OPEN ACCESS Freely available online

IJSSAI
International Journal of Social Sciences and Artistic Innovations

ISSN 2737-5293
Issue 4, Volume 3
https://www.iikii.com.sg/journal/IJSSAI
International Journal of Social Sciences and Artistic Innovations

Article

Research on the Personal Data Portability Based on the Perspective of Property Rights Theory in the Context of Enterprise Digital Transformation

Mengze Chen [1,*], Xiaoxiao Chen [2]

[1] College of Foreign Languages and Literature, Fudan University, Shanghai 200437, China
[2] College of Education, University of Stirling, Stirling FK9 4LA, UK; EricaChen211@outlook.com
* Correspondence: chenmengze2022@foxmail.com

Received: Nov 15, 2023; **Revised:** Dec 6, 2023; **Accepted:** Dec 15, 2023; **Published:** Dec 30, 2023

Abstract: This study examines the right to data portability under the industrial economics theory, and addresses the problems of ambiguous boundaries, inconsistent formats, and data sharing. Based on the relational transactions in China, this study analyses the right to data portability from three aspects: transaction boundaries, transaction frequency, and exclusive nature. From the viewpoint of transaction uncertainty, it is necessary to clarify the content of transaction data and define the property rights boundary. From the view of transaction frequency, more detailed regulation of data processing mode is needed to reduce transaction costs in the future. The data processing mode needs to find a balance between security and rapidness. The data processing mode should imitate distributed data transfer protocol or decentralized recommendation system. From the perspective of asset exclusivity, data sharing should be classified for different users. The relationship between user privacy and data sharing should be properly balanced to prevent a "one-size-fits-all" data management model. This study applies property rights theory to address the issue of data portability, focuses on the economic benefits brought by data portability, and expands the perspective of the data portability's nature. Based on relational transactions in China, this study enriches the research of personal data protection in developing countries. In addition, the results provide a theoretical basis for government management, help define the boundary of digital assets, promote the digital transformation of cities, and facilitate sustainable economic development.

Keywords: The right to data portability, Property rights theory, Relational transactions, Personal Information Protection Law

1. Introduction

The problems of privacy proliferation and big data price discrimination become increasingly severe in the era of digital economy. Merchants collect or leak user-private information to make profits. Platforms collect consumer information without obtaining user consent to obtain consumer preferences (Tolmie & Crabtree, 2018). Collaborative recommender systems recommend preferred products to users by big data, but the systems expose more user data to the attackable environment, giving rise to the problem of privacy proliferation (Polatidis et al., 2017; Wu et al., 2018). Even though some platforms offer users the option to avoid tracking, the specific information usage is still vague (Chen et al., 2017).

To safeguard personal privacy issues, many countries have introduced relevant policies. The EU enacted the General Data Protection Regulation (GDPR) in May 2018, which defines the right of data subjects to access their data (European Society of Radiology, 2017). USA passed the California Privacy Protection Act (CCPA) in 2020. The Chinese government enacted the Personal Information Protection Law of the People's Republic of China (hereinafter referred to as the "Personal Information Protection Law") on November 1, 2021. Similar to other developing countries, China lacked a specific privacy protection law and mostly addressed the issue of privacy infringement through sporadic laws such as consumer protection laws and human rights laws (Balsari et al., 2018). The Personal Information Protection Law marked China's move from sporadic laws to specialized legislation, providing basic institutional safeguards for the protection of personal information rights, promoting the development of China's digital economy, and demonstrating China's determination to integrate into globalized digital governance and converge with international standards.

Although many countries have enacted personal information protection laws successively, the specific scope of the right to data portability's application varies. CCPA defines data portability as "a business shall consider the methods by which it interacts with consumers, the manner in which the business sells personal information to third parties, available technology, and ease of use

by the consumer when determining which methods consumers may use to submit requests to opt-out." Article 20 of GDPR defines data portability as "the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided." Article 45 of China's Personal Information Protection Law defines that "if an individual requests the transfer of personal information to designated personal information processor, the personal information processor should provide the means to transfer if the conditions stipulated by the State Internet Information Department are met." It can be seen that the scope of the right to data portability's application is inconsistent in different countries. As for whether the right to data portability is a property right or a human right, there are controversies in different countries (Balsari et al., 2018; Borgogno & Colangelo, 2019; De Hert et al., 2018; Li, 2018).

On the one hand, the right to data portability has its unique advantages. Firstly, personal data portability further strengthens users' control over their data by granting them the right to access and port their data. Data portability protects privacy, allows users to display different data to reveal their unique personalities, and safeguards their freedom (Ramos & Blind, 2020; Wohlfarth, 2019). Secondly, the right to data portability standardizes data sharing, breaks monopolies, and improves market competition. The first company to enter the market can access a large amount of user data and attract more users, forming a virtuous circle for the company. However, at the same time, it also raises the market entry barrier and forms a monopoly. New enterprises have difficulty in accessing user data and cannot provide quality services. As a result, users flow to monopolistic enterprises, forming a vicious circle. The right to data portability promotes fair competition between large and small enterprises by forcing enterprises to transmit data, reducing user lock-in effects, breaking data barriers, and reducing transfer costs. The right to data portability promotes enterprises to enhance their services and products, thus improving user satisfaction (Colangelo & Maggiolino, 2019; Mercille, 2021; Ramos & Blind, 2020; Zhuo, 2019). Finally, the right to data portability can advance the pace of social innovation. The world will witness an explosion of companies with data processing as their core business, making raw data more useful and accelerating the process of social innovation (De Hert et al., 2018).

