

DEVELOPMENT, CHALLENGES AND REFLECTIONS OF THE RIGHT TO DATA PORTABILITY IN CHINA

Fu Xin

TABLE OF CONTENTS

I. INTRODUCTION	30
II. ANALYSIS OF THE RIGHT TO DATA PORTABILITY IN CHINA	32
<i>A. Personal Information Protection Law in China</i>	32
<i>B. Right to Data Portability in Other Representative Jurisdictions</i>	37
III. INFLUENCE OF INTRODUCING THE RIGHT TO DATA PORTABILITY IN CHINA	42
<i>A. Advantages of Introducing the Right to Data Portability in China</i>	42
<i>B. Potential Problems in the Exercise of the Right to Data Portability in China</i>	46
IV. REFLECTIONS ON THE IMPROVEMENT OF THE RIGHT TO DATA PORTABILITY IN CHINA	49
<i>A. Reinforcement of Technical Support for the Right to Data Portability</i>	49
<i>B. Clarification of the Right Attribute of Personal Data and the Scope of Application</i>	50
<i>C. Establishment of a System for the Assessment of Portability of Personal Data</i>	53
V. CONCLUSION	55

DEVELOPMENT, CHALLENGES AND REFLECTIONS OF THE RIGHT TO DATA PORTABILITY IN CHINA

*Fu Xin**

The right to data portability is an essential part of personal data protection in the booming era of big data, which is closely related to our work and lives, as it may play a crucial role in safeguarding self-determination right of the data subject and foster a favorable environment for the players in a fair competition market. However, the implementation of the right to data portability in China is still in its infancy, fraught with complexities and uncertainties. This paper studies the right to data portability in China based on the Personal Information Protection Law, and explores its development, current status and potential impact in China. Moreover, it conducts a comparative analysis of the EU and US experience, mostly from the legislative perspective, to better understand practices in the world. In addition, this paper puts forward some specific suggestions on implementing the right to data portability, hoping that the right to data portability can be fully guaranteed in our real life.

I. INTRODUCTION

The past few decades have witnessed dramatic changes arising from the information revolution. Modern society has gradually transformed from the Internet era into the age of big data, which continues to have a profound impact on all aspects of people's lives and work. Specifically, the age of big data requires much in terms of protection and processing rules on private information and individual privacy. To better protect the rights of personal information, the European Union (EU) enacted the *General Data Protection Regulation* (GDPR) in 2016, which superseded the *Data Protection Directive* previously adopted in 1995. Article 20 of the GDPR establishes the 'right to data portability' in the field of protecting personal information, which grants the data subject the right to obtain personal data that he provided to a data controller previously, while the described data could be transmitted to another data controller without any hindrance. In 2018, the European Commission published a report titled *Data Protection as a Pillar of Citizens'*

* Associate Professor at the School of Foreign Languages, and Research Fellow at the Human Rights Research Centre, Northwest University of Political Science and Law.

Empowerment and the EU's Approach to the Digital Transition—Two Years of Application of the General Data Protection Regulation, noting that the right to data portability has clear potential to promote competition, and unlocking that potential is one of the Commission's priorities. This assessment report made it clear that data portability within the EU has yielded significant benefits in the fields of health and insurance, access to public and private services, increased manufacturing productivity, and improved product quality and safety.

Moreover, the European Council formally adopted the *Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data* on November 27, 2023, which came into effect on January 11, 2024,¹ serving as an important addition to the EU's legal protection of personal data and privacy, and further improving previous legislation such as the GDPR, the *Regulation (EU) 2018/1725*, and the *Regulation on Privacy and Electronic Communications*. Through a harmonized construction of rules, the adopted Proposal mentioned above substantially expands users' data control and achieves dynamic protection of personal information within the EU.

The *Personal Information Protection Law of the People's Republic of China* (hereinafter referred to as the Personal Information Protection Law), adopted by the National People's Congress (NPC) in August 2021, is regarded as the first comprehensive law governing the protection of personal information in China. Paragraph 3, article 45 of the Personal Information Protection Law stipulates that 'Where an individual requests the transfer of his personal information to a designated personal information processor, which meets the requirements of the national cyberspace department for transferring personal information, the requested personal information processor shall provide means for the transfer.' The new law amounts to the introduction of the right to data portability in China, which would not only meet the growing requirements for the cross-platform transfer of personal information but also bring great changes to the overall Internet industry in China. In addition, the *International Standard for Distributed Data Transfer*

1 PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON HARMONISED RULES ON FAIR ACCESS TO AND USE OF DATA (DATA ACT), at [https://www.europarl.europa.eu/RegData/publications/trilogue/2022/0047/NEGO_CT\(2022\)0047\(2023-03-28\)_XL.pdf](https://www.europarl.europa.eu/RegData/publications/trilogue/2022/0047/NEGO_CT(2022)0047(2023-03-28)_XL.pdf) (Last visited on July 22, 2025); REGULATION (EU) 2023/2854 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 13 DECEMBER 2023 ON HARMONISED RULES ON FAIR ACCESS TO AND USE OF DATA AND AMENDING REGULATION (EU) 2017/2394 AND DIRECTIVE (EU) 2020/1828, at <https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng> (Last visited on July 22, 2025).

(IEEE P3250.03) approved by the Wechsler Bank in November 2024,² the first international standard in the field of trustworthy personal data portability, would contribute to further accelerating the release of the value of data elements and enhancing China's international discourse in the field of data circulation.

In the era of big data, digital economy is a natural evolution in a developing society, culminating with technological innovation and supporting policies. Under the background that China's Personal Information Protection Law has introduced the concept of the right to data portability into legislation, which has been recognized by some jurisdictions worldwide, how will this new type of right affect people's social life? Additionally, how will it affect the development of various enterprises as data controllers in China?

Taking the adoption of the Personal Information Protection Law in China as the starting point, this paper focuses on the right to data portability, discusses the current situation in relation to the actualization of the new right, identifies potential influence of the right to data portability in China, and explores feasible suggestions in addressing possible problems in practice by analyzing some experience in two representative jurisdictions of the world.

II. ANALYSIS OF THE RIGHT TO DATA PORTABILITY IN CHINA

In this section, the author will depict and analyze the right to data portability in China, especially after the introduction of the Personal Information Protection Law in 2021, and the factual practice before initial formal legislation and then the legislation on the right to data portability in some representative jurisdictions, namely the EU and the US.

The Chinese legislature holds a cautious attitude toward the introduction of the right to data portability. The Personal Information Protection Law introduced the right for the first time. As a matter of fact, China has practiced number portability for over ten years, which is considered to be a pilot scheme for the right to data portability.

A. Personal Information Protection Law in China

1. Practice Before Formal Legislation in 2021: Number Portability. — Before 2021, China had not clearly established a statutory right to data

2 TANG GUIJIANG & LI YAN, GUIDE FOR BLOCKCHAIN-BASED DATA TRANSFER APPLICATIONS APPROVED, at <https://t.cj.sina.com.cn/articles/view/1784473157/6a5ce6450200329ke> (Last visited on March 25, 2025).

portability, but it had already constructed the prototype of the right to data portability at the level of regulations and norms, and formed the practice of data portability in enforcing number portability as early as before. Number portability means that within the same local network, it enables a cellular mobile communication user to retain his mobile telephone number when changing from one mobile network operator to another. If the necessary service is not possible, the user will be locked into a specific telecom carrier. Without the practice of number portability, if a user changes the carrier, he would be required to change a phone number, which would have an inconvenient influence on the basic aspects of the user's daily life.

