Yale Law School
Paul Tsai China Center
耶鲁大学法学院蔡中曾中国中心

“Game of Laws”: Cross-Border Data Access for Law Enforcement Purposes

Models in the United States, Europe, and China

Hong Yanqing

BEIJING INSTITUTE OF TECHNOLOGY SCHOOL OF LAW

Foreword

Debates around global data flows and government access to data have moved to the center of geopolitical and legal conflict. In the following essay, "Game of Laws: Cross-Border Data Access for Law Enforcement Purposes—Models in the United States, Europe, and China," Professor Hong Yanqing provides a timely and important contribution to our understanding of the interaction among regional approaches and the perspectives of policymakers and stakeholders in different jurisdictions. Complex interactions among various countries' legal frameworks for data governance are having profound implications for personal privacy, cybersecurity, global trade, and economic and technological competitiveness.

A professor at the Beijing Institute of Technology School of Law, Hong Yanqing is a leading scholar on global data governance and China's data protection regulatory framework. His work has been influential in shaping China's emerging data governance regime amid ongoing discussions of data ownership and privacy taking place in China. His essay thus offers a unique lens on China's evolving data governance reforms.

This essay was first published in Chinese in the *Global Law Review* (环球法律评论), issue no. 1, 2021. It has been translated by the Yale Law School Paul Tsai China Center in conjunction with an ongoing series of dialogues on data security convened by the Center. Dr. Hong's essay originated as part of a special project under China's Ministry of Justice in 2018 entitled "Big Data and Cybersecurity Legislation" (18SFB1005).

The views expressed in this essay are those of the author alone and do not represent those of the Paul Tsai China Center or Yale University.

Samm Sacks
Senior Fellow, Paul Tsai China Center, Yale Law School

"Game of Laws": Cross-Border Data Access for Law Enforcement Purposes

Models in the United States, Europe, and China

Hong Yanqing

Abstract In administrative law enforcement and criminal proceedings, evidence generally takes the form of electronic data given the extensive application of information technology. Globalization and digitization make it necessary for law enforcement to access data across borders. Law enforcement cross-border data access mainly occurs in two scenarios: when the data requested is stored offshore, or a foreign law enforcement authority tries to access data stored onshore. Therefore, governments often need to "take" data from abroad under the first scenario and try to "block" access by a foreign entity under the latter. The United States and Europe, as two dominant players in the digital economy, adopted different models of "taking" and "blocking" data based on real needs, the state of their industrial development, legal tradition, and overall strategy. In recent years, China has developed its data access rules by adopting documents such as the *Law on International Criminal Judicial Assistance, Data Security Law, Personal Information Protection Law (Draft),* and other regulations. Analysis of the three jurisdictions' models reveals their potential interaction and impact on China's sovereignty, security, and development interests.

Keywords data sovereignty, cross-border data access, data retrieval/access, data blocking

Hong Yanqing, *Professor, Beijing Institute of Technology School of Law*

Introduction

In the era of globalization, interconnection, and digitization, cross-border access to data stored in other countries for law enforcement purposes ("cross-border data access") is almost inevitable[1] for any country. Sovereign states deal with cross-border data access under these two scenarios: when the data requested is stored offshore, or when a foreign law enforcement authority tries to access data stored onshore. The former requires "taking" data from abroad (hereafter referred to as "take") while the latter requires "blocking" access by a foreign entity (hereafter referred to as "block"). China's current regime towards cross-border data access for law enforcement upholds the pre-Internet-era concept of sovereignty, where data is bound within a geographical territory. However, there is no shortage of legislation or practice of "bypassing other countries' sovereignty" to retrieve data from abroad directly. Recent cases are found in the United States, a global Internet industry leader, and the European Union, a data legislation pioneer. The "bypass" is not entirely a neglect of sovereignty. It comes from real needs for law enforcement in the Internet age. China's adoption of the *Law on International Criminal*

1 For a general discussion on law enforcement access to data across borders, see Jennifer Daskal, Law Enforcement Access to Data across Borders: The Evolving Security and Rights Issues, Vol.8 (3), *Articles in Law Reviews & Other Academic Journals,* 473-502 (2016).

Judicial Assistance and the recent *Data Security Law* indicate an entirely different stance on cross-border data access from the U.S. or the European system. Therefore, it is practical and essential to analyze the similar and distinct approaches in China, the United States, and the European Union (EU). This paper begins with a detailed account of the "game of taking vs. blocking" in cross-border data access, followed by a summary of data access models in the United States and the European Union. The author analyzes China's scheme and explores the potential interaction between the three jurisdictions. The paper offers solutions to safeguard China's sovereignty, security and development interests in cross-border data access.

The "Game of Taking vs. Blocking" in Cross-Border Data Access for Law Enforcement

Human life is increasingly networked and digitized. In law enforcement and judicial practice, evidence increasingly exists electronically. "Instead of merely 'obtaining' independent legal status, electronic evidence is poised to become 'the king of all evidence' in the new age."[2] In borderless cyberspace, electronic evidence invariably contains cross-border elements, making it difficult for law enforcement authorities to access data stored offshore.

"Take" in the Right Way: The Present Practice of Cross-Border Data Access

In general, when a country's law enforcement agencies attempt to access the data stored offshore or vice versa, they shall obtain the consent and assistance of the competent authorities of the country where the data is stored and may not overstep their authority to show respect for the other's sovereignty.[3] Five typical modes of doing this fall within the framework of international law: First, international conventions which contain provisions on judicial assistance; second, judicial assistance procedures agreements signed between countries;[4] third, based on the principle of reciprocity where specific judicial assistance is carried out in a case-by-case manner; fourth, a letter requesting formal judicial assistance submitted by the court of one country to the court of the other country; fifth, bilateral and multilateral police cooperation.

