Who Has Access to Personal Data? Data Transaction Regulations in China

Author Mariko Watanabe

By Mariko Watanabe

Introduction

The leading excellent companies that have emerged from China are active in the field of information technology (IT). Alibaba, Tencent and TikTok are representatives, and they are extremely competitive in utilizing data. Japan, which cannot fully maintain competitiveness in the data technology field, needs to pursue the following targets: first, to invest more to gain competitiveness in this field, and secondly, to commit to the formation of international rules that ensure effective, safe and fair data transactions.

The IT revolution has been progressing in three steps since the 1990s. In the first stage, it drastically lowered the cost of communication via telecommunication technology, such as mobile phones. In the second stage, it reduced the cost of transferring the data information via the Internet.

Currently, it is in the third stage where the revolution is focusing on the reduction of the cost of human transportation, or the cost of face-to-face communication. The outbreak of Covid-19 forced substantial numbers of the world's population to lock down since February 2020 and significantly reduced such communication, encouraging greater use of data transfer instead.

In these circumstances, fully digitalized transactions of data will provide indispensable sources of innovation. Safe and fair use of data depends not only on the technology, but on the institution that governs incentives for those who deal with and handle the data. The incentives are regulated by the institutions concerned.

Accumulation of data may improve the efficiency of its usage, but a monopoly on data may violate the fairness of profit distribution as well as data privacy. We will need laws and regulations determining who should be benefitting from data use and how they should earn those benefits.

In this paper, I discuss the regulatory framework of data transactions, focusing on laws and regulations that governs data transactions in China and the business strategy of Chinese platform firms in the market. This field is at the forefront of technology, not only in China but in the world as a whole, and it is also a field with network externalities, and where only private enterprises may participate. Currently, digital technology from these tech platforms creates and supports offline business and new innovation.

The regulation of transactions involving data is closely related to how to deal with the data which belongs to individuals. Concern is growing about the need to establish ownership of data before allowing cross-border transactions involving it. The handling of personal information by the state and companies must be subject to appropriate restrictions.

In China, the philosophy of protection of personal information which is imposed on platform companies is close to that of Japan and Europe, contrary to the prevailing image. International harmonization of institutions in this area is likely to occur. While the behavior of a state involves questions of sovereignty and direct intervention is difficult, it will be effective to promote harmonization of international rules in this area.

Data Trading Regulations

The issues surrounding international trade in data have changed significantly in recent years.

1. Countering Data Localization

The development of rules for trade via the Internet, called cross-border data transfer or digital trade, has attracted attention as negotiations for the Trans-Pacific Partnership (TPP) have progressed. The TPP provides comprehensive provisions such as non-tariff charges, permission to transfer data across borders, prohibition of computer-related equipment installation requirements, and source code disclosure requirements.

Regulations regarding data localization are broadly divided into (1) restrictions on the transfer of data outside of the country, and (2) requirements for domestic storage of data collected (generated) within the country (*Yasashii Keizaigaku* by Hiroshi Mukunoki, *The Nikkei*, Aug. 30, 2018). A typical example of (1) is the European Union's General Data Protection Regulation (GDPR). The GDPR covers only personal information, and permits data transfer to third countries that have received a "sufficiency certification" that the European Commission recognizes as providing a sufficient level of protection. Japan and South Korea received sufficiency certification in 2018.

In addition to (1), domestic storage (2) is becoming widely imposed now. A typical example is the Chinese cyber-security law. As shown in the next section, infrastructure operators of important information must store any data acquired domestically within the country, and safety assessment is required before moving across borders. China also has several restrictions on data transactions. Not a small number of foreign websites cannot be browsed due to government censorship. Only domestically grown SNS and free Internet calling apps are allowed to be used. In addition, there are various regulatory movements such as requirements of software source code disclosure and controlled acquisition of domains by foreign companies, and its extension to the regulations related to cross-border data transactions (basically, digital protectionism) is a concern.

2. Data Ownership

The next topic is "data ownership". Prior to the enactment of the GDPR in the EU there took place an intensifying debate over the

handling of personal data. Personal information creates new value as data, while maintaining the privacy of individuals must be protected as a basic human right for consumers. In addition, companies such as platforms are processing data provided by individuals to create new value.

If so, the individual should have "data ownership". In addition, in order to facilitate the concept, it is necessary to guarantee "data portability". That is, individuals must be able to exercise their decision-making power over access to data and share it with third parties.

