents.

In general, EIO is a judicial decision issued or validated by the competent authorities of a Member State of the EU in order to obtain evidence, in accordance with the Directive, which contains one or more specific investigative measures to be conducted by another Member State. As it is implemented between the competent authorities of different EU member States, it still falls within the scope of MLA in criminal matters. However, different from traditional MLA in criminal matters, EIO is built on the basis of mutual recognition of the EU Member States, each participating Member State is obliged to recognize and implement the EIO, so seen from the EU as a whole, it is also equivalent to the EU's own intra-territorial forensics. Specifically, the core norms of the "Directive regarding the European Investigation Order in criminal matters" are as follows:

Table 12 Core Norms of the "Directive Regarding the European Investigation Order in Criminal Matters"

General Norms		
Article	**Topic**	**Specific Content**
Article 6(1)	Conditions for issuing and transmitting an EIO	The issuing authority may only issue an EIO where the following conditions have been met: (a) the issuing of the EIO is necessary and proportionate for the purpose of the proceedings referred to in Article 4 taking into account the rights of the suspected or accused person; and (b) the investigative measure(s) indicated in the EIO could have been ordered under the same conditions in a similar domestic case
Article 9(1), (2)	Recognition and execution	The executing authority shall recognise an EIO, transmitted in accordance with this Directive, unless that authority decides to invoke one of the grounds for non-recognition or non-execution or one of the grounds for postponement provided for in this Directive. The executing authority shall comply with the formalities and procedures expressly indicated by the issuing authority unless otherwise provided in this Directive and provided that such formalities and procedures are not contrary to the fundamental principles of law of the executing State
Article 12	Time limits for recognition or execution	In general, the executing authority shall take the decision on the recognition or execution of the EIO no later than 30 days after the receipt of the EIO by the competent executing, and the executing authority shall carry out the investigative measure not later than 90 days following the taking of the decision referred to above. But if it is not practicable in a specific case for the competent executing authority to meet the time limit of 30 or 90 days, it shall, without delay, inform the competent authority of the issuing State the reasons for the delay and in such a case, the time limit of 30 days may be extended by a maximum of 30 days, while the limit of 90 days may be extended to appropriate timing by a consultation with the issuing authority
Specialized Rules for Electronic Evidence in Two Circumstances		
Article 10(2)	General investigative measures stipulated in Article 10(1) should not be applied to the identification of persons holding a subscription of a specified phone number or IP address	
Article 30	Request for interception of telecommunications with technical assistance of another Member State	
Forensic Measures listed Separately		
Hearing by videoconference or other audiovisual transmission, collecting information on banking and other financial operations, investigative measures implying the gathering of evidence in real time, continuously and over a certain period of time, covert investigations, and so on		

Although the EIO has greatly improved the efficiency of cross-border forensics among EU Member States by providing a clearer time limit for its execution, it is still at odds with the rapidly developing practice of cross-border data forensics. Firstly, because the system is designed for all types of evidence, not specifically for data, it is obviously difficult to adapt to the increasingly urgent cross-border data forensic needs in recent years. Secondly, the maximum of 120 days of work for the cross-border data forensics is still too long. In addition, since the EIO does not apply to Ireland, which is an important Member State, its significance for cross-border data forensic practice in EU is also greatly reduced.

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

4.2 Recent Legislative Developments Regarding Cross-border Data Forensics in the EU

Since 2015, EU official bodies have made considerable efforts to revamp the existing system and to advance the expeditious cross-border data forensics in criminal investigations. With this aim in mind, the EU has taken the path of moving towards mandatory disclosure of cross-border data while promoting voluntary cooperation by service providers.