The common feature shared by the above five modes is full involvement of state sovereignty: the clauses in the conventions and treaties on judicial assistance are negotiated among sovereign states and need to be signed and ratified by them; other requests for assistance or police cooperation also need the participation of and implementation by competent authorities of the states. In practice, the "threshold" remains high when "bypassing" state sovereignty is not an option. For instance, the matter on which assistance is sought must also be recognized as a crime in the other country, and ultimately, the other country has the discretion to either accept or refuse the request. Out of national

2 Pinxin Liu, The Basic Theory on Electronic Evidence, Vol. 1, *Journal of National Prosecutors College*, 151 (2017).

3 See Marusa T. Veber and Masa Kovic Dine, *Big Data and Economic Cyber Espionage: An International Law Perspective,* Routledge, 2014, p.11.

4 See Valsamis Mitsilega, New EU-USA Cooperation on Extradition, Mutual Legal Assistance and the Exchange of Police Data, Vol.8 (4), *European Foreign Affairs Review*, 515-536 (2003).

security and public interest concerns, the states may consider non-judicial factors. For example, the United States often complains that the Russian government rarely assists the United States in law enforcement investigations of cybercrimes by Russians.[5]

Besides the high threshold and the need for significant coordination and cooperation, in reality, the greatest shortcoming of the above five modes is inefficiency. According to some U.S. scholars, it takes the U.S. government on average ten months to process judicial assistance requests from foreign countries.[6] Clearly, such speed fails to meet law enforcement agencies' needs, especially in the Internet age when changes are measured in milliseconds.

New trends have exacerbated the dissatisfaction among law enforcement agencies with judicial assistance procedures. With the wide adoption of communication encryption technology, law enforcement agencies can only intercept encrypted data packets that cannot be successfully decrypted, masking the real content. Therefore, it is necessary to "search" the servers, terminals, and cloud infrastructure where the communication content has "landed." However, communication service providers often deploy the hardware offshore due to cost and other considerations, making it an objective necessity to strengthen cross-border data access in law enforcement.[7] To complicate the matter, communication tools and channels are being changed all the time. In his testimony to the U.S. Senate Judiciary Committee, the United Kingdom's deputy national security adviser pointed out that British police effectively monitored the communications between terrorists in Britain. When the terrorists switched to communication products from the United States, the British government had to request that U.S. companies hand over the contents of such communications. However, the U.S. companies made it clear that the UK had to go through bilateral judicial assistance procedures.[8] In other words, crimes committed by local actors used to be monitored only through domestic legal procedures, but now because criminals use foreign communication products or services, the "threshold" of monitoring or searching stipulated by other countries' laws has to be met and the consent of other countries' judicial agencies obtained before accessing the data. When bilateral or multilateral judicial assistance is possible, the process is protracted, with huge workforce input. Law enforcement is almost impossible if criminals deliberately choose the communication tools produced by so-called "crime havens."

Judicial assistance procedures are rendered weak, if not obsolete, in combating crimes in the Internet age, and law enforcement is forced to explore other methods outside that framework. With the degree of transnationalization and informatization increasing, law enforcement agencies have found that if an organization that holds overseas data has a local headquarters or branch, law enforcement agencies may claim jurisdiction over that organization, which owns data stored overseas. By applying domestic procedures and legal doctrines, the local branch or head office may be requested or forced to "bring ashore" the data. For example, a Brazilian court imprisoned Facebook's Brazilian

5 See Roderic Broadhurst, Developments in the Global Law Enforcement of Cyber-crime, Vol.29 (3), *Policing: An International Journal of Police Strategies & Management,* 408-433 (2006).

6 See Peter Swire and Justin Hemmings, Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program, Vol.71 (4), *NYU Annual Survey of American Law,* 687-740 (2017).

7 See Peter Swire, From Real-time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud, Vol.2 (4), *International Data Privacy Law,* 200-206 (2012).

8 See Written Testimony of Mr. Paddy McGuinness, United Kingdom Deputy National Security Adviser, Before the Judiciary Sub-Committee on Crime and Terrorism, United States Senate, *https://www.judiciary.senate.gov/download/05-24-17-mcguinness-testimony*, last visited on [2021-01-07].

executives after the company denied access to WhatsApp's communications regarding a case of organized crime and drug trafficking. Facebook argued that WhatsApp had no staff in Brazil and operated independently from Facebook and hence was not liable.[9] On the other hand, the Brazilian court saw fit to exercise jurisdiction since Facebook had wholly acquired WhatsApp and set up an office in Brazil.

"Blocking" Measures: Typical Tactics in Blocking Cross-Border Data Access

While some countries have innovated the "taking" of data from abroad, others have developed countermeasures to block access. The most representative practice is that of "blocking statutes" in civil law countries, intended to block the discovery process in common law systems (mainly in the United States).

Discovery is a judicial process in American civil and criminal proceedings where the parties exchange evidence to reveal the truth from the adversarial process between the two parties. Judges will sustain and protect the parties' right to information. As a result, U.S. courts grant extensive rights to the parties to request evidence in the form of court orders (e.g., subpoenas).[10] As early as the 1970s, the Federal Court of Appeals for the Second Circuit clearly stated: "If a federal court has jurisdiction over a person who possesses or controls a document, the court has the power to require the person to provide the document located outside the country. This is not open to doubt."[11] In criminal proceedings, precedents in the United States have long supported prosecutors to issue subpoenas requiring companies operating in the United States to hand over documents, records, and other materials[12] located outside the United States. The U.S. Department of Justice (DOJ) has made it clear that prosecutors can request that foreign banks' U.S. offices provide data and documents located outside the United States, subject to DOJ's additional internal procedures.[13] Simply put, in the United States, the most critical factor in whether data can be retrieved from abroad is not where the data is stored but whether the case can be litigated in the United States. If a U.S. court has jurisdiction, the parties are required to provide case-related documents and data that they possess, control, or have access to, even if they are stored in another country.[14]

The "blocking statutes" in France are the most famous because the term originated from its French version. In 1980, to prevent the United States from engaging in an antitrust investigation against French shipping companies, France passed a special "Blocking Act."[15] Article 1 of the law prohibits any French person from disclosing economic, commercial, industrial, financial, or technological information to judicial or administrative authorities abroad as evidence without a French court order. France is not the only

9 See Jonathan Watts, Brazilian police arrest Facebook's Latin America vice-president, The Guardian, 1 Mar 2016, *https://www.theguardian.com/technology/2016/mar/01/brazil-police-arrest-facebook-latin-america-vice-president-diego-dzodan*, last visited on [2020-09-30].