Number portability signifies that phone numbers are no longer the property of the telecommunication providers, but are owned and managed by users. As a specific form of data portability, number portability has been implemented in more than 80 countries around the world.³ The introduction of number portability involves the transformation of the whole network, and considering that China is a major telecommunications country with more than one billion users, China's number portability service has experienced over a decade of development from the pilot stage to the final landing practice, and explored a set of technologies, services and legal solutions that could meet the national conditions.⁴ On November 11, 2019, the Ministry of Industry and Information Technology adopted and issued the *Regulations on the Administration of Number Portability Services*, which came into effect on December 1, 2019. Then, on November 27, 2019, the Ministry held a launching ceremony for the number portability service, officially providing number portability services nationwide. In addition, *China's Civil Code* stipulates that the information subject enjoys the right to copy personal data, but only one clause is available and in a general sense (article 1037).

China is not the first country to apply number portability. In order to promote competition in the telecommunications industry, the US Congress required all telecommunications carriers to provide number porting services under the *Telecommunications Act* introduced in 1996 and delegated the responsibility for implementation of such legal requirement to the Federal Communications Commission (FCC). Likewise, the EU also issued the *Universal Service Directive* in 2002 to state number portability in

3 Wang Qinghua, *The Right Structure, Legal Effect and Sinicization of the Right to Data Portability*, 3 China Law Review 189-201 (2021).

4 Gong Shuangjin, Huang Hexian & Qu Zhenhua, *Development of the Number Portability*, 1 Information and Communications Technology and Policy 5-8 (2020).

paragraphs (40) to (42) of the introductory part, and article 30.⁵

In addition to the number portability service, the National Information Security Standardization Technical Committee of China issued the *Regulations on Personal Information Security of Information Security Technology* (hereinafter referred to as the Regulations on Personal Information Security) on March 6, 2020, and paragraph 6, article 8 of the *Information Security Technology—Personal Information Security Specification* stipulates that personal information subjects shall have the right to obtain copies of personal information. Article 8 also states that the information controller shall, at the request of the personal information subject, transmit the above-mentioned information to a designated third party on the premise that it is technically feasible.

The Regulations on Personal Information Security introduce the right to data portability from the view of substantive national standards, but such provisions are still preliminary and tentative. National standards have important guiding significance in the data industry, and they are an important basis for practice. As for the effectiveness of national standards, they do not belong to the source of law.⁶

2. Practice After the Legislation in 2021: Legislative Regulation on the Right to Data Portability. — Before the promulgation of the Personal Information Protection Law, some officials, experts, and the public appealed to refer to the legislation of relevant jurisdictions and draft rules for the right to portability of personal information in order to facilitate individuals to access and transfer their personal information. The Personal Information Protection Law consolidated a rule on the right to data portability as a new clause (paragraph 3 of article 45) in the legislation. Based on such a right, individuals may freely transfer their personal information between various platforms or websites as long as data subjects meet the requirements raised by the national cyberspace administration. Unlike other negative rights (such as ‘the right to delete personal data’⁷) provided in Chapter IV, the right to data portability has fully reflected positive disposal of personal information held by individuals themselves.

5 DIRECTIVE (EC) 2002/22 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 7 MARCH 2002 ON UNIVERSAL SERVICE AND USERS' RIGHTS RELATING TO ELECTRONIC COMMUNICATIONS NETWORKS AND SERVICES, OJ L108/24 (UNIVERSAL SERVICE DIRECTIVE), 57 and 66 (2002), at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0022> (Last visited on July 17, 2025).

6 For detailed discussions of the Regulations on Personal Information Security, see Liu Yun, *The Personal Data Portability Right Under the Regulations on the Management of Network Data Security in China*, 1 *Industry Information Security* 25-30 (2025).

7 The right to delete personal data refers to the situation that when the personal information processor fails to erase information under legal situation, the data subject shall have the right to request deletion.

The right to consult with and duplicate personal data alongside the right to data portability in article 45 closely relates to the right to data portability in terms of content and overlaps with each other in operational requirements. It aims to guarantee the right to information and decides on the processing of personal information, while the right to data portability grants individuals the right to transfer their personal information from one data controller to another. The prerequisite for the transfer of personal data is that portable personal information should be accessed and copied, and *vice versa*.⁸ The right to duplicate can be realized when the information controller provides the individual with the requested copy of his personal information, while in the exercise of the right to data portability, what the individual concerned asks the information controller to transfer is a copy of his personal data kept by the controller. The right to consult and duplicate, and the right to data portability are closely linked, so it is not difficult for us to interpret the intent of the Chinese legislature, in the layout of these two rights regarding personal information.

After the Personal Information Protection Law came into force in 2021, the right to data portability in China's practice is still not adequate. According to the survey statistics in 2021, among the 50 most popular apps in China tested, only six apps explicitly mentioned their transfer service of providing personal information in the privacy policy.⁹ When it comes to September 2024, this situation had been substantively changed: The Cyber Security Association of China reported that 62 popular apps were proven to have complied with the legal requirement on the protection of personal information in terms of clarity and friendliness of privacy policies, regulated collection of personal information regarding the common functions, invocation or use of sensitive permission, recommended settings for personalized advertising and users' experience in exercising the rights and interests of personal information.¹⁰

To better protect the personal information, China has been improving the governance at the policy and legal levels. For example, the *Research Report on Consumer Data Circulation Patterns Based on the Right to Portability*

8 Fang Yu, *Personal Information Protection Under the Evolution of Data Value: Reflection and Reconstruction*, 6 Business and Economic Law Review 95-110 (2020).

9 HOW HARD IS IT TO 'COPY' YOUR OWN PERSONAL INFORMATION FROM AN APP?, at https://www.thepaper.cn/newsDetail_forward_15923625 (Last visited on July 16, 2025). See also REDNOTE USER PRIVACY POLICY, at <https://www.xiaohongshu.com/privacy> (Last visited on July 16, 2025); IQIYI, PRIVACY POLICY, at <https://privacy.iqiyi.com/policies> (Last visited on July 16, 2025).

10 LI LING, HAVE ALL THE 62 APPS YOU OFTEN USE COMPLIED WITH THE LAW IN THE COLLECTION AND USE OF PERSONAL INFORMATION?, at <https://baijiahao.baidu.com/s?id=1826815051984271979&wfr=spider&for=pc> (Last visited on July 16, 2025).

released in May 2024 points out that the right to data portability has become a legitimate right and interest of citizens in China.¹¹ The *Regulations on Network Data Security Management* adopted by the State Council in September 2024¹² strive to regulate cyber data processing activities, safeguard cyber data security, promote the lawful, rational, and efficient use of cyber data, protect the legitimate rights and interests of individuals and organizations in terms of personal information in a detailed manner and specify the obligations of online platform service providers. On February 14, 2025, the Cyberspace Administration of China promulgated the *Measures on the Administration of Compliance Audit of Personal Information Protection*, stipulating the requirement of conducting the compliance audit on the protection of personal data and listing 27 key items of audit matters in the form of attachment, and hoping to identify and correct the problems in a timely manner.¹³

Effectively on June 1, 2023, China started to pay attention to the regulation of cross-border transfer of personal data through the *Measures on Standard Contract for Cross-Border Transfer of Personal Information*, which was promulgated by the Cyberspace Administration of China.¹⁴ As a follow-up step, the Cyberspace Administration of China further detailed the cross-border collection and transfer of personal information in the *Regulations on Promoting and Standardizing Cross-Border Flows of Data* on March 22, 2024, in which articles 7 and 8 provide the threshold of the security impact assessment, filing for record of standard contracts and the authentication of cross-border transfer of personal information for data handlers other than critical information infrastructure operators that provide abroad the personal information.¹⁵

Despite these efforts, the right to data portability needs more effective legal support for implementation. The Cyberspace Administration of China investigated and handled 82 apps in February 2025 against the violations, among which 4 failed to disclose their rules on collection and use of the clients' personal information (resulting in removal from service) and 78 failed to provide the functions of deleting or correcting personal information

11 LIN ZHILAN, FOCUS ON THE 7TH DIGITAL CHINA SUMMIT: 3 SERIES OF RESEARCH RESULTS DEBUT, at <https://news.qq.com/rain/a/20240525A028RO00> (Last visited on June 3, 2025).

