Hitachi Research Institute Report

Tightened regulations on data distribution and retention in the United States, China, and Europe against the backdrop of competition for data hegemony

Takeshi Matsumoto, Senior Manager, 2nd Research Department

Data has come to be called "the oil of the 21st century" in recent years. The World Economic Forum, which was already aware of the value of personal data in 2011, noted that "personal data is the new oil of the internet and the new currency of the digital world" in its report for the same year, "Personal Data: The Emergence of a New Asset Class", and discussed the high economic value of personal data. In the eight years since then, with the advance in digital technologies such as IoT and AI, it is now recognized that leveraging data on things as well as humans can be a source of economic growth. On the other hand, data on both humans and things can readily be collected via the internet, making it easy for a company to succeed in data enclosure or monopoly as a result. In fact, platform companies like GAFA[1] in the U.S. and BAT[2] in China have grown rapidly through collecting and utilizing personal data. Even at the national level, there are now countries trying to limit the flows of data abroad as much as possible, while facilitating its inflows. This paper discusses the trends in cross-border data regulations in China, the U.S., and the EU from the viewpoint of competition over data hegemony among countries and companies.

1. Increasing Cross-Border Data Flows and Tighter Cross-Border Data Regulations

1.1 Increasing volume of cross-border data flows

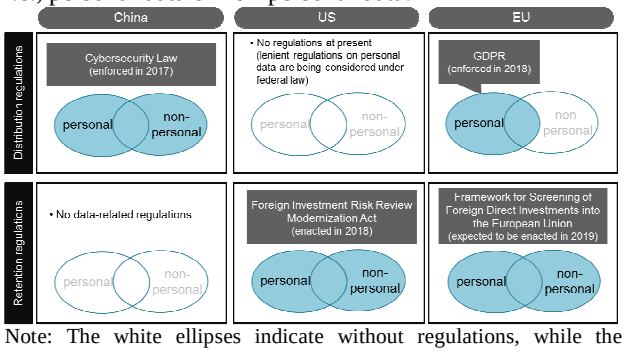
The cross-border movement of people, goods, and money across the world, which had been expanding since the early 2000s with the advance of economic globalization, has stagnated since the financial crisis in 2008, while cross-border data flows have been experiencing explosive growth on the back of the development of the internet, which connects countries, companies and individuals. The total amount of cross-border bandwidth (volume) used increased by about 45 times from around 4.7 Tbps (terabit per second) to about 221.3 Tbps in the 10 years from 2005 to 2014. The increase is particularly remarkable in the three regions of the U.S., Asia, centering on China, and the EU, which have been leading the growth of cross-border data in the world.

Cross-border data can broadly be divided into personal and non-personal data. Personal data includes names and addresses, as well as social security numbers, purchase histories and location information. Non-Personal data includes all data other than personal data, which contains, for instance, industrial data such as design drawings and manufacturing process layouts in the manufacturing industry, and infrastructure-related data, including facility operating information such as traffic and energy information. In recent years, the boundary between the two has become blurred, where data, such as medical history or financial account information, for example, is both personal data and non-personal data at the same time.

1.2 Tighter cross-border data regulations in the U.S., China, and Europe

There is an accelerating trend to place controls over cross-border data, especially in China, the U.S., and the EU, which have been driving the flows of massive amounts of data across national borders. Such control efforts can be classified into regulations for transferring data abroad and those for acquiring and retaining data from abroad. Data distribution regulations require companies to install physical servers within a country in which they must store and utilize data acquired in the country. Data retention regulations, on the other hand, prevent a third-country company from acquiring data that is important to the country in question through direct investment, such as corporate acquisitions.

Figure 1 shows the actual regulations implemented in China, the U.S., and the EU, considering the different means of regulation, i.e., distribution or retention of data, as well as the aforementioned different targets of regulation, i.e., personal data or non-personal data.



Note: The white ellipses indicate without regulations, while the shaded ellipses indicate with regulations.

Source: Compiled by Hitachi Research Institute by referring to various laws and regulations.

