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

THE CROSS-BORDER DATA FLOWS SECURITY ASSESSMENT: An important part of protecting China's basic strategic resources

by Yanqing Hong
Peking University Internet Development Research Center

Working Paper
June 20, 2017

FOREWORD

In late May China's government issued an important document associated with the new Cybersecurity Law that went into effect on June 1. The *Measures on the Security Assessment of Cross-Border Transfer of Personal Information and Important Data (revised draft)* will not go fully into effect until December 31, 2017, and they remain a work in progress. Nonetheless, they have already generated considerable concern and confusion among data-centric foreign and domestic businesses operating in China.

Concerns center around what new obligations the Measures will impose on those transferring different categories of data in and out of China. The prolonged drafting process, and the changing and often vague language of the Cybersecurity Law and the Measures before implementation, have contributed to the uncertainty experienced by a variety of actors.

The author of the accompanying essay, Dr. Yanqing Hong, is the research director at the Internet Development Research Institute at Peking University and an expert in legal issues related to data protection, cross-border data flows, and cybersecurity. He also leads the personal data protection project for the National Information Security Standardization Technical Committee of China (TC260) and is deputy head of the task force for the *Guidelines for Data Cross-Border Transfer Security Assessment*. Those Guidelines are designed to provide businesses with a means to assess whether their practices meet the requirements under the Measures for protecting personal data and a new category called "important data."

Hong is thus positioned to provide rare and authoritative insights into the way China's regulators understand and plan to operationalize the sometimes murky language of the Cybersecurity Law and the Measures. In this essay, Hong attempts to clarify some of the confusion about the meaning of important data, how companies should interpret the self-assessment clauses of the Measures, and the intent of the new rules. He argues that China is, along with many countries, grappling with new challenges that have emerged with the era of big data, and that the cross-border data flows framework in the Cybersecurity Law and the Measures is not intended to disrupt the business operations of multinational firms but instead to ensure any risks to national security, the public interest, or personal data protection are addressed before data is transferred out of China. Hong focuses on the balance China's government is trying to achieve between security and development in the realm of data, and his explanation of the rationale for the requirements in the Measures on self-assessment, as well as the relationships between different types of data and interests, provide an authoritative and balanced view.

This short essay was translated from an op-ed Hong was invited to contribute for the June issue of the prominent Chinese cyberspace policy journal *China Information Security*, coinciding with the implementation of the Cybersecurity Law. We are now also working to translate and adapt a full academic article, with citations, by the author on this same topic, in which he articulates the approach he believes the Chinese government should take in regulating cross-border data flows—an approach that in large part reflects that adopted by the Chinese government.

We modestly hope that the authorized and collaborative translation and publication of this essay will contribute to a much-needed understanding of a key element of China's emerging cybersecurity and data protection framework moving forward.

This publication is also an outcome of a new trilateral U.S.–China–EU project co-founded by Hong, Rogier Creemers of the University of Leiden, and Graham Webster of the Paul Tsai China Center to chart the direction of each jurisdiction's digital policies from the perspective of both differing and common interests. The authors of this foreword are also developing a new effort and platform to increase international understanding of China's digital policies.

Rogier Creemers
University of Leiden

Paul Triolo
Eurasia Group

Graham Webster
Yale Law School

THE CROSS-BORDER DATA FLOWS SECURITY ASSESSMENT: An important part of protecting China's basic strategic resources

by Hong Yanqing

INTRODUCTION

"Data has become a national basic strategic resource." This is the common understanding of the two basic official documents which are guiding China's future economic and social development: the *Action Plan to Promote the Development of Big Data* and the *13th Five-Year Plan*. The *Action Plan to Promote the Development of Big Data* also further states that "big data is increasingly affecting global production, circulation, distribution, consumption activities, and economic operating mechanisms, social lifestyles, and national governance capacity."

In fact, in the regulations and documents issued by the State Council and various ministries of China, only data (and big data), and archive files are eligible to be called "basic strategic resources." The label of "strategic resources," however, has been attached to land, grasslands, rare earths, oil, natural gas, food, water, forests, minerals, coal, and so on. Literally, the addition of the term "basic" necessarily makes data more important. This elevated designation of data reflects that the Chinese government and leadership have put data in a high position and developed a profound understanding of its role in China's future. But this contrast also highlights a grim reality: China's rare earth, oil, natural gas, minerals, forests, and other strategic resources have been supported by the establishment of a relatively mature protection system, whereas China clearly has not yet formed a protection system that is scientific, comprehensive, and commensurate with data's elevated importance.