4.2.1 Promoting Voluntary Cooperation by Service Providers

As data disclosure requests to service providers continue to be an important means of obtaining cross-border data in criminal proceedings, the EU continues to focus on voluntary cooperation with service providers. As it stands, this is to be realized based on five aspects:

First, law enforcement agencies of EU Member States is required to set up specialized liaison departments to strengthen collaboration with service providers and enhance the standardization of cross-border data requests, for example, Belgium and France have taken the lead in the implementation of this mechanism; second, the EU encourages service providers to set up counterpart liaison agencies to enhance the efficiency of cooperation with law enforcement agencies, for example, the European branches of multinational technology companies such as Apple, Facebook, Google and Microsoft have all set up corresponding functional departments; third, the EU tries to clarify the implementation process and applicable standards for service providers in the area of cross-border data disclosure, so as to enhance law enforcement agencies' understanding of their working mechanism; fourth, unifying the request formats of EU Member States and promoting standardized processing; and fifth, strengthen the collaboration between EU competent authorities and U.S. service providers in Europe, including developing special training programs and establishing a long-term experience exchange mechanism.

However, the promotion of voluntary cooperation with service providers does not address the shortcomings of the "voluntary cooperation" model itself. There are already some obvious problems with this mechanism as it currently operates. Firstly, the scope of cross-border data that can be collected under "voluntary cooperation" is limited. Taking the cooperation between the law enforcement departments of the EU Member States and the American ISPs located in Ireland as an example, the latter can only disclose the user registration information stored in the United States such as "non-content data" according to the principle requirements of the Electronic Communications Privacy Act (ECPA) which came into effect in 1986. As for "content data", such as specific content in e-mails, that concerning with privacy and other fundamental rights is specially protected by law, the corresponding data forensics still need to be carried out through the MLA. Secondly, as ISPs may face the risk of penalties from the country or region where the data is stored, it is difficult to ensure the enthusiasm and compliance of "voluntary cooperation". For instance, some countries have clear restrictions or even prohibitions on the cross-border flow of data for the purposes of data sovereignty and security, and the protection of citizens' personal information, etc., in which case ISPs submitting data to foreign investigative authorities in need of evidence will undoubtedly be penalized.

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

4.2.2 The Construction of Mandatory Disclosure Mechanism for Cross-border Data

As mentioned above, the stability and sustainability of cross-border data disclosure still cannot be ensured if only voluntary cooperation from service providers is optimized. For this reason, the EU has increasingly realized in recent years the need to make such data disclosure mechanisms mandatory. Even though the Budapest Convention has attracted the accession of the United States, Japan and other countries, the vast majority of the Contracting Parties are still Member States of the EU. Consequently, the relevant legislative process of the EU law can be considered to have been clearly reflected in the construction of mandatory cross-border data disclosure regimes under the Second Additional Protocol in 2022 and "Regulation on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings and for the Execution of Custodial Sentences Following Criminal Proceedings" (hereinafter referred to as the "Electronic Evidence Regulation") in 2023. Since the way in which the Second Additional Protocol facilitates mandatory data disclosure has already been summarized before, this section will focus on that in the Electronic Evidence Regulation, i.e., the European Production Order and the European Data Retention Order, which are aimed at strengthening the obligations of the ISPs to submit and preserve electronic data. The European Production Order and the European Preservation Order are designed as follows:

Table 13 Comparison between European Production Order and European Preservation Order

European Production Orders	European Preservation Orders
"European Production Order" means a decision ordering the production of electronic evidence, whether or not these evidence are stored in the EU, and addressed to a designated establishment or to a legal representative of a service provider offering services in the EU, where that designated establishment or legal representative is located in another Member State bound by this Regulation	"European Preservation Order" means a decision which orders the preservation of electronic evidence for the purposes of a subsequent request for production, and addressed to a designated establishment or to a legal representative of a service provider offering services in the EU, where that designated establishment or legal representative is located in another Member State bound by this Regulation
Where a notification to the enforcing authority is not required pursuant to Article 8, upon receipt of an European Production Order Certificate (EPOC), the addressee shall ensure that the requested data are transmitted directly to the issuing authority or the law enforcement authorities, as indicated in the EPOC, at the latest within 10 days following receipt of the EPOC; however, in emergency cases, the addressee shall transmit the requested data without undue delay, at the latest within eight hours following receipt of the EPOC	