12 For details, see THE ORDER NO. 790 OF THE STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA, at https://www.mee.gov.cn/zcwj/gwywj/202410/t20241003_1087417.shtml (Last visited on July 16, 2025).

13 LI LING, *supra* note 10.

14 For details, see *Order No. 13 of the Cyberspace Administration of China of 2023*. See also CAC PROMULGATES MEASURES ON STANDARD CONTRACT FOR CROSS-BORDER TRANSFER OF PERSONAL INFORMATION, at <https://wap.bjd.com.cn/news/2023/02/24/10347580.shtml> (Last visited on July 18, 2025).

15 For details, see also MEASURES FOR THE ADMINISTRATION OF PERSONAL INFORMATION PROTECTION COMPLIANCE AUDIT, at https://www.cac.gov.cn/2025-02/14/c_1741233507681519.htm (Last visited on July 18, 2025).

(resulting in making corrections within one month, or removal from service in case of failure to make such corrections) respectively.¹⁶ Similarly, a special campaign on data security and protection of personal information during the same period in the field of livelihood consumption also found 388 items of violations by 197 apps randomly chosen by the Beijing cyberspace information authorities.¹⁷

B. Right to Data Portability in Other Representative Jurisdictions

Globally, the right to data portability is not an unfamiliar data right. In Asia, *India's Personal Data Protection Bill* stipulates the right to data portability;¹⁸ and Singapore establishes special provisions for the right to portability in its *Personal Data Protection Act*.¹⁹ Currently, 'Indonesia, India, and Malaysia are working toward the full implementation of their newly amended laws. Additionally, Australia has announced the first phase of a comprehensive reform of its *Privacy Act* after a thorough government review. Furthermore, many of the new or amended laws in the region also require a data protection officer to be appointed.'²⁰

The practices in the EU and the US are more typical on such issue. Actually, when the right to data portability was first proposed in the EU regulations, it went through a long but complicated drafting process. Similarly, the US attempted to introduce such a right to shield the individual's rights to personal information as early as the end of the 20th century. The jurisdictions mentioned above have some legislative experience and practical feedback.

1. The EU Practice: GDPR and Other Relevant Regulations. — The right to data portability was first introduced in the *Draft of General Data Protection Regulation* (hereinafter referred to as the Draft) in 2012 when the European Commission committed to addressing the impact of new technologies, enhancing the internal market dimension of data protection, and

16 *Id.* See also OFFICIAL NOTICE: THESE APPS VIOLATED THE LAWS AND RULES. CHECK YOUR MOBILE PHONES, at <https://baijiahao.baidu.com/s?id=1824762121271167135&wfr=spider&for=pc> (Last visited on July 17, 2025).

17 ZHANG LIBIN, WANG SISI & ZOU QIYUAN, HOW TO PREVENT IT WHEN APP BECOMES 'PRIVACY ASSASSIN' TO EXCESSIVELY COLLECT INFORMATION, at <https://news.cctv.com/2025/07/16/ARTIvAoJkONdHxLLnFnrmfUY250716.shtml> (Last visited on July 17, 2025).

18 SECTION 19 OF THE PERSONAL DATA PROTECTION BILL OF INDIA (2019), at https://prsindia.org/files/bills_acts/bills_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf (Last visited on March 9, 2025).

19 SECTIONS 26F, 26G, 26H, 26I AND 26J OF THE PERSONAL DATA PROTECTION ACT OF SINGAPORE (2020 REVISED EDITION) (2021), at <https://sso.agc.gov.sg/Act/PDPA2012> (Last visited on March 18, 2025).

20 FRESHFIELDS LLP, LEADING THE CHANGE: 2025 DATA LAW TRENDS, at https://www.freshfields.com/globalassets/our-thinking/campaigns/data-trends/data-trends_2025.pdf (Last visited on July 19, 2025).

providing a stronger institutional arrangement for the effective enforcement of data protection rules.²¹ Article 18 of the Draft granted particular users a right to control personal data, i.e., the data subjects are entitled to obtain and transfer personal data from one data controller to another. This new personal information right proposed in the Draft brought about a major change in the legislative process of personal data protection. After merging with other personal information rights, and then being deleted from other versions of the Draft, the right to data portability was finally brought back into an appropriate context. In 2016, the European Parliament adopted the ‘right to data portability’ as a separate provision (article 20 of the GDPR). And on May 25, 2018, the GDPR was fully implemented in the EU member states, establishing an independent legal status of the right to data portability, and officially replacing the *Data Protection Directive of 1995*. The GDPR formalized the right to personal data portability for the first time in the world and added new legal terms—such as data subject, personal data, data processing, data controller, and data processor—in the Internet era.

For the smooth implementation of the GDPR, the EU Article 29 Working Party has developed several policy directives, among which the *Guidelines on the Right to Data Portability* (hereinafter referred to as the Guidelines) is key, as the Guidelines mainly introduce key elements of the right to data portability, when it applies and how to provide the data that is portable, and thus regulate the ways of implementing the right to data portability.

For example, the Guidelines explained that the scope applies to data ‘provided by’ the data subject. In addition to the data actively uploaded by the data subject, the data observed by the data controller from recording the data subject’s activities is also included. Furthermore, as far as the expected data format is concerned, for the term ‘generally used’, the EU Article 29 Working Party encourages data controllers to reach a technical consensus according to the application scenario.

Of course, the Guidelines are not a perfect one as some standards that are required to be unified in the personal data transfer process still remain blank. For instance, the security of personal data being transferred is not guaranteed under the current provisions of the GDPR. The findings of empirical research authored by *Janis* and *Tristan* regarding the right to data portability under the GDPR indicate that 74.8% of requests for the right to data portability were

21 EUROPEAN COMMISSION, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, at https://commission.europa.eu/publications/communication-commission-european-parliament-council-european-economic-and-social-committee-and_en (Last visited on June 6, 2025).

completed among which many failed to comply with the right's obligation, and the process of realizing the right was always found unmanageable.²² Furthermore, another empirical research in 2020 found that the right to data portability in the GDPR failed to explain to data subjects and transmit personal data between different IoT service providers.²³

Through article 20 of the GDPR, the EU has separately listed the right to data portability, granting individuals both the right to download a copy of the data and the right to upload the copy to a designated address as a protection for the personal information right. However, the GDPR does not extend this right to enterprises, limiting the subject of the right to individuals. In December 2020, the European Commission proposed the *Digital Markets Act* (DMA) to regulate gatekeepers in the digital sector by imposing direct restrictions on the behavior of tech giants, including but not limited to Facebook, Google, Amazon, Microsoft, and Apple. This proposal was approved by the EU member states on July 4, 2022, which indicated a further step taken in exploring the right to data portability for enterprises. The gatekeepers act as a data platform, usually serving as an important link between two or more user groups, such as users and service providers. The DMA, as a regulation mainly for companies that control ecosystems, is seeking better protection of personal data right and SMEs' sustainable development, creating a more competitive but fairer digital space. Furthermore, the DMA, as a rule against competitive behaviors in the Internet environment, is closely related to the GDPR. From the perspective of anti-monopoly, the DMA further refines and maintains the implementation of data portability. The data access rights established by the *EU's Data Act* and two pivotal Common European Data Spaces, the European Health Data Space (EHDS) and the Financial Data Access (FIDA) framework, are set to affect business operations in the EU market.²⁴

In terms of cross-border flow of personal data, article 46 of the GDPR states that in the absence of a decision pursuant to article 45(3), a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available, which is similar to the Chinese approach but contrasts with the US model.