President Xi Jinping has repeatedly stressed on many occasions, "cybersecurity and informatization are one body with two wings, with two driving wheels, and

there must be unified planning, unified deployment, unified promotion, and unified implementation." Therefore, in accordance with the *13th Five-Year Plan*, when "fully implementing the promotion of the big data development initiatives and accelerating the sharing of data resources and development of applications, to assist in industrial transformation and upgrading, and in social governance innovation," China's government must face as a top priority how to effectively protect data, a valuable national basic strategic resource.

With the official start of the implementation of the Cybersecurity Law on June 1, 2017, the basic framework of China's cybersecurity work and the work priorities for cybersecurity have been clearly defined. And specific to the issue of data security protection, Article 37 of the Cybersecurity Law has very specific provisions for establishing a personal information and important data outbound flow security assessment system. This paper will focus on how to understand this as an institutional innovation, and how the implementation of this system has great significance for the construction of China's protection of data resources.

THE CYBERSECURITY LAW'S THREE-TIERED DESIGN ON DATA

The provisions of the Cybersecurity Law on data can be divided into three levels according to their different dimensions of protection. This is shown in the table on the following page.

First, protecting data's confidentiality, integrity, and availability (CIA). This is the CIA triad of traditional information security. In the general provisions section Article 10 of the Cybersecurity Law, this is made clear. Article 21 specifies the security obligations of network operators (including the operators of critical information infrastructure), and clearly states the requirement to prevent the disclosure or theft of network data. Article 31 defines the scope of critical information infrastructure from the point of view of the possible harm of data disclosure in CIA terms.

Second, personal information protection. The Cybersecurity Law not only inherited the main clauses of China's existing laws on the protection of personal information, but also creatively added some provisions in accordance with the characteristics of the new era, development requirements, and protection concepts. For example, Article 40 clarifies that network operators who collect and use personal information are the foremost responsible agent with the responsibility for the protection of personal information. Article 41 adopted the data minimization principle. Article 42 added the conditions under which personal information can be shared and traded, namely with explicit consent and anonymization. Article 43 added the right of the individual in certain circumstances to delete or correct

Scope	Cybersecurity Law article
Data security	Article 10: "Protect the integrity, confidentiality, and availability of network data."
	Article 21: "Prevent the leakage or theft, and altering of network data."
	Article 27: "Do not supply for special use in… stealing network data, etc., software or tools that harm network security activity."
	Article 31: "As soon as damage, loss of function, or data leakage occurs to critical information infrastructure, that can seriously damage national security, the national economy, or the public interest."
Personal data protection	Articles 40 to 44
National-level data protection	Article 37: "personal information and important data collected and generated by critical information infrastructure operators operating within the borders of the People's Republic of China should be stored within China."
	Article 51: "National cybersecurity and informatization departments should plan and coordinate with relevant departments to strengthen cybersecurity information collection, analysis, and reporting work."
	Article 52: "Departments responsible for critical information infrastructure protection work should…according to regulations report cybersecurity inspection and warning information."

their personal information. Article 44 provides, at the level of law, legal space for information transactions for the first time. It can be said that the five provisions on personal information, focusing on the protection of information autonomy and control over an individual's own information, and the article-by-article innovations, mean that there is conceptually and in principle a comprehensive convergence with existing international rules and those of the United States and Europe in terms of legislation to protect personal information.

Finally, data protection at the national level. Articles 51 and 52 have provisions for cybersecurity (threat) information, requiring that national cybersecurity and informatization departments and other relevant departments strengthen the collection of cybersecurity information, and requiring critical information infra-

structure security protection departments to submit cybersecurity information in a timely manner. This means that for cybersecurity information (a type of important data in the sense of Article 37), including cybersecurity information held by private sector departments, the Cybersecurity Law gives relevant national departments a clear mandate and strong powers to collect and analyze the information. And Article 37 requires that the personal information and important data collected and produced by the operators of critical information infrastructure within the territory of the country shall be stored within China. To send personal information and important data abroad, it is necessary to first go through a security assessment.