Figure 1 Data distribution and retention regulations in China, the U.S., and the EU

[1] An acronym for the four big tech companies of Google, Apple, Facebook, and Amazon

[2] An acronym for the three top Chinese data companies of Baidu, Alibaba and Tencent

The regulations currently in force include China's "Cybersecurity Law", a distribution regulation concerning personal and non-personal data, and the "FIRRMA[3]" of the U.S., a retention regulation concerning personal and non-personal data. In the EU, the "GDPR[4]", which is a distribution regulation on personal data, was enacted in 2018. Further, the "Framework for Screening of Foreign Direct Investments into the European Union" is currently under discussion by the European Parliament, which should come into effect from the spring to the summer of 2019 as EU-wide regulations on personal and non-personal data. The data regulations of each country and region have embedded policy intentions of not only protecting privacy and securing cyberspace, but also ensuring national security and future growth through achieving international data hegemony. In fact, although each set of regulations is equipped with content calling for non-discriminatory application to other countries, the U.S., and the EU, in particular, have a specific country in mind when it comes to their implementation. Starting from Chapter 2, we examine the regulations of China, the U.S., and the EU individually from the perspective of data hegemony.

2. China: Data Distribution Regulations to Keep a Vast Amount of Data under State Control

The Cybersecurity Law, which was implemented by the Chinese government in June 2017, triggered wide international interest in cross-border data regulations. The law defines "critical information infrastructure (CII) operators", which have a particularly large impact on state security, the national economy and public interest among "network operators" who own or operate some type of information system, and requires CII operators to store personal information and "critical data" collected and generated in China within the country. The definitions of "network operators", "CII operators", and "critical data" are not clearly stipulated in the main text of the Cybersecurity Law, and we will have to wait for the enactment of various related regulations, Benho (equivalent to governmental and ministerial ordinances in Japan) and guidelines that are currently being formulated. Still, judging from the draft published for public consultation, it is expected that nearly all companies will be required to store virtually all data, regardless of whether it is personal or non-personal, within China's borders[5]. If it is absolutely necessary to take data out of the country, a company must apply to the competent authority (Ministry of Industry and Information Technology or Ministry of Transport, etc.) for cross-border transfer of the data, and undergo a review process, including a safety assessment. However, it is unknown whether obtaining permission from the authority is possible in actual practice. In addition, personal information cannot be taken out of the country without the approval of the authorities, even if the consent of the individual is obtained. This is a critical difference from the EU's GDPR, which allows the transfer of data across borders with individual consent. Accordingly, it can be said that data in China is placed under state control through the Cybersecurity Law.

In the past, the Chinese government believed that data should be freely distributed in order to leverage it. Thereafter, however, with the spread of the internet within the country, China started pursuing the "Internet Plus" initiative as a national strategy in 2016, linking internet technologies (mobile internet, cloud computing, big data, IoT) with industrial systems, including manufacturing, medical care, and logistics, in an attempt to achieve economic growth. The Chinese government explains that the Cybersecurity Law aims to prevent cyberattacks against, and intrusion into, government and corporate networks and control/management systems to maintain cyberspace security. This may be one of the reasons for placing data under its control, but there seems to be a deep-rooted desire to manage and utilize the data generated in the huge Chinese market personally, as opposed to by other countries, with the idea of such vast amount of industrial data generated by the Internet-Plus initiative being the very source of growth. Article 1 of the law, which states "safeguard cyberspace sovereignty", is an excellent example of this.

3. The United States: Strengthening Data Retention Regulations with a Focus on the Policy toward China for National Security

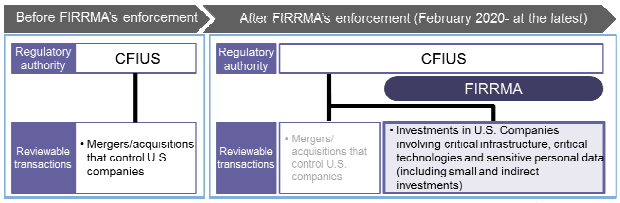
Since 1989, the U.S. has restricted inward foreign direct investment (FDI) primarily for national security, particularly to protect the country's defense industry, and CFIUS[6], a cross-agency body, has been undertaking the actual review. Although the overall framework of this regulation remains unchanged, FIRRMA, which was enacted in August 2018, expanded the scope of transactions reviewable by CFIUS to include investments involving the acquisition of data with national security concerns. Figure 2 shows the transactions subject to CFIUS's review prescribed by FIRRMA, which now specifies three new categories: critical infrastructure, critical technology, and sensitive personal data. As for critical infrastructure and critical technology, they are assumed to cover non-personal data, such as infrastructure facility layout data and failure data, as well as design and experimental data, including data on automated operation for critical technologies.