At the same time, platforms or other data processing companies have intellectual property rights to any new product or value that can be created by processing the data. However, the argument that proposes "data ownership" claims that, whoever processes the data and creates value, the data itself belongs to the individual as a basic human right. For example, if a company that owns such personal data goes bankrupt, can you sell that personal data as an asset without permission? The argument is that the individual's consent is necessary (*Economics for the Common Good by* Jean Tirole, Chapter 15, Princeton University Press, 2017).

The idea of "data ownership" is that once frameworks for enabling ownership have been established, data can then be distributed. While the GDPR was criticized for restricting foreign data transfer and incurring additional costs, as shown above, its intention was to enable transfer by establishing ownership. Even in the United States, which was critical of the idea of data ownership, there has been a debate about actively utilizing this idea following the case of Facebook's unauthorized data provision to Cambridge Analytica. Eric A. Posner and E. Glen Weyl, in their book *Radical Markets* (Princeton University Press, 2018), have taken this idea further and argued that individuals should be paid "data dividends". California has established such a system in 2019.

The idea of data ownership and basic human rights is similar to the concept of prohibiting slavery in labor. It is similar to the basic concept that workers have both freedom of movement and freedom of work, but that their rights must be protected by law.

Personal Information Protection Regulations in China

1. Institution

Next we will examine China's policy on data usage and regulations on personal information protection. In China there are (1) policies that promote data sharing and utilization, laws and regulations on (2) protection of personal information, and (3) the disclosure and confidentiality of state and government information. In addition, regarding international transfers, there are (4) laws and regulations in which the state imposes certain restrictions on data transfer.

(1) Policy to promote data sharing. "The plan to establish a social credit system (2014-2020)" is the first comprehensive policy. In its transition from a planned economy to a market economy, Chinese society has experienced difficulties in the issue of trust in economic activity, or what is known as "information asymmetry" in economics; borrowed money was not returned, purchased items were not paid for, and counterfeits were rampant. Implementation of contracts and policies is not fully guaranteed. In order to improve the situation, a system for exchanging credit information and sharing information between financial institutions was begun in the early 2000s.

The social credit system was developed to include the information related to administrative services, industry management, and commercial transactions, etc. The People's Bank of China has established the Credit Reference Center, whereby it aims to share credit information. The goal is to build a database that shares not only creditor information of financial institutions but also information on faulty parties such as unpaid taxes and bad debts.

(2) Protection of personal information. This legal institution has been making progress since 2019. In 2013, the "Regulation on the Administration of Credit Investigation Industry" was promulgated. This is the first Chinese version of the Personal Information Protection Law. When collecting personal information and sharing it with third parties, an entity is called an "information sharing organization" and must comply with this law. If a third-party company wants to use personal information held by platform companies such as Alibaba and Tencent for advertising or other businesses, they must follow this law. In June 2019, a public comment draft of the "Measures for Data Security Management" was submitted to create ground rules for data handling.

(3) Disclosure and Confidentiality of the State. The regulation that requires disclosure and confidentiality of state and government information is the Government Information Management Ordinance (promulgated in 2019), which requires entities to disclose information to government officials. Regulations that act to protect confidential information include the Law of the People's Republic of China on Guarding State Secrets, promulgated in 2010, which forbids the leakage of confidential information, and the National Intelligence Law, promulgated in 2017, which requires all entities in the country to cooperate with the government's information collection, in a way that complies with the law.

(4) Finally, the Cyber Security Law is an example of the state placing certain restrictions on international transfers of data. In April 2020, the Measures on Cybersecurity Review, which provided additional review on import and installment to basic and substantial industries, most of them belonging to the state-owned enterprises, were promulgated.

2. International Data Transfer

Then, based on the legal framework above, how is the handling of personal information regulated?

First, the organization that collects information from individuals and then provides it to third parties is required to protect specific personal information, which is in line with the idea of personal information in Europe and Japan.

Concerning the transfer of information, the consent of the person must be obtained for the most part (Articles 13-17), collection of information regarding religion, beliefs, DNA, fingerprints, blood type, diseases, and medical history are prohibited (Article 13), and the retention of delinquency information has a fixed term (Article 15). For this reason, information sharing organizations should require consent from or notification to the individual in order to share their data with the government. However, it is unclear whether there are laws and regulations that would allow the government to overstep these limitations.