Moreover, the scope of data to be submitted and kept by ISPs has significantly broadened, and has been extended to include content data, in addition to subscriber information which is required to be included in the disclosure requirements under the Budapest Convention. If an ISP refuses to comply with the European Production Order and the European Preservation Order without a justified reason, this may lead to sanctions or enforcement according to provisions in Chapter III of the Regulation. In a nutshell, these two types of orders will undoubtedly substantially change the current form of voluntary cooperation from service providers, thus shifting the cross-border data disclosure regimes in the EU Member States to a distinctly mandatory one.

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

4.2.3 Evaluations on the Recent Legislative Developments in EU

It can be seen that the new legislative developments in the EU have a strong trend of cross-border unilateral forensics, and the fact that this kind of unilateralist forensics has been given full attention in the legislative program is sufficient to show that a certain degree of consensus has already been reached within the EU on the provision of new cross-border remote forensics measures on the basis of the Budapest Convention. In this context, the MLA mechanism will inevitably be gradually transformed into a more "operational" forensic regime without the authorization of the state where the data is located, which will undoubtedly bring potential risks regarding data sovereignty and security, and the protection of legitimate rights and interests related to data to EU's cross-border data forensics. Take cross-border remote search as an example, when the law enforcement officials of one country "go to the database located in another country" to search the computer system without authorization, the lack of coordination and cooperation will give rise to procedural law and sovereignty issues.

In addition, the trend towards faster cross-border data forensics has effectively expanded the investigative powers of the competent authorities in EU Member States. This trend would pose a risk to the protection of the rights of the private entities. As the tension between the exercise of investigative powers and the protection of the rights of suspects in the criminal justice process has always existed, the rapid development of the cross-border data forensic system may further exacerbate this contradiction, and make the protection of rights face even more serious challenges than the traditional situation. For example, when the scope of disclosure is extended from non-content data regulated by the current system to content data, the consequences of any infringement of rights caused by procedural violations or abuses of power will show a geometrically magnified effect.

5 Overview and Evaluation of the U.S. Cross-Border Data Forensic Regimes

5.1 The Development of Cross-Border Data Forensic Norms in the United States—An Example of the "Data Controller" Model

The Stored Communications Act (SCA), issued in 1986, authorizes U.S. law enforcement to require ISPs to disclose content and non-content data of users or subscribers, subject to a court order. However, the Act does not specify whether disclosure includes data stored outside the country. This shortcoming triggered a major controversy in the Microsoft Corp. v. United States (hereinafter referred to as the "Microsoft-Ireland cases") and has spurred a series of subsequent legislation. In July 2017, the U.S. Congress prepared the International Communications Privacy Act, which would allow law enforcement authorities to compel cross-border ISPs to disclose data through a court writ if the foreign government receives advance notice and does not raise an objection. However, including this Act, none of explorations concerning cross-border data forensics have been substantively advanced.

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

It was not until the United States formally introduced the "Clarifying Lawful Overseas Use of Data Act" (hereinafter referred to as the "CLOUD Act") in March 2018 that the forensics of data stored outside the country through ISPs was generally recognized. Specifically, the CLOUD Act provides that a company subject to the jurisdiction of a state may be required to export data under the company's control, regardless of when and where the data is stored. In other words, the CLOUD Act explicitly adopts the "data controller" forensics model by allowing the U.S. government to require ISPs registered in America to submit information about their subscribers that is stored in another country. This suggests the U.S. extents its jurisdiction to the data of U.S. businesses operating outside of its borders through the idea of nationality jurisdiction.

5.2 Introduction on Key Elements of the CLOUD Act

The CLOUD Act's cross-border data forensics regimes can be analyzed from the perspectives of two different forensic subjects: "the U.S. law enforcement authorities' access to data stored outside the U.S. through a service provider" and "access to data stored in the U.S. by a qualifying foreign government through a service provider":

5.2.1 U.S. Competent Authorities' Access to Data Stored outside the U.S. through a Service Provider

According to the CLOUD Act, a provider of electronic communication service or remote computing service shall comply with the obligations to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.