[3] FIRRMA: The Foreign Investment Risk Review Modernization Act

[4] GDPR: General Data Protection Regulation

[5] With regard to "critical information infrastructure operators", while Article 37 of the law cites the industries in which they are located, including telecommunications, finance, energy, water, and transportation, the list is not exhaustive, and there is a chance that a wider range of industrial sectors will be covered by applying "Security Controls of Critical Information Infrastructure (draft for consultation)" and laws and regulations. In the "Guidelines for Data Cross-Border Transfer Security Assessment (draft for consultation)", the scope of data falling under "critical data" is broadly defined to include data in all 27 sectors, such as the electricity, transportation, and electrical and electronics industries.

[6] CFIUS: Committee on Foreign Investment in the United States



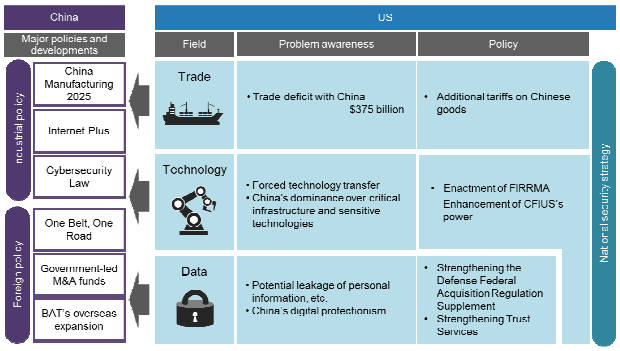
Source: Compiled by Hitachi Research Institute by referring to various sources.

Figure 2 Transactions subject to CFIUS's review prescribed by FIRRMA

In strengthening data retention regulations, the U.S. appears to have China in mind as a country against which it should take security measures. The U.S. government has been dealing with data acquisition by Chinese companies as a national security concern, with its disapproval of Tencent's investment in German HERE Technologies (digital mapping services) in 2016, and also Ant Financial's acquisition of U.S. MoneyGram (international remittance services) in January 2018. While both of the above cases were the government's response in implementing the regulation before FIRRMA's enactment, it should be noted that, from a security perspective, FIRRMA's implementation has disciplined the U.S. government's stance on strictly examining inward FDI involving the acquisition of data.

It should also be noted that data retention regulations under FIRRMA constitute an important component of the comprehensive policy of the U.S. toward China. In the U.S., there is a basic view that national security is guaranteed by broad predominance over the economy, trade, technology and data, not just by military strength. Figure 3 summarizes China's major policies and developments, and the corresponding U.S. policy toward China. In recent years, China has increasingly enhanced its international presence through strengthening industrial policies such as China Manufacturing 2025, and the Internet Plus and Cybersecurity Law discussed in Chapter 2, as well as external policies reflected in the One Belt, One Road initiative. Further, it is clear that the U.S. regards such developments in China as a threat to its national security[7]. In trade, for example, while the U.S. imposed additional tariffs one after another in 2018 against the backdrop of its trade deficit of $375 billion with China, its motivation behind these tariffs was not merely to rectify trade imbalances but to ensure security by protecting its industrial base known as intellectual property, as suggested by the fact that China's infringement of intellectual property rights was cited as the reason for the tariffs. For data as well, concerning information leakage caused by the use of Chinese telecommunications equipment among U.S. government agencies, in addition to the regulations on inward FDI under FIRRMA, the U.S. tightened the Defense Federal Acquisition Regulation Supplement and prohibited government procurement of such equipment. As the confrontation between the U.S., and China is expected to continue for a long time, the United States will further strengthen its data retention regulations with China in mind.

[7] The U.S. government's assessment of the Cybersecurity Law is discussed by Mr. Lundell and others in a paper presented hereafter in this journal.



Source: Compiled by Hitachi Research Institute by referring to various sources.

Figure 3 Major policies and developments in China, and the U.S. policy toward China

4. EU: Confining the Region's Data Location through both Distribution and Retention Rules

4.1 The GDPR retakes data sovereignty from U.S. companies and returns it to EU citizens

Under the GDPR implemented in May 2018, the EU regulates the distribution of data. In principle, the regulation bans the transfer of personal data outside the EU while ensuring the free movement of such data. Since the content of the GDPR has already been explained in many texts, this paper omits an explanation thereof. However, under its basic principle of protecting the fundamental rights of individuals, it strictly defines clarification of the individual rights with respect to the use of data by businesses, as well as setting high penalties for violations by businesses.