10 See Bing Song, *A Reader: The Judicial System and Procedure in the United States and Germany,* CUPL Press, 274-279 (1999).

11 See United States v. First Nat'l City Bank, 396 F. 2d 897, 900-01 (2d Cir. 1968).

12 See In Re Grand Jury Proceedings (Bank of Nova Scotia), 740 F. 2d 817 (11th Cir.), cert. denied, 469 U.S. 1106 (1985); In Re Grand Jury Proceedings (Bank of Nova Scotia), 691 F. 2d 1384 (11th Cir. 1982), cert. denied, 462 U.S. 1119 (1983); In re Grand Jury Subpoena Directed to Marc Rich, 707 F. 2d 663 (2d Cir. 1983).

13 See Department of Justice, Criminal Resource Manual, *https://www.justice.gov/usam/criminal-resource-manual-279-subpoenas*, last visited on [2020-09-30].

14 See Joel R. Paul, Comity in International Law, Vol. 32 (1), *Harvard International Law Journal*, 1-79 (2001).

15 See The French Blocking Statute (Law No. 80-538 of 16 July 1980).

country to say "no" to the United States. Germany, the United Kingdom, and many other countries have similar blocking statutes. The United Kingdom enacted the *Protection of Trading Interests Act* of 1980, which authorized the Ministers of State to deny the discovery of evidence by foreign courts or public authorities to protect the UK's sovereignty or trading interests.[16] Also, there are laws to protect customer information. In light of the frequent demands for cross-border data access in the banking industry, strict confidentiality articles are often provided in banking laws that are considered de facto blocking statutes (such as those in Switzerland, Luxembourg, Singapore, and other countries).[17] In addition, there are laws on privacy protection, the most typical one being the *General Data Protection Regulation (GDPR)* of the European Union enacted in 2018.

MNCs Caught in the Middle

Multinational corporations (MNCs) operate in many countries. They face conflicting legal provisions in host countries. In practice, whether or not to cooperate with law enforcement requests for cross-border data access may raise legal liabilities and operational risks.

On the one hand, MNCs face legal uncertainties, including whether data requested by foreign law enforcement authorities can be freely transmitted from the country of storage and whether, even if the transmission is possible, the data can be disclosed to foreign governments or used in law enforcement investigations.

On the other hand, MNCs may be subject to future operational risks even if they allow cross-border data access by overseas law enforcement agencies. First, meeting one country's law enforcement authorities' data access requirements may trigger a chain reaction where other countries pursue the same goal,[18] leading to a conflict in applying the laws of different jurisdictions. To avoid this, MNCs need to set up data centers in each jurisdiction to keep copies of data for regulatory and judicial access,[19] which is tantamount to commercial suicide due to the staggering cost. Second, the host country of data storage may enact local laws to prevent the MNCs from accepting data access requests from another jurisdiction, thus damaging the requesting government's credibility. The laws may start with localization of data storage and later mandate the full localization of products and services.[20] Third, end-users may lose faith in the MNCs and opt for other products or services if they believe their data could be easily transferred to a foreign government.

16 See Protection of Trading Interests Act of 1980, *http://www.legislation.gov.uk/ukpga/1980/11*, last visited on [2020-09-30].

17 See Christopher H. McGrath and Neil J. Schumacher, Beyond Blocking Statutes: Revisiting Foreign Discovery Under the Hague Convention, *Paul Hastings*, 3 February 2015, *https://www.paulhastings.com/publications-items/details/?id=719ce369-2334-6428-811c-ff00004cbded*, last visited on [2020-09-30].

18 See Andrew Pincus, Why is the U.S. government trying to help Vladimir Putin access information stored in the United States? 9 February 2018, *http://www.scotusblog.com/2018/02/symposium-u-s-government-trying-help-vladimir-putin-access-information-stored-united-states/*, last visited on [2020-09-30].

19 See Matthew Kahn, Microsoft-Ireland Oral Argument Preview: Will the Supreme Court Stave Off Data Localization? Lawfare Blog, 26 February 2018, *https://www.lawfareblog.com/microsoft-ireland-oral-argument-preview-will-supreme-court-stave-data-localization*, last visited on [2020-09-30].

20 In *Microsoft Corp. v. United States*, if the U.S. Supreme Court had adhered to the data controller doctrine, the German government would have taken the stance of localization. See Craig A. Newman, Can the United States Search Data Overseas? New York Times, 26 February 2018, *https://www.nytimes.com/2018/02/26/opinion/united-states-searching-data-overseas.html*, last visited on [2020-09-30].