22 Janis Wong & Tristan Henderson, *The Right to Data Portability in Practice: Exploring the Implications of the Technologically Neutral GDPR*, 3 International Data Privacy Law 173-195 (2019).

23 Sarah Turner, July Galino Quintero & Simion Turner et al., *The Exercisability of the Right to Data Portability in the Emerging Internet of Things (IoT) Environment*, 10 New Media & Society 2861-2881 (2021).

24 FRESHFIELDS LLP, *supra* note 20.

2. *The US Practice: California Consumer Privacy Act and Other Subsequent Acts.* — The main focus of the US is to use data to promote technological progress and business development. The US mainly depends on industry self-discipline and *ex post facto* judicial remedies to achieve personal data protection. It holds a cautious attitude towards the right to data portability as a whole, and there is no unified data protection law similar to the GDPR or the regulatory institution responsible for data protection. Most of the practice on the right to data portability is achieved through a series of self-regulatory industrial guidelines formulated by government agencies and industrial groups.

As early as the 20th century, the US began to study new types of data rights in some sectors. For example, the *Health Insurance Portability and Accountability Act* (HIPAA) has granted individuals the right to access personal health information collected by health insurance agencies. The *HIPAA Privacy Rule*, an essential component of the HIPAA, enables individuals to actualize the right to consult and receive copies of personal health information maintained by a HIPAA-covered entity. Likewise, the *Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology of 2014* has discussed relevant technical feasibility and standards set out in §170.314(b)(7) ‘Data portability’.²⁵ The ‘Blue Button’ initiative, a national movement aimed at granting every American access to their own health records easily in a usable format, seeks to expand patient access to their medical records, allowing data subjects to track their own health records, and extend shared records to doctors and specialists.²⁶

The *California Consumer Privacy Act of 2018* (CCPA) was the first comprehensive privacy law in the US, which provided a variety of privacy rights to California consumers, including the right to data portability. The regulations on transferring personal data in the CCPA are designed to hold the data controllers responsible for personal information as a part of any transaction with a third party who assumes control of the business. The data transfer occurs only when there is a business transaction between data controllers, rather than data subjects claiming the right when they have such a need. Data subjects are still in a passive position under the CCPA.

25 KATHRYN MARCHESINI & TIMOTHY NOONAN, HIPAA & HEALTH INFORMATION PORTABILITY: A FOUNDATION FOR INTEROPERABILITY—HEALTH IT BUZZ, at <https://www.healthit.gov/buzz-blog/privacy-and-security/hipaa-health-information-portability-a-foundation-for-interoperability> (Last visited on February 22, 2025).

26 KRISTEN HONEY & PHAEDRA CHROUSOS, MY DATA: EMPOWERING ALL AMERICANS WITH PERSONAL DATA ACCESS, at <https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access> (Last visited on June 2, 2025).

Self-discipline is also an indispensable element of improving the right to data portability. For example, the Data Transfer Project (DTP) was a collective initiative launched in 2018 with Apple, Microsoft, Facebook, and Twitter that has extended data portability to directly transfer their data between any two participating online service providers. It relies on tools that can convert a participating service provider's Application Programming Interfaces (API)—a software intermediary that enables a mutual dialogue between two applications—to a set of standardized data formats. These tools, which are being built by the open-source community and are available on GitHub, make data transfer possible using existing industry-standard infrastructure and authorization mechanisms. Besides the DTP, tech giants also have their own projects to promote consumers' data transferring more easily, like Facebook's 'Access Your Information' and Google's 'Takeout'. According to *Ali Lange*, Public Policy Manager at Google, Google's data portability initiatives have allowed users to export a copy of the content in their Google account to back up or use with a service outside of Google.²⁷

Without a comprehensive national privacy act in place, individual states have been expanding their own laws and regulations to safeguard consumer privacy since the enactment and implementation of the *California Consumer Privacy Act*. For example, on December 31, 2023, the *Utah Consumer Privacy Act* came into effect²⁸ and the *American Privacy Rights Act of 2024* was adopted in April 2024.²⁹ During July 18, 2023 and July 1, 2024, the *Florida Digital Bill of Rights*,³⁰ the *Oregon Consumer Privacy Act*,³¹ and the *Texas Data Privacy and Security Act*³² became effective within their respective jurisdictions. So far, 'over 40 percent of US states have implemented consumer privacy laws, and momentum continues to grow as additional states propose and consider their own legislation. Furthermore, certain states are also introducing specialized privacy laws, such as those focused on consumer health data.'³³ This series of laws and regulations represented a delicate reconciliation

27 DATA TO GO: AN FTC WORKSHOP ON DATA PORTABILITY, at <https://www.ftc.gov/news-events/events/2020/09/data-go-ftc-workshop-data-portability> (Last visited on January 14, 2025).

28 UTAH CONSUMER PRIVACY ACT, at <https://utah-ucpa.org/> (Last visited on May 21, 2025).

29 THE AMERICAN PRIVACY RIGHTS ACT OF 2024, at <https://www.commerce.senate.gov/services/files/E7D2864C-64C3-49D3-BC1E-6AB41DE863F5> (Last visited on January 13, 2025).

30 FLORIDA DIGITAL BILL OF RIGHTS (FDBR): A COMPLETE GUIDE FOR 2025, at <https://wplegalpages.com/blog/florida-digital-bill-of-rights-fdbr/> (Last visited on May 16, 2025).

31 NANCY LIBIN, MICHAEL T. BORGIA & JOHN D. SEIVER ET AL., OREGON CONSUMER PRIVACY ACT SIGNED INTO LAW, at <https://www.dwt.com/blogs/privacy--security-law-blog/2023/07/oregon-consumer-privacy-law-signed> (Last visited on January 26, 2025).

32 TEXAS DEPARTMENT OF INFORMATION RESOURCES, TEXAS DATA PRIVACY AND SECURITY ACT, at <https://dir.texas.gov/technology-legislation/texas-data-privacy-and-security-act> (Last visited on January 12, 2025).

33 FRESHFIELDS LLP, *supra* note 20.

between the importance of personal data protection and a cautious attitude toward the right to data portability in the US.

In addition, it is worth noting that starting from 2024, the US authorities successively promulgated a series of legislations and official documents to further restrict, regulate and control the flow of sensitive privacy and data from the US to overseas, particularly the so-called foreign adversaries, including its attempts to curb China's rise of economy and technological development, such as the *Protecting Americans' Data from Foreign Adversaries Act of 2024*,³⁴ the *Protecting Americans from Foreign Adversary Controlled Applications Act*³⁵ and the *Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*.³⁶

III. INFLUENCE OF INTRODUCING THE RIGHT TO DATA PORTABILITY IN CHINA

In the context of the increasingly mature development of Internet big data, the contradiction between the protection of personal data privacy and information development becomes more prominent in China. When the practice of data portability expands and spreads to the entire data industry after the introduction of the concept of data portability in legislation, it would bring about some profound implications concerning Chinese data subjects, data enterprises, and the information society.