The CLOUD Act imposes data disclosure obligations to specific service providers. There are two categories of service providers within this scope, namely "electronic communication service providers" and "remote computing service providers", as further illustrated in the table below:

Table 14 Service Providers Stipulated in the CLOUD Act

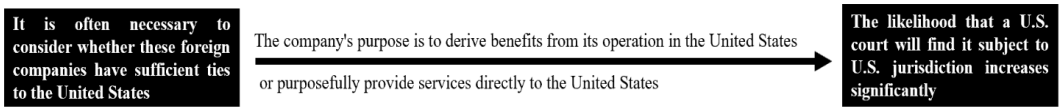
Electronic Communication Service Providers	**Remote Computing Service Providers**
The term "electronic communication service" is defined in 18 U.S.C. Section 2510 as: "any service which provides to users thereof the ability to send or receive wire or electronic communications"	The term "remote computing service" is defined in 18 U.S.C. Section 2711 as "the provision to the public of computer storage or processing services by means of an electronic communications system"
Service Providers Generally Include:	
These definitions include such companies as email providers, cell phone companies, social media platforms, and cloud storage services. They do not include a company just because it has some interaction with the Internet, such as certain e-commerce sites. These definitions are consistent with Article 1.c. of the Budapest Convention.	

It is important to note that the two categories of service providers are not limited to United States corporations in general meaning, United States-based corporations or Americans-owned corporations, but also include foreign corporations under the jurisdiction of the United States operating in its territory, and possibly

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

even foreign corporations operating outside the United States but providing services to its territory. For foreign corporations operating in American territory, the determination of jurisdiction is more complex. Under general standards of U.S. law, the issue needs to be analyzed on a case-by-case basis:

Figure 1 Factors Considered While Determining Whether the U.S. Can Exercise Jurisdiction



As for foreign corporations operating outside the United States but providing services to its territory, the United States does not have jurisdiction over them in principle. If these companies or their branches in the foreign country in possession of the electronic data required for the investigation, then it should be considered whether the company operating in the United States have sufficient control over the corresponding data, so as to determine whether the jurisdiction of the United States is established. Therefore, this also needs to be analyzed on a case-by-case basis rather than generalized. In this regard, page 8 of "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act" (hereinafter referred to as the "White Paper") sets out the relevant criteria for establishing nationality jurisdiction:

Figure 2 A Procedure to Justify the Exercise of Jurisdiction over a Specific Type of Foreign Company



When it comes to the content of disclosure, the "data" subject to disclosure is the content of wired or electronic communications, and all records and other information relating to users or subscribers of the information, that are in the possession, custody or control of the service provider and that should be preserved, copied or disclosed. Specifically, according to the White Paper, the types of data that United States law enforcement authorities and "qualifying foreign government" may collect, as well as those that they are not authorized to collect, are shown in the figure below:

Table 15 Data that are Authorized to be Collected and those are Not

Types of Data to be Disclosed	Data that are Not Authorized to be Collected Mandatorily
Contents of communications	The CLOUD Act is "encryption neutral." It does not create any new authority for law enforcement to compel service providers to decrypt communications. Neither does it prevent service providers from assisting in such decryption, or prevent countries from addressing decryption requirements in their own domestic laws
Non-content information associated with such communications	
Subscriber information	
Data stored remotely in the cloud on behalf of a user	

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

Whenever law enforcement authorities issue a data disclosure order to a service provider in the course of a criminal investigation in accordance with the statutory procedures, the latter is required by law to make the disclosure, with the exceptions set out below, irrespective of whether the corresponding electronic data are located in the United States or not. A service provider's refusal to comply with a cross-border data disclosure order may constitute a contempt crime under the relevant provisions of the U.S. Code. In order to protect its legal rights, a service provider may file a motion with the court within 14 days to modify or quash the legal process, thereby staying the disclosure of data stored outside the U.S. The filing of such a motion is subject to the following requirements:

Table 16 Reasons to File a Motion and the Requirements during the Pendency of a Motion

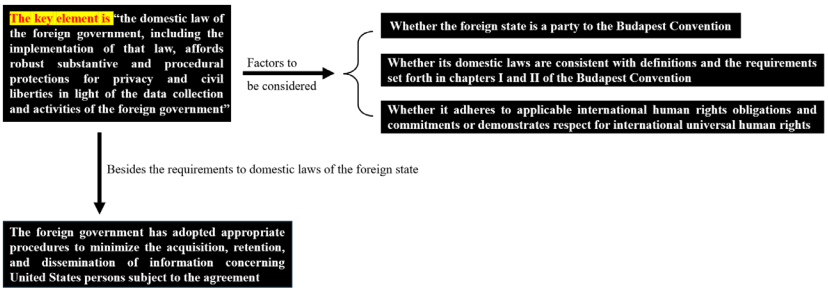
The Requirements to a Service Provider during the Pendency of a Motion	Justifiable Reasons to File a Motion
A service provider shall preserve, but not be obligated to produce, information sought during the pendency of a motion	The customer or subscriber is not a United States person and does not reside in the United States
	The required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government
	Besides the above two factors, the Court can base on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed

5.2.2 Qualifying Foreign Governments' Access to Data Stored in the U.S. through a Service Provider

Based on the so-called "principle of reciprocity", the CLOUD Act not only authorizes U.S. law enforcement to access data stored outside of the United States through service providers, but also allows "qualifying foreign governments" to access data stored in the United States directly in this manner without the consent of U.S. authorities. However, the so-called "reciprocity" provided by the U.S. to certain countries is not absolute. The CLOUD Act set restrictions on qualifying foreign governments' access to data stored in the United States. If the requirements are not met, the country concerned will still have to go through a lengthy MLA process to request the United States authorities to collect electronic data on its behalf.

The limits set by the CLOUD Act can mainly be seen in the scope of qualifying foreign governments. It requires an executive agreement between the foreign state and the United States, which must be reported in written form to the Congress by the Attorney General of the United States (along with the Secretary of State). A foreign government will be determined to be "qualifying" under the CLOUD Act when it is found to meet all of the following elements:

Figure 3 Limits Set Forth by the CLOUD Act in the Scope of Qualifying Foreign Governments



© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

It is clear from the above limitations that "qualifying foreign governments" would be limited primarily to the States Parties to the Budapest Convention. However, since the vast majority of States Parties are the Member States of the EU, most governments in the world would probably not be able to satisfy the criteria of a so-called "qualifying foreign governments". It is clear that the CLOUD Act is not reciprocal since it only restricts the collection of data stored in the United States by foreign governments, but not limiting the geographic scope of the U.S. government's access to data stored outside of the United States.

6 Reflections on the American-European "Data Controller" Model of Cross-border Data Forensics

Currently, there are two main data jurisdiction models in the international arena: the "data controller" model and the "data storage place" model. The so-called "data controller" model refers to the acquisition of data under the control of a cross-border cloud service provider by seeking its cooperation or issuing instructions to it under the technical framework of cloud computing, while the "data storage place" model means a state can only exercise jurisdiction over the data stored in its territory. The American-European approach should clearly be categorized as a data controller model, i.e., accessing data under the control of cross-border cloud service providers by seeking their cooperation or imposing mandatory data disclosure obligations on them. This is a profound reflection of the loosening of the traditional "data storage place" model and the rise of the emerging "data controller" model in the age of networks and electronic information. While the "data controller" model meets the development of the times and greatly improves the efficiency of forensics, it also carries certain pitfalls and risks (especially in terms of national judicial sovereignty).