The U.S. Cross-Border Data Access Model

The United States has rich experience in "taking" and "blocking" of cross-border data. In particular, for law enforcement purposes, the U.S. Congress fast-tracked the *Clarifying Lawful Overseas Use of Data Act* (the CLOUD Act) in 2018, which indicates the centerpiece of the U.S. model is treating its enterprises as an extension of national territory. The point can be illustrated with *Microsoft Corp. v. United States*, which prompted the law's enactment.[21]

The "Taking" and "Blocking" Provisions in the Stored Communications Act

The Stored Communications Act (SCA) is the primary legal ground for U.S. law enforcement agencies to forcefully access individuals' or enterprises' private electronic communications. It is mainly applied in the United States and does not give clear instructions on overseas data. The dispute between the parties in *Microsoft Corp. v. United States* involved jurisdiction over data stored abroad, pointing to gaps in the law which the SCA later filled. Microsoft submits that the country where the data is stored has jurisdiction over the data (the "storage site doctrine"). The FBI insists that the United States has jurisdiction over the data that Microsoft controls regardless of whether the data is stored in the United States or not. In other words, the United States may access the data because the United States has jurisdiction over the data controller (the "data controller doctrine"). Each doctrine has its pros and cons. The storage site doctrine respects the sovereignty of the country where the data is stored, but the requesting country will suffer from inefficient and protracted law enforcement. Under such circumstances, criminals would choose foreign communication products or services to encumber investigations. The location of data centers chosen by MNCs may adversely affect investigations, which will create "data havens" and hinder cross-border law enforcement. Therefore, law enforcement agencies are motivated to use the data controller doctrine to forcefully access data stored overseas, claiming jurisdiction over the entity that controls the data. Nevertheless, such a practice may be perceived as an infringement of foreign sovereignty and subject the MNCs to legal liability in the country where the data is stored, due to conflicting legal provisions. It may bring higher operational and reputational risks to the MNCs in their overseas markets. Countries may demand data localization in new legislation, which will eventually increase the operating costs of MNCs.

21 In December 2013, the U.S. District Court for the Southern District of New York issued a search warrant requiring Microsoft to submit the e-mail content and account information of the user involved in a drug case to the U.S. Government. However, the user's e-mail content data was stored in Ireland. Microsoft refused to provide it to FBI and filed a motion to revoke the search warrant. In April 2014, the court rejected Microsoft's motion and Microsoft filed an appeal. In July 2014, the U.S. District Court for the Southern District of New York upheld the original ruling. Microsoft subsequently appealed to the U.S. Court of Appeals for the Second Circuit. In the appeal, all parties in the case agreed that the search warrant based on the *Stored Communications Act* may not apply extraterritorially, but the difference was that Microsoft believed that the search warrant was only applicable to data stored in the United States and might not cover the data stored in Ireland. However, the government believed that the search warrant only required Microsoft to perform certain operations in the United States and to disclose data to the government within the United States. Therefore, the search warrant was not applied extraterritorially. In July 2016, the U.S. Court of Appeals for the Second Circuit held that the FBI search warrant had no extraterritorial effect and that overseas data should be obtained through bilateral mutual legal assistance treaties. The FBI applied for a retrial. The case was referred to the Supreme Court of the United States after the U.S. Court of Appeals for the Second Circuit refused to rehear the case. In February 2018, the Supreme Court heard the case for the first time, but the dispute was rendered void because of the entry into force of the *CLOUD Act*, and the Supreme Court rejected the case in April 2018.

The SCA stipulates the prevention of access to data in the United States by law enforcement agencies of other countries. Section 2702 provides that a remote computing service provider or electronic communication service to the public shall not knowingly divulge a record or other information of a subscriber or customer of such service.[22] In Section 2703, the SCA authorizes a "governmental entity" to require the disclosure of data contents from the service provider by using a warrant procedure. A "governmental entity"[23] is limited to "a department or agency of the U.S. government, a state government, or a government at a lower political level."[24] In effect, the SCA requires a U.S. data controller only to disclose information to the U.S. government. According to the SCA, when a foreign government seeks data based on its internal legal procedures and the controller hands over the data, the controller would be guilty of violating the law.

In summary, the SCA is unclear on "taking" data from abroad but has clear stipulations on "blocking" data access by a foreign entity.

The CLOUD Act Centers on the Controller Doctrine

The SCA of 1986 is ambiguous on "taking" data from overseas and too prohibitive on "blocking" data access. In the absence of legal reform, in *United States v. Microsoft Corp.*, the U.S. Supreme Court had to choose between two bad options: impeding legitimate enforcement actions or bringing great harm to the global operations of U.S. companies. In February 2018, Senators submitted a draft CLOUD Act bill to address these concerns, which proposed a solution to the dispute between Microsoft and the FBI. The bill also opened up a channel for foreign law enforcement agencies to access the contents of communications data stored in the United States. In March 2018, the CLOUD Act was quickly passed and took effect immediately, gaining the support of many U.S. companies, including Microsoft, Apple, Google, and others.[25]

DEFINITION OF THE DATA CONTROLLER

The CLOUD Act explicitly adopts the data controller doctrine, stipulating that service providers shall keep, backup, and disclose communications, records, or other information they own, regulate, or control, regardless of whether or not the storage sites are in the United States. Service providers include electronic communications service providers and remote computing service providers. The Act applies to U.S. businesses and foreign businesses operating in the United States. It is worth noting that the businesses governed by the CLOUD Act are not limited to businesses incorporated in the United States. In its white paper on the CLOUD Act, the U.S. Department of Justice made it clear that as long as a foreign company's operation has a sufficient connection to the United States, it is sufficient to trigger the U.S. law's jurisdiction.[26] Given the pivotal position of the United States in the global Internet industry, the CLOUD Act has de facto jurisdiction over most influential Internet companies, maximizing the U.S. government's ability to access data in law enforcement actions.

22 See 18 U.S.C. § 2702.
23 See 18 U.S.C. § 2703.
24 See 18 U.S.C. § 2711 (4).
25 See *https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf*, last visited on [2021-01-07].
26 See Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, April 2019, *https://www.justice.gov/opa/press-release/file/1153446/download*, last visited on [2021-01-07].

To alleviate the legal conflicts that service providers may face under the data controller doctrine, the CLOUD Act also specifies the circumstances under which service providers may dispute the orders: if service providers can reasonably prove that the subject of investigation is not a U.S. person and does not reside in the United States and that the disclosure will expose them to a substantial risk of violating the laws of a "qualifying foreign government," they may file a "motion to quash or modify the enforcement order" with the court.