A. Advantages of Introducing the Right to Data Portability in China

The establishment of the Personal Information Protection Law reflects the legislative idea of returning the right of personal information to individuals, affording subjects' managerial control over their personal data. When the

34 PUBLIC LAW 118-50, 138 STAT. 895, 118TH CONGRESS, APRIL 24, 2024, at https://www.ftc.gov/system/files/ftc_gov/pdf/padfa_plaw-118-50.pdf (Last visited on July 18, 2025). The statute makes it unlawful for a data broker to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available personally identifiable sensitive data of a US individual to any foreign adversary country or any entity that is controlled by a foreign adversary. See also DAVID PELOQUIN, FRAN FAIRCLOTH, EDWARD R. MCNICHOLAS ET AL., US ENACTS SWEEPING LEGISLATION TO RESTRICT FLOWS OF SENSITIVE DATA TO THE PEOPLE'S REPUBLIC OF CHINA AND OTHER FOREIGN ADVERSARIES, ROPES AND GRAY, at <https://www.ropesgray.com/en/insights/alerts/2024/04/us-enacts-sweeping-legislation-to-restrict-flows-of-sensitive-data-to-the-peoples-republic-of-china> (Last visited on July 18, 2025).

35 This bipartisan legislation is allegedly to protect Americans by preventing foreign adversaries from targeting, surveilling, and manipulating the American people through online applications. See H. R. 7521, 118TH CONGRESS 2ND SESSION, 10 U.S.C. 4872(D)(2), at <https://www.congress.gov/118/bills/hr/7521/BILLS-118hr7521eh.pdf> (Last visited on July 18, 2025).

36 See EXECUTIVE ORDER 14117 OF FEBRUARY 28, 2024, FEDERAL REGISTER VOL. 89, NO. 42, at <https://www.govinfo.gov/content/pkg/FR-2024-03-01/pdf/2024-04573.pdf> (Last visited on July 18, 2025).

right to data portability can be implemented, data subjects will have greater clarity regarding their own data on the platform and have more personalized control over their private data on the platform. In addition, digital data is closely related to individuals' personalities, which can reflect the personal characteristics of data subjects in the Internet world.³⁷ By interactive processing of data, the Internet platform connects each real individual through the network. The 'digital personality' is formed when the real person's qualification and dignity are mapped in the network community.³⁸ Along with the rapid development of the Internet, electronic personality is becoming an obvious trend.³⁹ For example, the comments, pictures, and labels posted by data subjects on WeChat, Weibo, and other social media platforms are strong reflections of personal characteristics.⁴⁰ The right to data portability allows data subjects, as consumers, to be fully respected by exercising the right to choose in the data market. With the rapid development of network technology and the growing range of online platforms providing similar services, consumers have the right to freely choose service providers that can meet personal needs according to personal preferences and usage habits.⁴¹ The introduction of the right to data portability will legally require the platform owner not to restrict the data subject's transfer requirements, but to respect personal choices and to provide the user with data owned by the platform to help the data subject carry personal data to other platforms.

For the vast number of data enterprises, the introduction of the right to data portability undoubtedly promotes the construction of a fair competition environment among enterprises. Especially for small and medium-sized data enterprises, the right to data portability may 'attract' more users to their platforms. Some leading data enterprises regard the data provided by users as their own data and use such personal data to obtain certain commercial value.⁴² To prevent the loss of users, data companies do not focus on product

37 Digital personality refers to an individual's attitudes, interests, social roles, and other traits that relate to his or her use of technology. See JASON MOATS, INFLUENCES ON THE ACCEPTANCE OF INNOVATIVE TECHNOLOGIES USED IN LEARNING OPPORTUNITIES: A THEORETICAL PERSPECTIVE, in HANDBOOK OF RESEARCH ON INNOVATIVE TECHNOLOGY INTEGRATION IN HIGHER EDUCATION, at 20 (Fredrick Muyia Nafukho & Beverly J. Irby eds., GI Global, 2015).

38 Ma Jinfei, *On the Legal Review of the Right to Data Portability*, 23 Shanghai Legal Studies 224-232 (2021).

39 GABRIELA ZANFIR, THE RIGHT TO DATA PORTABILITY IN THE CONTEXT OF THE EU DATA PROTECTION REFORM, 2(3) INTERNATIONAL DATA PRIVACY LAW (2012), at <https://academic.oup.com/idpl/article-abstract/2/3/149/660539?login=false> (Last visited on July 18, 2025).

40 Zhuo Lixiong, *Right to Data Portability: Concept, Problems and China's Response*, 6 Administrative Law Review 129-136 (2019).

41 Wang Jingzi & Fu Xin, *On the Development of Right to Data Portability in China and Its Challenges*, 4 Case File 389-390 (2024).

42 Shen Jia'ni, *Who Is in Charge of My Rights?—A Study on the Boundary Between Personal Data Portability and Enterprises' Data Rights Based on 'Dispute Between Byte Dance and Tencent'*, 6 China Internet 22-27 (2019).

innovation, but try to raise data transmission barriers and lock in users by raising the transfer costs. Originally, under the joint action of platform mode and network effect, Internet products or services usually maintain a high degree of adhesion, which results in an equally high degree of dependence on the part of consumers when choosing products or services, thus eventually producing a consumer lock-in effect.⁴³ When users find that the cost of moving to another service platform is very high, they tend to choose to remain on the same platform, even though a similar platform may offer superior service.⁴⁴ Accordingly, the leading enterprises use their existing advantages and lock-in effect to retain users and destroy the fair competition environment on the grounds of protecting so-called corporate data rights. The right to data portability will break down barriers for small and medium-sized enterprises (SMEs) in the data industry and promote the healthy development of developing data enterprises.

For most of the SMEs, market barrier is an inevitable dilemma. At one time, low barriers to market access were regarded as one of the characteristics of data-driven market. However, the choices before users are quite diversified today, given the abundance of Internet products and services. Managers who want to win the favor of users from similar products or services will certainly require ample data for reference and guidance. Along with the increasing emphasis of Internet service providers on data, the access barriers to the data market are becoming more and more serious.⁴⁵ Compared with a small number of technology giants and leading enterprises in the industry, the financial and technical disadvantages of SMEs are fully exposed. Capital and technology are two complementary and mutually influencing factors of production, both of which determine the quantity and quality of data acquired, analyzed and utilized by enterprises. If the limited personal data is always in the hands of select large enterprises, the market structure will be solidified, resulting in a difficult development situation for SMEs.

The right to data portability creates conditions for the data resources possessed by big data controllers to be transferred to new controllers and opens up dynamic development space for new operators. From the perspective of social innovation, the right to data portability can stimulate the activity of data subjects in the big data economy with the full free

43 Jin Zeng, *The Competitive Characteristics of Internet Product and Definition of Relevant Market*, 39(3) *Journal of Xiangtan University (Philosophy and Social Sciences)* 52-57 (2015).

44 Barbara Engels, *Data Portability Among Online Platforms*, 5 *Internet Policy Review* 1-17 (2016).

45 Li Boxuan, *Anti-Monopoly Effect of the Right to Data Portability: Mechanism, Reflection and Strategy*, 12 *Journal of Social Sciences* 105-116 (2021).

circulation of data and promote the flow of personal data. This will lower the threshold for innovations in data enterprises. When the data subject can obtain or transfer the relevant personal data, this will reduce the cost for data enterprises to access and use personal data. Accelerating the pace of social innovation is in line with the development direction of the era of big data. When enterprises highlight product and service innovation to attract users to choose the platform, rather than locking in users by raising barriers, the innovation power of the society will be substantially improved. In the long run, the virtuous cycle of an ordered, sustained, and coordinated industry will be restored. A report on the impact of the right to data portability on the innovation and development of European companies in competitive markets shows that online platforms like Spotify will increase investment, make use of data-driven innovations, and improve user engagement and retention to avoid losses.⁴⁶ Also, data portability will moderately break the phenomenon of ‘data island’ and ‘data lock-in effect’, promote the effective exchange and sharing of data, and improve the level of open sharing of public data in China.⁴⁷

Moreover, since the implementation of the Personal Information Protection Law, there has been a positive shift in the protection of the right to data portability in various Chinese industries. For instance, in the financial industry, commercial banks should strictly comply with the legal provisions in practice, and they should provide personal information in a timely manner when a financial consumer requests access to or a copy of his personal information. Meanwhile, if a consumer notices that his personal information recorded is inaccurate or incomplete, commercial banks are obliged to correct or supplement it. As far as the Internet industry is concerned, Internet companies have increased their investments in data security after the implementation of the Personal Information Protection Law. In terms of the healthcare industry, a stricter information management system is established to ensure the safety and accuracy of clients’ personal information. In the hospital, patients may have the right to access their own medical records, and may enjoy the right to demand that the hospital concerned make corrections and supplements if they find that their personal information is inaccurate or incomplete.⁴⁸ In the process of consumption, the system of personal

46 Esmeralda F. Ramos & Knut Blind, *Data Portability Effects on Data-Driven Innovation of Online Platforms: Analyzing Spotify*, 44 Telecommunications Policy 1-8 (2020).