Since forensics under the "data controller" model bypasses the competent authorities of a certain state but directly collects data from the private entities, it is considered as unilateral forensic measures. At present, the international attitude towards unilateral cross-border data forensics can be divided into two camps: one is the view that cross-border data forensics outside the framework of criminal MLA would infringe on the judicial sovereignty of the state; the other is that countries including the States Parties to the Budapest Convention advocate the free flow of data and oppose the concept of data sovereignty. Western countries hope to maintain their dominant position in cyberspace through the establishment of international legal rules on cyberspace, while developing countries hope to safeguard their own cyber sovereignty, and the arguments between the two sides are becoming more and more acute.

According to the principles of international law, criminal jurisdiction is based on the principle of territoriality. Since criminal jurisdiction is an important manifestation of national sovereignty, criminal judicial activities, including investigations, once carried out across national borders, are in principle a violation of the sovereignty of other countries. However, setting the boundaries of cross-border data forensics in accordance with the traditional notion of sovereignty may result in a portion of the data in cyberspace being removed from the jurisdiction of any one country, which is not conducive to combating crime. Taking the data in the "dark web" as an example, the existence of multiple encryption technologies makes it impossible for law enforcement officials to determine the actual physical storage location of the data, thus making it impossible to exercise criminal jurisdiction according to the geographical scope. It can be seen that if criminal justice

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

is strictly governed by the traditional principle of territorial jurisdiction, cross-border data forensics will be greatly restricted, thus seriously falling short of the real needs in law enforcement practice.

However, the phenomenon the United States and Europe completely abandon the traditional "data storage place" model and turn to the "data controller" also has obvious negative impacts: first, states that adhere to the principle of territorial jurisdiction may lodge diplomatic protests or reciprocal response against countries conducting unilateral cross-border data forensic measures, and even induce more serious international disputes; second, abandoning the principle of territorial jurisdiction may lead to the imitation of other countries or regions, and further incentivize countries to take unilateral actions in the field of data forensics in an arbitrary manner to circumvent international cooperation. Such a trend would undermine the existing framework for international cooperation and ultimately lead to the fragmentation and disorganization of cross-border data forensics rules on a global scale.

7 Remarks: The Future of China's Cross-border Data Forensics Rules

Cross-border data forensics has become increasingly important in the digital age, but also faces multiple challenges such as data sovereignty and international cooperation. Based on the international practice and domestic legislative developments introduced above, China can improve its regimes of cross-border data forensics in following aspects:

Firstly, the basic principles of cross-border data forensics system should be clarified, i.e. the principle of equality and reciprocity, and the principle of data sovereignty. Since the former one is not only a basic requirement of international law, but also a core element of "Law of China on International Criminal Judicial Assistance", China should adhere to the principle of equality and reciprocity in cross-border data forensics, emphasizing the reciprocity of the rights and obligations of all parties in international cooperation. Through equality and reciprocity, China is able to ensure that its own interests are not infringed upon when cooperating with other countries, while at the same time promoting the healthy development of international judicial assistance in criminal matters. Moreover, data sovereignty is a core issue in cross-border data forensics. China should advocate exploring the definition of data sovereignty with Chinese characteristics based on international consultation and cooperation, rather than unilateralism.

Secondly, as completely turning to "data controller" model is not the proper way to establish the cross-border data forensics regimes, China should construct a restricted application and reciprocal response system for the "data controller" model. Even though the "data controller" model is highly efficient, it may infringe on the sovereignty of other countries. China is should in favor of applying the model under strictly limited conditions to avoid abuse. For example, cross-border forensics through the "data controller model" should be allowed only if permitted by foreign law or international comity. When it comes to the response to the "long arm jurisdiction" of the CLOUD Act, China should propose a reciprocal response strategy, in which China can request United States ISPs to provide data stored in the United States when necessary. This mechanism would not only protect China's sovereignty, but also provides legal protection for Chinese enterprises.