The CLOUD Act recognizes the court's discretion in considering data access requests and defenses by following a comity analysis. The CLOUD Act defines the factors for comity analysis: (1) the interests of the United States; (2) the interests of the qualifying foreign government in preventing any prohibited disclosure; (3) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider; (4) the location and nationality of the subscriber or customer whose communications are being sought, and the nature and extent of the subscriber or customer's connection to the United States; (5) the relationship between the service provider and the United States and the nature and extent of its activities in the United States; (6) the importance to the investigation of the information required to be disclosed; (7) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences. In summary, the CLOUD Act attempts to address the legal conflicts faced by MNCs by balancing competing interests and following the rule of proportionality.

FOREIGN GOVERNMENTS' ACCESS TO DATA IN THE UNITED STATES

The CLOUD Act encourages foreign governments to sign executive agreements with the United States (thus "qualifying" them) to access data stored in the United States Then, they can directly issue data access orders to organizations in the United States.

The core criterion for "qualifying a foreign government" lies in "whether its legislation and the implementation of the laws provide robust substantive and procedural protections for privacy and civil liberties." Here, the following factors are considered: (1) whether foreign governments have adequate substantive and procedural laws on cybercrime and electronic evidence, and whether they have acceded to the *Convention on Cybercrime,* or whether they have domestic laws consistent with the definitions and requirements in Chapters 1 and 2 of the *Convention;* (2) whether they respect the rule of law and the principle of nondiscrimination; (3) whether they abide by international human rights protection obligations and commitments and fully respect international human rights; (4) whether there are clear legal requirements and procedures for the collection, acquisition, use and sharing of data and the supervision thereof; (5) whether there are sufficient safeguards for the accountability and transparency of data access by other foreign governments; (6) strong commitments to the free flow of information, and to the open, distributed nature and interconnectivity of the Internet.

Orders issued by "qualifying foreign governments" directly to the U.S. organizations are subject to strict limitations. For example, data related to the prevention, investigation, and prosecution of serious crimes, including terrorism, shall be limited to specific individuals, accounts, addresses, or personal devices and subject to review by courts or other independent agencies.

The Essence of the U.S. Model

On the "taking" side, the CLOUD Act follows the controller doctrine and, in effect, allows the U.S. government to directly access data globally through the U.S. data controller. The service provider is allowed to raise a defense only when the data is related to a non-U.S. person in the United States, subject to U.S. courts' discretion. Given the United States' expansive global Internet business and the intricate mechanisms provided by the CLOUD Act, the U.S. government can easily access data stored overseas, effectively extending its jurisdiction to other countries. On the "blocking" side, the CLOUD Act addresses concerns raised by the SCA. The law only authorizes qualifying foreign governments to directly retrieve data from service providers under specific conditions. In this way, the United States assumes absolute control over the data held by enterprises governed by U.S. law. Any foreign governments wishing to request data directly are forced to abide by the U.S.-style human rights principles and basic privacy protection safeguards and give the U.S. government reciprocal treatment.

The design of the "taking" vs. "blocking" mechanism in the CLOUD Act allows the U.S. government to convert the enterprises it governs into national territory in cyberspace. U.S. data sovereignty will expand into any country where the U.S. businesses have a presence. Simultaneously, the CLOUD Act allows qualifying foreign governments to "enter" U.S. cyber territory in exchange for the United States "entering" their cyber territory. The CLOUD Act fully considers the United States' industrial advantages and reinforces U.S. supremacy in the international market, maximizing its national interests.

The EU Cross-Border Data Access Model

What is the model for countries that are neither the data storage site nor the data controller's domicile? A typical case is the European Union (EU). The following cases adjudicated in the EU indicate the essence of the EU model: expanding the jurisdiction of the EU's rules beyond its borders and leveraging its single digital market as a bargaining chip to make the world accept the de facto extension of its territory in cyberspace. The EU's expansive jurisdiction over cross-border data access relies on a vast single digital market and a relatively well-off global consumer base of 500 million as a bargaining chip. MNCs have to "voluntarily" play by the EU rules if they decide to enter the EU market.

Judicial Decisions on "Taking"

EXPANDING JURISDICTION OVER DATA CONTROLLERS

The European Union has taken a very different approach to similar data access disputes. In 2010, the Belgium law enforcement authorities requested that Yahoo disclose certain users' identities, such as IP addresses, e-mail addresses, and other identifying information. Yahoo claimed that it is a United States company with no office in Belgium and is not subject to Belgian law. The Supreme Court of Belgium held that an entity "actively treating Belgian consumers as the primary targets of its economic activities," irrespective of the absence of its physical presence in Belgium, shall abide by the disclosure order.[27]

27 See Cass. 18 January 2011, nr. P. 10. 1347. N Vol. 8, *Digital Evidence and Electronic Signature Law Review*, 216, 217 (2011).

The court further noted that the order requiring Yahoo to disclose data did not require the Belgian government to send law enforcement officers abroad or to take substantive action abroad, but rather that Yahoo bring the data into Belgian territory and then disclose it to Belgium authorities. Therefore, the order was not an enforcement action executed abroad and hence did not overstep the territorial limits of jurisdiction. The Belgium courts appear more aggressive than the U.S. courts in *Microsoft Corp. v. United States*

GDPR has instituted the Belgium court's interpretation on jurisdiction as the European Union's official position in similar cases. Article 3 Paragraph 2 of the GDPR provides that the Regulation applies to a data controller or processor with no physical presence in the Union, as long as it offers goods or services to data subjects in the Union, irrespective of whether a payment is required. The European Commission's recent draft *Digital Services Act* follows the same line of thinking.[28] Article 2 of the draft stipulates that even information society service providers without physical establishment in the European Union should also be considered "a provider of services in the Union" and subject to the EU's jurisdiction if they engage in "the targeting of activities towards one or more Member states." Article 31 of the draft further requires that very large online platforms under the Union's jurisdiction shall cooperate with the European Commission in investigation and law enforcement actions and provide the European Commission with data related to their operations.