47 Zhao Jingwu, *Construction Basis and Regulatory Transformation of Stand Form Contract in Cross-Border Data Transmission*, 2 Science of Law (Journal of Northwest University of Political Science and Law) 148-161 (2022).

48 Liu Tianle, *Practical Path for the Protection of Financial Consumers Personal Information Based on the ‘Informed Consent’ Rule of the Personal Information Protection Law*, 5 Modern Finance Guide 77-80 (2022).

information protection is also being established and improved. On shopping platforms, consumers can check their personal information, such as the order and address of delivery. If they find that the information is incorrect, they may request the platform concerned to amend it. Thus, the Personal Information Protection Law has also promoted openness and transparency for individuals regarding personal information handled by service providers, strengthened individuals' right to decide on the handling of personal information, and provided them with an effective way of judicial protection for personal information.

B. Potential Problems in the Exercise of the Right to Data Portability in China

Although the concept of data transfer has been officially incorporated in Chinese law, it is mainly at the theoretical stage, and there are limited practical examples in article 45 of the Personal Information Protection Law. Data is not an isolated code, and when it is extracted from the native environment, data that has lost connection with the context means that the data itself lacks the ability to fully reproduce its original meaning. When data controller A transmits a copy of the user's data to the user, and then the user provides his or her data to data controller B, data controller B will obtain a copy of the user's data only, not the context. Due to the lack of complete contextual information, data controller B can only provide an incomplete benchmark test and analysis.

The nature of the right to data portability is still unclear. As we know, the right to data portability is closely related to the individual's dignity and personality freedom. In essence, personal data is an extension and embodiment of personal personality in the digital space. Users have the right to decide whether to carry and transfer their own data to meet their demands among different platforms or service providers, which reflects the respect for the autonomy of individuals' personality and is consistent with the basic features of personality rights. This right, which relies to a certain extent on digital technology and the network environment as well as the support of specific technical means and platforms, may distinguish itself from the traditional personality rights, such as the rights to name and portrait. In the era of digital economy, personal data is of economic value and embodies the attribute of certain property rights, and the right to data portability will allow users to control their own data to obtain economic benefits. They may carry their fan data accumulated on one platform to another, resulting in more

business opportunities. Compared with the object of traditional property rights, however, data is intangible, making it difficult to accurately quantify the property value of the data involved. In judicial practice, due to the vague attribute of such a right, when the parties have disputes related to the right to data portability, a series of problems, such as difficulties in determining the liability and inconsistent standards in judicial decisions, will arise.⁴⁹ When the parties' right to data portability is infringed upon, they are unable to determine whether they should claim damage to their personality right or property right in terms of the remedies.

The right to data portability is interoperability-demanding. However, 'even the internationally respected Mayo Clinic, which treats more than a million patients a year, has serious unresolved problems after working for years to get its three major electronic records systems to talk to one another.'⁵⁰ In a study that evaluated the impact of open standard document formats on interoperability, the cost and difficulty of realizing interoperability were emphasized. The study tested document formats and found a 'lack of 100% interoperability between implementations'.⁵¹

Moreover, the right to data portability may encounter the potential risk of privacy or intellectual property infringement. When users transfer their personal data from one platform to another, the data may face the risk of improper information disclosure in the process of transmission and the subject who newly receives the data may use the data beyond the user's expectation, posing a potential danger of secondary utilization. For example, the user's browsing records and purchase records in the consumption process may not involve core privacy. Besides, the right to data portability may also result in intellectual property infringement in the course of implementation due to the problems of theft of the original content, algorithm-derived data, or leakage of trade secrets.⁵²

Furthermore, there is a certain risk of leakage in the process of data transfer. Admittedly, the original intention of the right to data portability was to facilitate data subjects to obtain and transfer personal data related to them, but in the process of data transfer, opportunities for hackers to steal

49 Zhang Yifei, *Logics and Rules on the Application of the Right to Data Portability*, 1 *Presentday Law Science* 65-76 (2024).

50 MILT FREUDENHEIM, THE UPS AND DOWNS OF ELECTRONIC MEDICAL RECORDS, NEW YORK TIMES, at <https://www.nytimes.com/2012/10/09/health/the-ups-and-downs-of-electronic-medical-records-the-digital-doctor.html> (Last visited on July 28, 2025).

51 Rajiv Shah & Jay P. Kesan, *Lost in Translation: Interoperability Issues for Open Standards*, 8 *I/S: A Journal of Law and Policy for the Information Society* 113-120 (2012).

52 Tang Xia, *Difficult Situation in the Application of Data Portability, and Solutions and Local Construction*, 1 *Administrative Law Review* 95-107 (2023).

personal data became possible. Therefore, while the right to data portability enhances the individual's control over personal data from the attributes of such right, the risk of practice may weaken the control of personal data in turn and increase the risk of exposure to personal data and privacy. Hackers will be possible to get personal data by using false identities, when data receivers are weak in data processing or have a deficient system for users' authentication.⁵³ As mentioned earlier, despite the laws and regulations being available now, there are still violations of personal data protection in China. In addition, the implementation effect of data protection regarding the cross-border data from China to overseas is subject to the tests in practice, given that such regulations and measures were just released 1-2 years ago.

For the implementation of data portability, technical upgrades such as personnel management configuration and data interface, as well as the risk of user loss caused by easier transfer of personal data, will escalate the cost of compliance and increase the burden on enterprises. Examining the *Guidelines on the Right to Data Portability* as an example, when data controllers consider which format to provide data, they should consider the situation of the data subject reusing the data, so as to help users achieve the purpose of data reuse.⁵⁴ Present data controllers, therefore, not only have to respond to users' requests, but also pay extra attention to possible form requests of another data controller to which users intend to transfer their personal data. Conducive to meeting the legal requirements, the SMEs with a smaller scale and a weaker foundation will inevitably invest in heavy technology and management costs, which will lead to reduced corporate innovation costs, an influence on the incentive for enterprises to innovate, and hinder the willingness to engage in the development of data industry.

It is worth noting that the establishment of the right to personal data portability may create barriers to the development of start-up industries. For those start-ups, the role of data portability in lowering market entry barriers is not absolutely positive, and it may lead to the situation of end consumers and competitors getting worse. *Lam* and *Liu* demonstrated that under the demand-expansion effect and network effect, entry is likely to become more prohibitive as the big data service is valuable enough.⁵⁵ Their analysis of

53 Zhuo Lixiong, *supra* note 40, 139.

54 ARTICLE 29 DATA PROTECTION WORKING PARTY, GUIDELINES ON THE RIGHT TO DATA PORTABILITY, at https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf (Last visited on May 31, 2025).