The concept of "data portability" introduced by the GDPR in Europe in 2018 is an effective way of protecting personal information and deterring the harmful effects of monopoly due to the use of tech platform data. However, this "data portability" concept has not yet been introduced in China. In addition, technological innovation has opened

TABLE
Definition & utilization of personal data in China

Definition	**Guideline for Information Safety Technology and Personal Data**
Personal Data	name, status, biometrics, network ID, health, education, property, communication, login record, etc.
Personal Sensitive Data	property, health, biometrics, ID number, network ID, sexual orientation

Utilization	**Data Safety Management Regulation**
Article 27	Network operators need to obtain consent and to notify the information entity, except in these cases: (a) Collecting data via legal open channels, and not clearly against the will of the information entity (b) The information entity voluntarily discloses the data (c) Anonymization (d) Necessity of law enforcement (e) Referring to state safety, public interest or risk of life of the information entity

Source: Compiled by the author

the door to information collection and identification based on facial and figure recognition, etc., but regulations on such data are currently lacking globally. Regulations cannot keep up with the speed of technological innovation.

Regarding the international transfer of data, protections for personal information are required and restrictions on international transfer are provided as part of the protection of personal information (Articles 41 and 76). In addition, censorship and management of "important data" by the government is a feature of China's cyber-security law. The government has the authority to decide what is "important data". Because of this, regulations in China take on a different tone from the European ideas of restricting international data transfer for the purpose of protecting personal information. Finally, data must be stored in China.

From these specific provisions, we can see that private companies such as tech platforms in China are following regulations that are developing into a highly compatible form with European-style data ownership, which regards the protection of personal information as a fundamental right. However, the idea of deterring these platforms' monopoly on data through ideas such as data portability has not yet been introduced. On the other hand, the authority of the state is so strong that the outcome of this issue is unclear.

Open Transaction Strategy of Chinese Platforms

So how is data utilized in China? The market in which Chinese platform companies are active has the following characteristics.

First, digital platformers are playing in a market where only private companies participate. For this reason, there is almost no discrimination due to ownership or competition conditions.

Second, several companies occupy an oligopolistic position because of the nature of the network externality that works more favorably for companies with a large number of users. In particular, mobile payment services have a positive externality that promotes the expansion of economic transactions, and the large number of users in this field is a source of overwhelming strength. Alipay has begun to effectively use its own big data in order to improve the ease of use of mobile payment systems (the "user behavior habit estimation system" started in 2012).

Third, these companies follow the strategy of launching new services openly, while having monopolistic power. In order to popularize new mobile payment services, a strategy to reduce the barriers to entry of users has resulted in a series of innovations that connect online and offline to generate new benefits.

Fourth, data is used as a source of their innovation, but no institutional framework has been developed to make any payments to individuals with data ownership. However, even in Chinese society, there is a growing concern over privacy protection, and calls for restrictions on the distribution of personal information. In 2018, there were two consecutive incidents in which women who joined a dating app, part of a ride sharing app called DiDi, were violated and killed by a driver. In this dating app, the personal information of passengers was widely distributed to drivers, allowing the driver to select his victim and plan his attack. Later, DiDi ceased operation of this dating app. These incidents spark social interest in society regarding the handling of personal information.

Fifth, regarding the relationship to the state, the Regulation on the Administration of the Credit Reporting Industry includes detailed stipulations requiring the consent of the data owner when transferring data to a third party, and the government is not explicitly excluded from this requirement. However, the National Intelligence Law also requires all organizations to cooperate with the state in its information collection, and it is unclear how this will be constrained by the Regulation on the Administration of the Credit Reporting Industry. In China, where administration and political power sometimes act above the law, there are no restrictions on the state giving up protection of personal information. It remains a challenge to find a way to secure the balance between the state's use of personal information and privacy protection through the formation of trade rules. This may lead to greater protection of personal data and the concept of "data portability" as a deterrence against tech platforms' monopoly on data usage.

Conclusion

Chinese tech platforms involved in international data transfer are as large as those in the US, and continue to create new services using the data they have collected, while also forming duopoly and oligopoly conditions domestically and internationally. This additionally lowers the threshold for third parties to use such services, such as mobile payments, and promotes innovation in the form of online/offline interactions.

In this respect, they can provide services that are more advanced than US tech platforms. Nonetheless, none of these tech platforms have introduced systems that bestow "data ownership" and "data portability" on individuals. We believe it would be desirable to use these tech platforms as a means of integrating and introducing into China international trends and systems that seek greater coexistence between privacy and innovation. JS

Mariko Watanabe is a professor of the Faculty of Economics at Gakushuin University.