EXPANDING THE SCOPE OF THE CONTROLLER

The European Court of Justice (ECJ) further expanded the scope of "controller" in the Google Spain case. In this case, Google argued that the indexing on which Google's search engine relies was done by Google's United States headquarters, governed by U.S. law, not EU law. However, the ECJ held that Google Spain was mainly "promoting and selling advertising space provided by the 'United States' Google search engine, carrying out its economic activities towards Spain," and is therefore subject to EU law.[29]

The ECJ's position on Google Spain has further expanded the scope of the "controller." The European Court of Justice did agree that Google U.S. was the data controller in the case, but since the ultimate purpose of Google Spain's activities in Spain was to serve the profits of Google's search engine and Google, Google U.S. should also be "jointly and severally" brought under European jurisdiction due to Google Spain's presence in the EU.

The ECJ's view is also reflected in the GDPR. Article 3 Paragraph 1 of the GDPR stipulates that the Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. As long as jurisdiction is established, member states' data protection agencies naturally have the authority to access data across borders.

28 See EU Commission, the Digital Services Act, *https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN*, last visited on [2021-01-13].

29 See Google Spain SL & Google Inc v Agencia Españolade Protecciónde Datos (AEPD) & Costeja González.

GDPR Provisions on "Blocking"

Before the U.S. Supreme Court hearing of the *United States v. Microsoft Corp.* case, the European Union submitted an amicus curiae brief indicating its attitude towards and requirements for other countries in accessing data within the EU. The European Union believes that the storing of data in data centers within its territory and data transmission from the EU to the United States are data processing acts stipulated by GDPR. The data access request in *United States v. Microsoft Corp.* must comply with the provisions of GDPR Chapter 5, "transfers of personal data to third countries or international organizations."

When analyzing how to apply the provisions of Chapter 5 of the GDPR, the European Union first proposed that Article 48 of GDPR specifically stipulates the circumstances and requirements of court decisions, arbitral awards, and decisions of administrative agencies of third countries requiring data controllers or processors to transfer or disclose personal data, which is, in essence, a form of judicial assistance. At the same time, the provisions of Article 48 indirectly indicate that the legal grounds and circumstances for cross-border transmission stipulated in Articles 45 to 47 of the GDPR do not apply to the access of data by foreign courts or law enforcement agencies. Thus, when judicial assistance is not sought, the cross-border transmission may be possible only through "derogations for specific situations" stipulated in Article 49. Two situations may apply: (1) where the transfer is necessary for important reasons of public interest; (2) where the transfer is not repetitive, concerns only a limited number of data subjects, and is necessary for "compelling legitimate interests" pursued by the controller which "override the interests or rights of the data subject." At the same time, the data controller shall assess all the circumstances surrounding the data transfer and provide suitable safeguards. The controller shall inform both the entity under supervision and the data subject of the transfer. Finally, the European Union held that the derogations provided in Article 49 shall be strictly applied on a case-by-case basis.

The European Union's basic view on cross-border access to EU data is judicial assistance under the data storage site doctrine. "The EU and its member states have signed many international treaties and agreements that can provide judicial assistance to the United States. The European Union hopes that law enforcement cooperation relies on a legal framework that avoids inconsistencies of laws and is based on continuous dialogue, voluntary cooperation, and respect for each other's fundamental interests in privacy and law enforcement."[30]

The Legislative Proposal on Electronic Evidence

In April 2018, less than one month after the CLOUD Act entered into force, the European Union announced the *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters* (the "legislative proposal on electronic evidence"[31]), which has been regarded by the international community as the legislative plan for the EU version of the CLOUD Act. When commenting on the reasons behind the legislation, besides the objective necessity

30 See *United States v. Microsoft Corp.*, 584 U.S. (2018).

31 See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, *https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN*, last visited on [2021-01-07].

for law enforcement agencies to access data faster than criminals, a top EU judicial official said that the EU hopes to increase its leverage and "we have to agree on the reciprocity with the American authorities."[32]

The content of the proposal affirms previous EU courts' adjudications and the reasoning behind the GDPR. The proposal provides that law enforcement agencies can access the personal data of citizens of any country as long as they are involved in investigating crimes related to the European Union with a minimum penalty of three-year imprisonment. All service providers targeting the EU market shall cooperate with law enforcement agencies in providing data. In retrieving data stored abroad, the said data shall be provided to the member state issuing the order, as long as the judicial authority issuing the order for the retrieval of evidence has jurisdiction over criminal investigations and the service provider does provide services to EU residents (whether or not a branch has been established in the EU). Concerning conflicting laws, the European Union adopts a similar approach to that of the CLOUD Act, allowing service providers to file a motion to quash the transfer order, followed by comity analysis by the member states' courts.

The Essence of the European Union Model

On the "taking" side, the European Union largely adopts the data controller doctrine but applies two measures to address data controllers outside the EU: (1) the overseas data controller shall accept EU jurisdiction if it knowingly provides services in the EU; and (2) the data controller and its branches that are seen as closely connected and the overseas controller which performs the processing per se shall accept EU jurisdiction when their EU branches engage in activities in the context of processing taking place outside the Union. As a result, the European Union has extended its de facto territory in cyberspace. On the "blocking" side, the European Union adheres to the concept of territory and insists on an extended territory through expansive interpretation. In summary, between taking and blocking, the European Union has extended its territory in cyberspace well beyond its geographical territory. The EU's sovereignty covers as much territory as it claims in cyberspace.