55 Wing M. W. Lam & Liu Xingyi, *Does Data Portability Facilitate Entry*, 69 International Journal of Industrial Organization 2-52 (2019). See also Liu Hui, *Conflicts and Adjustment of the Right to Personal Data Portability and Enterprises' Access to 'the Principle of Three-layer Grant'*, 7 Political Science and Law 114-131 (2022).

the game theory model found that the right to data portability encourages consumers to disclose more data to incumbents, as consumers care little about the data-induced switching costs that may occur when transferring data to a new platform. However, as consumers disclose more data, existing enterprises will have a higher data analysis network effect,⁵⁶ strengthening the competitive position of existing enterprises relative to new market entrants and raising the barriers to entry. Although data portability promotes the circulation and conversion of data, this influence can be comprehensively offset by the increase in the network effect of data analysis. Therefore, the author concludes that although the right to data portability reduces the switching cost, data portability may adversely affect the long-term efficiency. With reference to innovation, some scholars believe that there is no direct evidence for the assertion that ‘free circulation of data may promote social innovation’, and data portability may hinder innovations in some industries. As the data collected by oneself can be easily transferred by others, the enthusiasm of data controllers to collect, analyze and utilize data resources will be dampened. Thus, this school of scholars believes that the right to data portability⁵⁷ may be even more detrimental to social innovation.⁵⁸

IV. REFLECTIONS ON THE IMPROVEMENT OF THE RIGHT TO DATA PORTABILITY IN CHINA

Based on the discussions above, there are some suggestions for addressing the problems in practice mentioned above, but all these should consider China’s national conditions, and either absolute reference or blind borrowing is not advisable in the Chinese context.

A. Reinforcement of Technical Support for the Right to Data Portability

First of all, the sustainable and healthy development of the right to data portability requires not only legislative and judicial protection but

56 Data network effect refers to a product’s value grows due to the accumulation of users’ usage times, which makes the product able to constantly refine and develop its serving performance.

57 Urs Gasser & John Palfrey, *When and How ICT Interoperability Drives Innovation*, 33 Berkman Center Research Publication 1-28 (2007).

58 INGE GRAEF, JEROEN VERSCHAKELEN & PEGGY VALCKE, PUTTING THE RIGHT TO DATA PORTABILITY INTO A COMPETITION LAW PERSPECTIVE, LAW: THE JOURNAL OF THE HIGHER SCHOOL OF ECONOMICS, ANNUAL REVIEW 53-63 (2013), at <https://research.tilburguniversity.edu/en/publications/putting-the-right-to-data-portability-into-a-competition-law-pers> (Last visited on July 16, 2025).

also technical support in China. In practice, empirical studies reported the technical difficulties and low response rate in timely satisfying the users' requests for personal data transfer.⁵⁹ Thus, relevant authorities should formulate unified standards for data format to realize unimpeded transmission of data. In the meantime, Chinese authorities are advised to promote open data format standards, such as JSON and XML, so as to effectively reduce costs of data conversion and improve the degree of data portability.

Secondly, China may ensure smooth transmission of data between different network environments and platforms by developing a common data interface that supports multiple communication protocols. For example, Chinese authorities should also strengthen the security authentication mechanism and establish a sound authentication and authorization mechanism in practice to ensure that only legitimate users and authorized third parties can access and obtain personal data. This may also be applicable to the cross-border flow of such data from China to overseas.

Last but not least, simple and intuitive user interfaces should be designed for users from the technical perspective, through which detailed and simplified data portability instructions and guidelines on such interfaces are available to facilitate users to initiate data transfer requests and track the progress of data transfer in real time.

B. Clarification of the Right Attribute of Personal Data and the Scope of Application

The right to data portability is merely an open clause authorizing the data subjects for the given right, and its future practice will also depend on the setting of specific conditions for starting and exercising this right in the future.⁶⁰ But the provisions of the Personal Information Protection Law on the right to data portability are still relatively general in China. First, the scope of the data to which the right to data portability applies is unclear.

As far as the method of data transfer is concerned, paragraph 3, article 45 of the Personal Information Protection Law states that 'the requested personal information processor shall provide means for the transfer', which does not specify the requirements that the format of the transmitted data

59 Liu Chun, Feng Qiqi & Zhu Jiayue, *An Empirical Analysis of the Right to Data Portability in Chinese Application Software*, 2 New Horizons from Tianfu 41-52 (2025).

60 Wang Xixin, *The Justice of Distribution Between the Right to Data Portability and Data Governance*, 43(6) Global Law Review 5-22 (2021).

should be met. Article 20 of the GDPR uses the expression ‘in a structured, commonly used and machine-readable format’ to transfer personal data. In Singapore, the Parliament passed the *Personal Data Protection (Amendment) Bill* in late 2020, amending the *Personal Data Protection Act* passed in 2012. The revised *Personal Data Protection Act* has added new content in relation to the right to data portability and data transfer obligations, making Singapore a representative country in Asia to follow the EU’s approach to data portability legislation. The revised *Personal Data Protection Act* in Singapore has set up a special chapter to regulate the issues related to ‘data portability’, which includes articles 26F, 26G, 26H, 26I and 26J. This chapter not only introduces the legislative purpose, relevant terminology, and the right to transmit personal data under data porting request, but also provides detailed provisions on the right to data portability and data transfer obligations, including the circumstances in which data transmission can be carried out to meet the requirements of individuals, the scope of data that can be transferred, and the storage time of related data.⁶¹

Regarding the two questions mentioned above, the current Personal Information Protection Law in China stipulates that ‘meeting other conditions set forth by laws and administrative regulations and by the national cyberspace department.’ However, the Cyberspace Administration of China has not yet promulgated specific provisions on the right to data portability. Accordingly, both the national cyberspace administration and the Chinese legislature should supplement laws and regulations as soon as possible to stipulate the basic standards for data portability and promote the first step in the implementation of data portability in China. Also, it is suggested that various stakeholders take a part in reaching a final decision about the right’s code of conduct so that data controllers can better understand and exercise the right to data portability.

Moreover, when the Chinese legislature employs more supportive policies regarding the right to data portability, data security provisions could be refined, further reducing the risk of data leakage. When the data subject makes a request to obtain the data he or she has uploaded or transmitted, the data controller shall verify the identity of the data subject and implement ‘multi-factor authentication’ for the transmission of sensitive information, that is, the data controller requires the user to go through two or even more authentication mechanisms before the demander obtains the authorization and access to personal data. For example, after the user enters the PIN code to log

61 Dong Chunhua, *Data Portability of Personal Data Protection Law in Singapore*, Chinese Social Sciences Today, at A07.

in, the identity verification is also required through fingerprint comparison or face comparison. The verification procedures can improve the security factor of data transmission to a certain extent and reduce the occurrence of identity theft and fraud. Simultaneously, the data controller should be given guiding suggestions that ask the data controller to comprehensively consider the nature and purpose of the transmitted data and the various possibilities of risks. Alternatively, the government could require that the two servers should discuss the data encryption protocol in advance, to achieve security protection during the transmission of data.