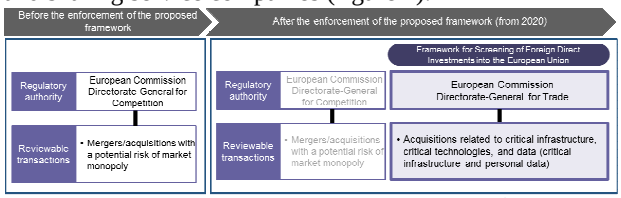
While the GDPR is primarily aimed at protecting the individual rights, its implementation appears to intend to restrain GAFA, U.S. platform companies that have expanded their services in the EU. On May 25, 2018, when the GDPR went into effect, a French nonprofit privacy protection organization filed a suit against Google and Facebook, accusing them of forcing individuals to consent to the use of their data. The French supervisory authority for data protection launched an investigation into this matter. Further, in January 2019, for the first time since the regulation took effect, Google was fined 50 million euros (approximately 6.2 billion yen) for violating the GDPR. This is a move to retake the EU's data sovereignty, which emphasizes that the data of EU citizens belongs to the EU, not to American companies.

4.2 Draft framework for inward FDI screening with China in mind

In the EU, the European Parliament is considering the introduction of data retention regulations concerning both personal and non-personal data. They are referred to as the "Framework for Screening of Foreign Direct Investments into the European Union" and will have the same regulatory details as FIRRMA in the U.S.

While the EU has been preventing company acquisitions by foreign companies via antitrust laws, the scope of application of the laws had been limited to cases where there was a risk of market monopoly. Under the Framework for Screening of Foreign Direct Investments into the European Union, which is expected to be enacted between

the spring and summer of 2019, company acquisitions in the EU will be halted when the EU authorities judge that such FDI poses a threat to EU security, regardless of the risk of monopoly. Each EU member state had similar restrictions on FDI, but this framework allows the European Commission and member states to share information and make decisions. The current draft includes in the transactions subject to screening, company acquisitions that involve the acquisition of data, such as EU citizens' personal information and critical infrastructure data. In the future, the transactions to be screened may include acquisitions of EU companies that own data, such as infrastructure operators, facility maintenance companies, and sharing service companies (figure 4).



Source: Compiled by Hitachi Research Institute by referring to the Framework for Screening of Foreign Direct Investments into the European Union.

Figure 4 Transactions subject to screening prescribed by the Framework for Screening of Foreign Direct Investments into the European Union

The EU's proposed framework targets Chinese companies in particular. In recent years, there has been an increasing number of cases where Chinese companies acquire EU companies, mainly in the high-tech field, with examples including the acquisition of robot manufacturer Kuka AG and semiconductor manufacturer Aixtron SE (both in 2016). As a result, the EU has come to recognize the need to strengthen EU-wide FDI regulations against China in order to ensure defense, military, and economic security, and has started working on the proposed framework[8]. In developing this framework, the European Parliament revised the draft proposed by the European Commission to include data in reviewable transactions, demonstrating the importance the EU places on data protection. The same applies to the case of China, with the proposed framework suggesting that the EU is taking account of investment by not only companies in high-tech sectors, such as robots, but also service companies that handle end-user data, including BAT.

5. Conclusion

While we looked at trends in cross-border data regulations in this paper, a framework to facilitate cross-border data flows has started to be developed and international discussions to that end have begun recently. For example, TPP11, which came into effect in December 2018, incorporates rules on the liberalization of cross-border data flows. Additionally, Japan, the U.S., and the EU have held discussions during the past year at the WTO, and in January 2019, Japan called on 34 willing WTO member countries and regions to draw up specific rules. A joint statement has already been issued confirming the intention to start formal negotiations at the WTO, and it is expected that the rulemaking process will accelerate in the future. The rules under consideration by Japan, the U.S., and the EU would allow the transfer of both personal and non-personal data between countries and regions where data protection is adequate and the mechanisms to collect and use data are reliable, while strictly limiting the transfer of data to countries with those that are inadequate. The rules are thought to have an inherent objective of deterring China, which places data under state control, and in fact, the EU has a policy intention to cooperate with the U.S. in its relations with China, although it feels a threat posed by U.S. companies. As the Japanese government refers to this framework as "Data Free Flow with Trust", it is believed that the international frameworks and rules for digital technology and data distribution in the future will become based not only on the text but also on mutual "trust". To this end, it is important to establish a system to secure "trust" among countries. Expectation is growing for the establishment of a cross-border distribution infrastructure, i.e., having an organization in place to prove the authenticity of data to be distributed and developing a framework for mutual recognition among countries to secure the credibility of the organization.

[8]European Parliament Report in May 2017 "Foreign direct investment screening - A debate in light of China-EU FDI flows"