The China Cross-Border Data Access Approach

In sharp contrast to the "aggressive" stance of the United States and Europe, China adheres to the principle of sovereignty in a traditional geographical jurisdiction sense and emphasizes that cooperation among sovereign states should be the way to resolve extraterritorial matters.

China's Legal Framework for Cross-Border Data Access in Law Enforcement

China has always stressed that foreign authorities should respect China's national sovereignty in requesting data and the only channel for doing so is judicial assistance. This is why China refused to accede to the *Convention on Cybercrime*. Article 32 of the *Convention*

32 See Julia Fioretti, Europe Seeks Power to Seize Overseas Data in Challenge to Tech Giants, Reuters, 26 February 2018.

provides for the method of directly obtaining overseas electronic data evidence through the Internet, which China regards as a violation of other countries' sovereignty. To safeguard national sovereignty and security, China has always refused to accede to the *Convention* and chose to promote a new international treaty on cybercrime at the United Nations level.[33]

Before enacting the *Law on International Criminal Judicial Assistance,* the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security jointly handled the collection of evidence in foreign-related criminal cases based on electronic evidence procedures and judicial interpretations related to cybercrime. In 2005, the Ministry of Public Security issued provisions on "remote inspection" in the *Rules for Computer Crime Scene Inspection and Electronic Evidence Inspection*. In 2014, the three agencies mentioned above jointly issued the *Opinions on Several Issues Concerning the Application of Criminal Procedures in Handling Cybercrime Cases,* specifying that if it is impossible to obtain the original storage media located abroad, electronic data may be extracted. In 2016, the same three agencies jointly issued the *Provisions on Several Issues Concerning the Collection, Extraction, Examination, and Judgment of Electronic Evidence in Handling Criminal Cases,* in which Article 9 authorizes the public security authorities to extract electronic evidence through the Internet when it is impossible to seize the original storage media located abroad and to verify and validate the evidence remotely. The contents of these documents are materially similar to the provisions of Article 32 of the *Convention on Cybercrime,* which indicate inconsistency in the stance between China's practicing authorities and its diplomatic agencies.[34]

In October 2018, the *Law on International Criminal Judicial Assistance* was ratified, bringing China's foreign-related criminal judicial assistance into a law-based framework. As far as cross-border data access is concerned, Article 4 of the law stipulates: "Without the approval of the competent authorities of the People's Republic of China, institutions, organizations, and individuals within the territory of the People's Republic of China shall not provide evidence materials and assistance stipulated in this law to foreign countries." In its explanation, the National People's Congress explicitly mentioned that the article was added to resist foreign "long-arm jurisdiction" requirements in response to the practice of foreign judicial and law enforcement agencies requiring relevant assistance from institutions, organizations, and individuals within the territory of China without the permission of the competent authorities of China.[35]

Shortly after adopting the *Law on International Criminal Judicial Assistance*, the Ministry of Public Security issued the *Rules for the Collection of Electronic Data Evidence by Public Security Agencies in Criminal Cases*. Compared with the normative documents released by the three agencies above, the biggest difference in the Rules is the absence of the word "overseas," which has led to a controversy over whether the Rules do not provide for the collection of "overseas" electronic data evidence or prohibit the collection through unilateral means. A systematic reading and analysis of the Rules' structure and specific

33 See Shengjian Hu & Zhixiong Huang, The Predicament and Prospect of the International Law Mechanism of Combating Cybercrime: From the Perspective of the Council of Europe Convention on Cybercrime, Vol. 6, *Chinese Review of International Law* (2016).

34 See Kun Liang, Reshaping the System of Cross-Border Remote Electronic Forensics, Vol. 2, *Global Law Review,* (2019).

35 See Report of the Constitution and Law Committee of the National People's Congress on the Outcome of the Deliberation of the Law of the People's Republic of China on International Criminal Judicial Assistance (Draft), *http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-10/26/content_2064519.htm*, last visited on [2020-09-30].

provisions indicates an amendment to and abolishment of the provisions of the three agencies mentioned earlier on remote verification and validation of data stored abroad. On the one hand, the Rules comprehensively regulate the collection of electronic data evidence in criminal cases, with chapters covering the full process and every aspect of the collection of electronic data evidence, making it difficult to surmise that the Rules intentionally overlook the practice and norms of collecting overseas electronic evidence. On the other hand, Article 23 of the Rules explicitly refers to the restrictions of "domestic" data, which indicates that the Rules have considered the issue of cross-border data access. The reason why overseas data is not mentioned is that the Rules amended the practice and norms of collecting electronic data evidence in criminal cases in previous laws and regulations, so the new framework is well within the scope of the *Law on International Criminal Judicial Assistance*. In the meantime, Article 61 of the Rules specifically points out that "if documents previously issued by the Ministry of Public Security are inconsistent with this Rule, the provisions in this Rule shall prevail," which indicates that the new rules represent China's latest position and requirements of collecting electronic data evidence.

China's Basic Stance

China's basic position on cross-border data access in law enforcement prohibits the violation of sovereignty and insists that legislation, legal practice, "taking" or "blocking" actions should rely on equal and mutually beneficial cooperation between sovereign countries. In July 2020, the *Data Security Law (Draft)* was released for comments. Article 33 of the law is in line with Article 4 of the *Law on International Criminal Judicial Assistance*. Although the law has not been formally passed, it shows China's adherence to the above-mentioned basic position. In short, China takes a "defensive" stance on cross-border data access and tries to balance national sovereignty, security, and development interests, while giving greater weight to national sovereignty and security interests.

Deduction and Analysis of the Interaction of the Three Data Access Models

At present, the United States and the European Union have adopted the "expansion" model of cross-border data access, while China has adopted a "defensive" model to counteract the "long-arm jurisdiction" of the United States and Europe. To what extent is such interaction consistent with China's sovereignty, security, and development interests?