The converse of data security risks is brought about by potential data editing capabilities. When the data is out of the original context, the third-party platform that accepts the transferred data cannot judge its authenticity and accuracy if such data is maliciously edited. The risk of fraud posed by data editing capabilities cannot be ignored, and therefore, the legislature should also pay attention to the editable nature of data and protect the data from being altered during the process of transfer. The reality is that when a shop gains control over its rating data, the bad reviews disappear inexplicably. The UK had previously enforced the Open Banking practice, and consumers began to author fake personal records, as exemplified.⁶² The starting point of polishing up regulations on the right to data portability in China should consider the national conditions and develop into a distinctive pattern, just as the EU's point starting from the humanism of developing local corporations and the US style of reflecting the dominant characteristic of big companies.⁶³

In addition, the Supreme People's Court in China may issue some guiding cases to explain and demonstrate the specific application of the attribute and scope of application of the right to data portability in judicial practice. At the same time, the relevant administrative and regulatory authorities, such as the Cyberspace Administration of China, can formulate more specific regulatory rules and implementation regulations to clarify the attributes and scope of application of the right to data portability, and pay attention to law enforcement in this respect. Relevant technical organizations and industrial associations may also formulate technical standards and specifications for data portability to ensure that data between different platforms and systems can be effectively and securely ported and transferred. Finally, industrial associations can formulate their own specifications on

62 Marshall W. V. Alstyne, Georgios Petropoulos & Geoffrey Parker et al., 'In Situ' Data Rights, 64(12) Communications of the ACM 34-35 (2021).

63 Wen Libin & Zou Ying, *Reflection and Revision on the Object Boundary and Realization of Method of the Right to Information Portability*, 2 Journal of Chongqing University of Posts and Telecommunications (Social Science Edition) 53-62 (2023).

the right to data portability according to the characteristics and needs of the industry, and clarify the right attribute and the scope of application.

C. Establishment of a System for the Assessment of Portability of Personal Data

The types of data available to individuals are diverse, and the nature of the data is complex. The goal of the right to data portability covers public benefit and private interest at the same time. The application of the right shall balance the two benefits.⁶⁴ But, it is undeniable that the right to data portability and the right to self-determination of information by third parties are prone to cause conflicts. Few scholars think that the request for a data subject's data transfer is less likely to affect the rights of others, as controversy only happens when the nature of the data is closely linked to third parties.⁶⁵ In social networks, personal data often involves information about others, inevitably leading to a contradiction between the right of third parties to self-determination of information and the right to data portability. In social networking platforms, personal dynamic records, pictures, and chat records posted by individuals may involve information about other subjects. Additional right protection problems are triggered when data transfer concerns intellectual property and trade secrets of third parties. Does a data subject need to obtain the consent of another person when transferring personal data to another social networking platform? If the information requested by the user contains personal information of others, who should evaluate whether the transmission of such information will bring any adverse effect on the rights and interests of others? If a third party is not informed or notified about the data transfer between data controllers which is demanded by a data subject, will this constitute a crime of illegal data collection? If a third party is informed but refuses to allow the transfer, how do we resolve such conflicts?

The third parties are passive in exercising their right to data portability. They are not the ones to initiate the motion, but their privacy and property are potentially involved. A package of third-party-related mechanisms is needed for assessing the portability of data to obtain informed consent. First, the data to be transferred should be assessed. Is there integrity regarding the data subject's individual data? Is there evidence of any third parties' personal

64 Yuan Junyu & Zhang Binfeng, *Normative Construction and Coordinated Application of Personal Information Portability System*, 3 Journal of Nantong University (Social Sciences Edition) 81-91 (2023).

65 Beata A. Safari, *Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection*, 47 Seton Hall Law Review 809-848 (2017).

information, such as pictures, chat records and intellectual property? For example, although the GDPR is designed as a general control mechanism, which is suitable for any kind of data reuse, the coordination between the GDPR and intellectual property rights may once again limit the subsequent use of data portability for specific purposes.⁶⁶ The assessment of data portability requires the coordinated development of uniform standards within a country or an industry in order to ensure that the rights and interests of third parties' relevant information will be fairly treated. Thus, there should be a system for third parties to get informed and express their decision about whether they consent to transferring data involving their personal information or not.⁶⁷ If the transferred data is not authorized by third parties, the new data controllers should promise neither to analyze nor utilize the data.

To establish such a huge data analysis system, it needs not only technical support, but also the clarification of legal relationships, which is particularly important. What matters most is who will take the responsibility for evaluating the portability of data? When the data controller is given full authority for such evaluation, the cost of the data controller's obligation of review and compliance will undoubtedly increase greatly. So far, even the EU, the first jurisdiction to propose the right to data portability, has not discovered a solution for balancing it effectively. In the GDPR, the right to data portability is described as 'the data subject shall have the right to receive the personal data concerning him or her', which shows that the information of the data subject can only be identified as purely personal data. It more accurately serves as guidance for third parties. There is a clear bottom line in the DMA while leaving a space for judges' discretion to code with. Essentially, it can be understood that on the one hand, the EU hopes to protect personal data, and promote competition and free circulation of personal data through the right to data portability. On the other hand, there are concerns that the emergence of this right will have adverse effects on the rights of others, so there are some vague restrictions.

Building a system to assess data portability is a complex and complicated project. China's legislature might adopt a 'one size fits all' approach. The measure seems straightforward and mechanical, but in the period when the right to data portability was initially introduced into China, it can improve the enforceability of the new right and set up a preliminary platform for further advancement. But the detailed system for the assessment of the portability

66 Inge Graef, Martin Husovec & Nadezhda Purtova, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, 19(6) German Law Review 1359-1398 (2018).

67 Wang Jingzi & Fu Xin, *supra* note 41.

of personal data requires more engagement of stakeholders in China, which may need further tests in practice.

V. CONCLUSION

As the core resource of information economic competition, the vast commercial value behind personal data drives market economy entities to collect and process a large amount of personal information, especially in the network environment, concluding that personal information faces more potential risks. The position of data subjects requires stronger legislative protection and effective law enforcement. The right to data portability allows individuals to freely choose service providers because it facilitates the transfer of personal information between different service providers without hindrance. Such a right may be applied to inter-provincial social insurance, inter-provincial health insurance, and the unified credit system, which benefits data subjects as well. Moreover, the right to data portability plays a part in boosting a fair, healthy market, cutting off the monopoly of big data, and stimulating technological innovation.

The establishment of the right to data portability in the Personal Information Protection Law is a completely new attempt in China. It is undeniable that the right to data portability is still controversial among various jurisdictions and in academia worldwide. Under the background of rapid development of the emerging Internet economic industry, China has seized the opportunity at this time to actively improve its legislation on online personal information and caught up with the legislation of other jurisdictions. Meanwhile, China's provisions on the right to data portability are not sufficient, so the definition, operation, and regulatory rules of this new right need to be further improved. It is necessary to gradually implement the right to data portability, fully consider the current situation of China's data industry, and balance the interests of data enterprises. Considering the potential risks in the process of data portability, China should also establish and improve the assessment system of data portability accordingly to avoid conflicts with the legitimate rights and interests of third parties or malicious access to personal data of the data subjects by others.

However, given that the right to data portability was introduced into China as a legal concept just a few years ago and the legal provisions are quite general, the implementation of such a right remains to be further studied, and more specific rules and judicial interpretations are still required when practicing this new right.

Last but not least, we should also note that the threats to global cybersecurity continue to evolve, penalties for non-compliance are on the rise, international data transfers are under the spotlight, and navigating the evolving landscape of cross-border data flows will be essential⁶⁸ when the right to data portability involves cross-border elements. This might be another topic that Chinese scholars should focus on in future research.

(Edited by Gong Li)

中国数据可携带权的发展、挑战与对策

内容提要 数据可携带权是大数据时代个人信息保护的一项重要内容，与我们的生活息息相关。该权利的使用有助于维护数据主体的自决权，且有利于营造公平竞争的市场环境。在实践中，我国的数据携带权具有复杂性和不确定性。本文以我国第一部个人信息保护立法《中华人民共和国个人信息保护法》为视角对数据可携带权进行研究，回顾该权利相关立法及现状，探索数据可携带权对我国的未来影响，并通过与欧美国家的数据携带权立法与实践对比，提出完善数据可携带权实施的建议。

68 FRESHFIELDS LLP, *supra* note 20.