In short, the requirements of the Cybersecurity Law on data can be summarized as follows:

- Data Security = Confidentiality + Integrity + Availability
- Personal Information Protection = Data Security + Basic Principles on Personal Information Collection and Use (legality, justification, necessity, transparency, etc.) + The Individual Right to Delete or Correct
- National-Level Data Protection = Data Security + Control Over Important Data + Cross-Border Transfer Security Assessment

AN ACCURATE UNDERSTANDING OF THE MEANING BEHIND THE TERM 'IMPORTANT DATA'

Before discussing the data outbound security assessment system proposed in Article 37 of the Cybersecurity Law, it is necessary to focus on the concept of "important data."

On November 7, 2016, when the Cybersecurity Law was passed by the National People's Congress (NPC), the word "business" was removed from the phrase "important business data," which had appeared in the third draft. This small but significant change actually reflects the legislators' last-minute considerations: The conception of important data is aimed at the interests that are at national and societal levels—that is, to protect national security, the population's livelihood and wellbeing, and the public interest. Therefore, as long as the network operator's data does not implicate the national and societal levels of interests, then it does not belong to the category of "important data." For example, the transcript of an executive meeting of an Internet company is very important to the company itself, but if it does not involve the state or the public interest, the transcript as such obviously does not belong to the "important data" category. Such data can be freely sent out of the country. However, for a company that produces combat readiness materials, the import and export records of its information systems, the level of inventory, etc., may involve national security

matters, and should be identified as "important data." The Cybersecurity Law requires a security assessment of this type of data before it leaves the country.

The change from "important business data" to "important data" indicates that the Cybersecurity Law is going beyond the relatively familiar classification method of "personal data, business data, and national data," and is proceeding from the value of the data. In other words, whether it is personal data or business data, as long as it may endanger the national and societal level of interests, it will be identified as "important data." Therefore, in the recently published *Measures on the Security Assessment of Cross-Border Transfer of Personal Information and Important Data (revised draft)* (hereinafter referred to as the Measures), important data is defined as "data closely related to national security, economic development, and the society's public interests." The drafted national standard *Guidelines for the Cross-Border Data Flows Security Assessment* provides examples and identification guidelines for important data in the appendices.

To sum it up in one sentence, the introduction of the concept of "important data" in essence serves the objective need to protect national security and public interests in the big data era, and on the national level it is a natural response to the particularities of data security protection in the big data era. In the past, the classifications of "personal data, business data, and national data" had some meaning, because often only data controlled by the state could affect interests at the national and societal level. But in the big data era—when data collection, aggregation, transmission, etc., are widespread outside the public sector—many private businesses control vast amount of data resources. These data may have already influenced national and public interests. For instance, the huge amount of user information held by Alibaba, currently covering over 400 million users, is certainly personal information and business data—but because of its scale and granularity, it can also match the public security organs' basic national population database and even surpass it in accuracy. For the country, any eventual leak or damage of this scale of basic population data could create a serious threat to national security.

The same goes for data produced through network security protection processes for critical infrastructure—including system structure, security protection plans, tactics, implementation plans, and vulnerabilities—in industries like finance, energy, transportation, telecommunications, etc. Even though these data are in the hands of private cybersecurity service providers, any leak of these data would substantially increase the cybersecurity threats to critical infrastructure. Therefore, from a national perspective, these data certainly constitute "important data," even if held in the private sector. To sum up, determining what constitutes "important data" requires us to stop judging by who holds the data and instead proceed by determining what values and interests the data can affect.

SECURITY ASSESSMENT FOR TRANSFERRING PERSONAL INFORMATION AND IMPORTANT DATA ABROAD

The *Measures on the Security Assessment of Cross-Border Transfer of Personal Information and Important Data (revised draft)* (the Measures) have already passed the public comment stage. On May 18–19, the Cyberspace Administration of China (CAC) convened discussions on the Measures with domestic and foreign businesses. Although the final text has not been published, the framework set forth in the Measures will probably not see major changes. The remainder of this essay examines three aspects of that framework.