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

Furthermore, data should be regulated based on its classification and grading. To be begin with, based on the existing trichotomy of data, i.e. “key data”, “core data”, “general data”, China can set up different protection measures and cross-border forensic procedures for different levels. For example, core data should subject to the strict application of “data storage place” model, while general data can subject to looser restrictions. With this idea as the principle, China can explore the establishment of a data “white list” system, which allows law enforcement authorities to access data directly from servers outside China under specific conditions. This system would improve the efficiency of forensics while safeguarding national security.

Funding

Supported by the National Social Science Foundation of China "Research on Anti-Monopoly Regulation of Acquisitions of Start-ups in the New Pattern of International Competition" (Grant No. 22BFX194)

References

[1]Pei, W. (2024). The History of the Development of the United Nations Convention against Cybercrime, its Core Content and Dynamic Adaptation in China. China Information Security, (08), 53-56, 56.

[2]Liang, K. (2019). On the Change Logic of Terrorism Development Trend and Enlightenment of EU Cross-border Fast Electronic Evidence System. Journal of People’s Public Security University of China (Social Sciences Edition), (01), 33-43, 34.

[3]Richard A．Clarke，et al., Liberty and Security in a Changing World: Report and Recomm-endations of The President’s Review Group on Intelligence and Communications Technologies, the White House President Barack Obama (Dec.12, 2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[4]Hu, J.S., Huang, Z.X. (2016). The Problems and Prospects of the International Legal Regi-mes in Combating Cybercrimes——From the Perspective of Council of Europe’s Convention onCybercrime. Chinese Review of International Law, (06), 21-34, 26-27.

[5]Liang, K. (2023). Data Sovereignty and Security: Cross-border Electronic Data Forensics, T-singhua University Press.

[6]Wei, G.X., Liu, X.S. (2024). Public-Private Cooperation in Cross-Border Data Forensics——From the Perspective of the United Nations Convention against Cybercrime. Hebei Law Scienc-e, (08), 78-100, 83.

[7]Liang, K. (2019). Restructuring the System of Cross-Border Remote Collection of Electronic Evidence. Global Law Review, (02), 132-146, 136.

[8]Pei, W. (2022). On Remote Inspection: Based on the Systematic Review of Investigative Me-asures. Tribune of Political Science and Law, (04), 156-166, 162.

[9]Nicolai Seitz，Transborder Search: A New Perspective in Law Enforcement，7 Yale Journal of Law and Technology 23 (2004)．

[10]Marloes C. van Wijk (2017). Cross-border evidence gathering: equality of arms within the EU?, Eleven International Publishing.

[11]Liu, P.X. (2022). EU’s Approach to Cross-border Electronic Evidence Collection and Its Enlightenment to China. Journal of National Prosecutors College, (05), 3-23, 9.

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

[12]Wu, S.K., Chen, B.C., & Zhen, N. (2018). Analysis of the (Draft) EU E-evidence Regulat-ion. Civil-Military Integration on Cyberspace, (12), 42-49, 42.
[13]Xia, H. (2023). Strengthened Market Regulation of EU in Legislation for Cross-Border Data Flow and Implications for China. Hebei Law Science, (08), 169-182.
[14]Anna-Maria Osula, Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritor-ially Located Data, 9 Masaryk University Journal of Law and Technology 43 (2015).
[15]Lu J.P., Wang J.X., & Yang, Y.L. (2003). International Cooperation on the Crack Down upon Internet Crimes and the Internet Terrorism. The Jurist, (05), 60-69, 62.
[16]Alessandro Bernardi, Daniele Negri (2017). Investigating European Fraud in the EU Memb-er States, Hart Publishing.
[17]Mei, H (2020). On Data Governance, China Renmin University Press.
[18]XU K. (2018). The CLOUD Act in the Perspective of Data Sovereignty. China Information Security, (04), 40-42, 42.
[19]Yu Z.G. (2015). The Standpoint of China in Concluding and Participating in the Internation-al Convention on Cybercrime. Tribune of Political Science and Law, (05), 91-108.

© 2025 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)