First, when the United States and Europe expanded their jurisdictions beyond traditional geographical borders while China upholds it, it is necessary for China to adhere to or take more "defensive" measures: In addition to requiring organizations or individuals located in China to obtain the approval of competent authorities before responding to the cross-border data access requests of overseas law enforcement authorities, China can further ensure that foreign-funded organizations or individuals cannot become data controllers in the first place as legally defined by U.S. and European laws. Take cloud service as an example: Foreign cloud service providers such as Microsoft and Amazon entered China's market under technological cooperation frameworks. Following passage of the CLOUD Act, China's approach is seen as an effective way to ward off the United

States' and Europe's long-arm jurisdiction because neither Microsoft nor Amazon controls the data. The strict control of the examination and approval of domestic enterprises' responses to cross-border data access applications in effect exerts pressure on the competent authorities. To tweak the definition and standards of data controller through legislation or supervision seems like a more effective and convenient way. Following this logic, the cloud service model should be extended to all businesses that may involve cross-border data access by the United States and Europe. However, there are spillover effects such as violating China's policy of deepening reform and opening up and lifting market access restrictions for overseas entities, and giving foreign governments and enterprises additional excuses to criticize China's "protectionism."

Second, parties that take an "offensive" posture are more likely to reach a compromise, as the European Union stated—it intended to achieve reciprocity with the United States when it put forward its legislative proposal for electronic evidence. Following passage of the CLOUD Act, the United Kingdom has reached a bilateral agreement with the United States under the framework of the CLOUD Act, and Australia is also actively negotiating with the United States. Once more countries negotiate and reach compromises with the United States, forming a broader agreement, China may be excluded from the rule-making club, and its demands would not be heard, causing greater political pressure on China. At that time, China's defensive measures will be unsustainable, or may have to be increased again.

Finally, the overseas businesses of Chinese ICT companies may face difficulties. When conflicts between "taking" and "blocking" get more heated, Chinese ICT companies will face more cross-border law enforcement and data access challenges. Their optimal strategy for avoiding legal liabilities is to segregate the products into a Chinese version and an overseas version, storing data locally in each jurisdiction and disallowing users in the jurisdiction of one version from registering in the other, as seen by Tencent's WeChat and TikTok under Bytedance. This strategy's outcome is the failure to "deploy globally," preventing Chinese ICT companies from upgrading services by using a global data pool and limiting the gains from economies of scale. Once the United States and the European Union reach an agreement, at least their enterprises can avoid data localization and segregated operations, which will put Chinese ICT enterprises at a disadvantage.

Because of this, defensive strategies may not be the best way out. China should mitigate the pressure of unilateral response by resorting to a multilateral framework. In his speech at the summit commemorating the 75th anniversary of the United Nations' founding, President Xi Jinping stressed: "Unilateralism is not the way. We must adhere to joint development through sharing and consultation. All countries should jointly safeguard universal security, share development achievements, and determine the future of the world." The mechanism of cross-border data access should be designed in the same spirit. Each country has its core values and choices, and any solution should have mutual respect for sovereignty as a pre-condition. At the same time, in today's globalized digital service market, this critical issue is not only about the efficiency differential between law enforcement and criminal acts, it is also about the global operation of Chinese and overseas MNCs. No country can deal with the challenge alone. The solution to balancing local and extraterritorial interests relies on international cooperation. China's recent proposal on a "global data security initiative" is an effort in this direction.

Given the global political situation today, it is difficult to set up a reasonable order and sound rules quickly on issues of global governance of the Internet, including cybersecurity and cross-border data flows. At this moment, China can start exploring multilateral (such as the "the Belt and Road Initiative") or bilateral schemes (such as clarifying the cross-border investigation procedures recognized by both sides). On this premise, China can upgrade and transform judicial assistance treaties, improve collaboration efficiency, and respond to judicial assistance requests to the best of its ability. This may ease the pressure on Chinese ICT companies with a global presence and protect their interests.

To counter the expansive legislation by the United States and Europe, China may stress data security in dealing with the cross-border transfer of data. The *Data Security Law (Draft)* and the *Personal Information Protection Law (Draft)* made it clear that relevant organizations and individuals can provide data stored in China to overseas law enforcement agencies upon the competent authorities' approval. In the follow-up legislative process, it is also necessary to clarify the specific legal procedures and time limits in application, examination, and approval, and the relationship and coordination between the security assessment of outbound data transfer and the legal liabilities for violating such obligations. At the same time, the competent authorities should uphold the underlying principles but allow room for flexibility, protecting China's data sovereignty while mitigating the adverse effects on the overseas interests of Chinese ICT companies.

Summary: Data Sovereignty—an Evolving System

China has chosen to uphold the traditional concept of sovereignty in cross-border data access, based on the overall international situation and the need to safeguard China's overall sovereignty, security, and development interests. It is natural for China to defend against interference in China's internal affairs and infringement of its sovereignty. Given the uniqueness of the digital economy, while subjecting sector-specific interests to overall national interests, can China strike a balance between old principles and flexibility and smartly safeguard data sovereignty?

Unlike physical territories, data inevitably flows across borders. The country that attracts more data flows controls more data. Therefore, data sovereignty is more than a government's control over data within its jurisdiction. It must also enhance the capability of a country (including organizations and individuals under its jurisdiction) to access, process, and utilize data (local and extraterritorial). To safeguard data sovereignty, China should also consider how to enable Chinese enterprises to access and utilize more data globally. After all, the United States can extend its "arm" because its enterprises are all over the world.

It is time to broaden the scope of data sovereignty. While adhering to the traditional concept of sovereignty and multilateralism, in the digital era, China needs to establish a good data flow order for Chinese ICT companies with global business and "globally integrated operations." It is a critical component in the design of China's model of cross-border data access.

This article is the research result of a special project entrusted by the Ministry of Justice in 2018—"Big Data and Cybersecurity Legislation" (18SFB1005)—in which the author participated.