1. International trends in data exit control measures

First, from a geographical perspective, statistics indicate that more than 60 countries and regions have put forth data exit control requirements. The U.S. Information Technology & Innovation Foundation (ITIF) on May 1, 2017, published a research report on cross-border data flows called "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" The report points out that countries implementing data exit controls can be found on every continent, including developed regions such as Canada, Australia, and the European Union, and developing countries such as Russia, Nigeria, and India. Of course, each country's regulations vary in terms of scope and level of control.

In terms of timing, existing data localization and storage rules have mostly emerged after 2000. The chart below reveals an interesting point: The rise of data localization and storage rules coincides with the development of information technology such as the Internet, distributed systems, cloud computing, and big data. On the one hand, as cloud computing, distributed systems, etc., have been widely adopted, data holders' ability to control data has significantly weakened, and intermediaries have proliferated. In the era when an original copy resided on a single machine, it was quite easy to understand, for instance, how many types or how much data one held, where it resided, and who could access it. Now, those questions are not so easy to answer.

On the other hand, the development of big data technology has greatly increased data holders' demands to control data. If large amounts of data are revealed, whether purposely for open public collaboration or because an information system is breached and its data leaked, they can be used maliciously. For instance, hostile forces could combine the data with other datasets and use various analysis methods such as data mining to gain information that could threaten national security.

From these two perspectives, it is easy to understand that setting up national data exit control measures is to a great extent a response to the above mentioned two dilemmas.

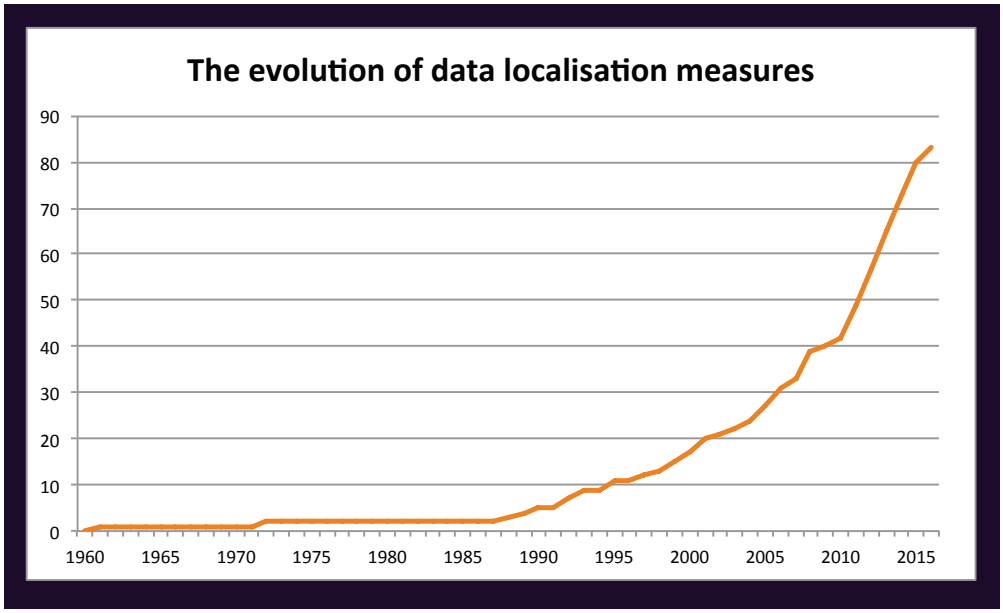

Chart source: Martina Francesca Ferracane, Data Localization Trends, European Centre for International Political Economy, Presentation in Beijing, July 19, 2016

2. Achieving balance between development and security

A fundamental consensus has emerged today that data naturally flows across national borders, that data flows produce value, and that data flows can lead to flows of technology, capital, and talent. Therefore, data flows are the norm, and circumstances where flows are limited are the exception. This is well reflected in the Measures.

First, the Measures conform with basic principles of the exercise of government power: legitimacy and necessity. According to the latest measures, the exit security assessment only assesses threats to security interests at the national and societal level and at the personal level. This is because the individual is vulnerable and constrained in resources and therefore requires legal protection. It is also because national security and public interests are public goods that natural persons and businesses will not voluntarily provide; instead they must depend on government power to produce these public goods. For this reason, the introduction of the newest edition of the Measures clearly states that its goal is to "protect cyberspace sovereignty, national security, and public interests, and to protect

citizens' lawful interests," and the interests of enterprise are not listed. As for the majority of cases today, which involve the transfer abroad of data purely affecting a single business or organization's interests, the Measures do not require undertaking security assessment. Imagine if the data being transferred abroad did not implicate on individual- or national/society-level security interests, but the government still to required businesses to undergo assessment regarding their own interests in commercial secrets, intellectual property, etc. This would not only be unnecessary but also a waste of effort for the assessors. Businesses would think the government regulated too broadly and too much, interfering with the freedom to conduct business. The government might also find they simply do not have the capacity to decide, from a business' perspective, what data most requires protection—a question the business definitely is in better position and has better ability to answer than the government.

Second, the Measures adhere to the principle of self-assessment. When it comes to transferring personal information abroad, individual informed consent is the main approach. With a complete and accurate understanding of the goal, scope, type, and recipient of information to be transferred abroad—as well as of the potential risks—individuals can agree to authorize the transfer abroad of personal information. The Measures also require network operators that are going to export personal information or important data to self-organize or entrust a cybersecurity service entity to undertake data exit security assessment before making transfers abroad. In the circumstance that the transfers could affect national security or public interests, they must directly report the result of the assessment to the sectoral regulators. Once again, the Measures' main goal in restricting data exit is to prevent harm to national security or the public interest, as well as to ensure personal information is not transferred abroad without personal consent.

In summary, the Measures focus on security interests at the national and societal level and specifically seek to eliminate or contain risks related to transferring data abroad. In this way, the Measures successfully achieved a balance between development and security.

3. The scientific design of evaluations

The design of the Measures is both scientific and complete. In accordance with the regulations, the exit assessment first assesses whether the outbound data activities are legally valid and justified, and building on that, there will then be an assessment of whether or not the risks of the data exit plan can be controlled. For the latter, the Measures start from two aspects. One is to assess the properties of the transferred data, that is, borrowing from the traditional risk assessment of the importance of digital assets, including the amount of data, and its scope, type, sensitivity, etc. The second is to assess the possibility of outbound

data security incidents, the assessment of which includes: whether the data sender implemented appropriate outbound data technology and management capabilities; data transmission; whether the data receiver has adequate security capabilities for the data it receives; and the political and legal risks of the country or region where the data receiver is located. By assessing the nature of the data and the likelihood of a security incident in each link, the network operator can estimate the risk of data transfer and take appropriate security measures accordingly. The national standard *Cross-Border Data Security Assessment Guidelines* that is in development right now further elaborates these ideas.

LOOKING AHEAD

The Cross-Border Data Flows Security Assessment, as an important part of the data protection level designed at the national level, is a key step in establishing a comprehensive data resource protection system in China. However, the comprehensiveness of the existing institutional design of the Cybersecurity Law is commensurate with the importance of data, a basic strategic resource designated by the Chinese state. For example, for the right to control important data, the Cybersecurity Law only provides for one type, that is cybersecurity (threat) information. When it comes to preventing the use of malicious data against national security, the Cybersecurity Law also only provides for an outbound security assessment. The Cybersecurity Law is off to a good start, but obviously we also need to develop data security management measures and other measures to make data protection really catch up with the pace of development of big data.

Translated from the Chinese by Graham Webster and Paul Triolo

THE AUTHOR

Dr. Yanqing Hong is the research director at the Internet Development Research Institute, Peking University of China. He focuses on data protection, cross-border data flow, and cybersecurity related legal issues. He now leads the standardization project on personal data protection under the National Information Security Standardization Technical Committee of China, and acts as deputy head of the task force for Guidelines for Data Cross-Border Transfer Security Assessment. He regularly participates in bilateral or multilateral dialogues on cyber related issues, such as China-EU Digital Economy and Cybersecurity Expert Working Group which is organized by the Cyberspace Administration of China and DG Connect of the EU Commission. Before joining Peking University, he worked in the Cyberspace Administration of China on issues relating to international cooperation and cybersecurity. He received his Ph.D. in Law from the School of Law, Utrecht University, the Netherlands.