On the other hand, the right to data portability also has some negative effects on the limitations associated with data. Firstly, the use of the right to data portability can lead to increased costs for companies, which will then be passed on to the user side. The loss of social platform interactivity due to the restriction of cross-platform access limits users' freedom of personality to access across platforms (Graef, 2015; Kramer & Stallein, 2019; Wäljas et al., 2010). Secondly, the right to data portability restrictions may deepen monopolies. Given that data interoperability is very difficult, the right to data portability can increase the cost of small businesses and create a monopoly for large businesses, resulting in a loss of user benefits (Borgogno & Colangelo, 2019; Zhuo, 2019). Thirdly, the right to data portability makes data processing and control more complex. It is more difficult to control infringement, identity definition, etc., leading to security risks (Van der Auwermeulen, 2017). Finally, since the right to data portability is not a mature right (Ding, 2020) and has ambivalence in the definition itself (Zhuo, 2019), developing countries are not yet in a position to establish the right to data portability. Therefore, more controversies exist in the data portability studies.

This study focuses on the attributes of the right to data portability based on property rights theory, examines the applicability to China in terms of transaction uncertainty, transaction frequency, and exclusivity, and further studies the impact of the right to data portability on the enterprises' digital transformation and government's digital governance. This study points out that from the perspective of transaction uncertainty, it is necessary to clarify the scope of transactional data content, define the property rights boundary, and appropriately expand the scope of the right to data portability based on the relational transactions in China. In terms of transaction frequency, more detailed specifications for the data processing mode are needed in the future to reduce transaction costs. The data processing mode needs to find a balance between security and speed, and the data processing mode should imitate distributed data transfer protocols or decentralized recommendation systems. From the viewpoint of asset exclusivity, data sharing classifications should be made for different users and different data heterogeneous ranges should be specified according to different customer categories to encourage certain boundaries of data sharing.

This study has the following contributions. Firstly, most existing studies examine the right to data portability from the legal and rights perspectives (Borgogno & Colangelo, 2019; De Hert et al., 2018; Ding, 2020; European Society of Radiology, 2017; Kolasa et al., 2020; Stalla-Bourdillon et al., 2018; Urquhart et al., 2018). This paper uses industrial economics theory to address the issue of the right to data portability, focusing on the economic benefits brought by the right to data portability and expanding the perspective of portability. Secondly, the existing literature focuses on the functions of the right to data portability under the GDPR framework, with less attention to the application of the right to data portability in developing countries (Borgogno & Colangelo, 2019; Colangelo & Maggiolino, 2019; De Hert et al., 2018; Hesse & Teubner, 2020; Ramos & Blind, 2020). Relational transactions are common in Chinese companies (Fang & Zhang, 2016; Li, 2017). This study focuses the right to data portability based on relational transactions in China, which enriches the research results on personal data protection in developing countries. Finally, the

results of this study have certain practical significance, which providing a theoretical basis for government management, helping to define the boundary of digital assets, promoting digital transformation of cities, and facilitating sustainable economic development.

2. Legal Framework and Literature Review

2.1. Comparison of Legal Frameworks for the Right to Data Portability

Many countries rely on the GDPR to introduce bills related to the right to data portability. Developed countries have an early start on data protection laws, such as the US, which passed the Privacy Act in 1974 and issued the CCPA in 2018; the UK passed the Data Protection Act in 1984; Australia published the Privacy Act in 1988 and the Australian Consumer Data Right (CDR) came into force in 2019; Japan published the Personal Information Protection Act in 2005. Developing countries started late with data protection bills, such as China's Personal Information Protection Law coming into force in 2021, India's Personal Data Protection Bill in 2018, Pakistan's Personal Data Protection Bill in 2020, Brazil's General Data Protection Law (LGPD) in 2020, and Russia's Federal Personal Data Law in 2006. Some developing countries, such as India and Pakistan, have many provisions borrowed from the GDPR with fewer changes (Javed et al., 2020); other developing countries, such as China and Russia, develop bylaw provisions according to national conditions (Wang & Ding, 2021; Zharova & Elin, 2017).

China issued the Cyber Security Law of the People's Republic of China (Cyber Security Law) on November 7, 2016, which sets out the scope of protection for information infrastructure, establishes the principle of sovereignty in cyberspace, and protects consumer interests (Wang, 2017; Zhang, 2016). The Data Security Law of the People's Republic of China (Data Security Law), which came into force on September 1, 2020, is the first law on data security management in China, promoting data utilization and establishing a hierarchical data management system (Deng, 2020). On November 1, 2021, the Personal Information Protection Law came into effect, which is the first law for personal information protection in China, mentioning the right to data portability for the first time and legislating clearly that data controllers shall not over-collect personal information. So far, the Network Security Law, Data Security Law, and Personal Information Protection Law have become the three major regulations of network data security in China. The advantages of the Personal Information Protection Law are: firstly, it elevates the legal status of personal information rights by extending the protection of personal information to the Constitution. Secondly, it focuses on vulnerable groups and provides a higher degree of protection for minors. Thirdly, it establishes special provisions to regulate the problems reflected by society, such as big data price discrimination. It reflects the people-oriented concept by protecting the right of individuals to use their data. However, there are still some problems with the description of the right to data portability. First, the concept is not clear and the relevant principles and technical conditions are still vague. When the right to data portability conflicts with the rights owned by the enterprise itself, it is not clear how to arbitrate. Second, the feasibility of the right to data portability is not strong. The introduction of the right to data portability is not equal to effective implementation. China lacks experience in data transfer, and it is unclear how to effectively enforce the right to data portability and regulate the enterprises.

Table 1 compares developed and developing countries' bills on the right to data portability in terms of four aspects: conditions of use, the definition of personal information, applicable objects, and special provisions. Compared to developed countries, developing countries tend to exclude government agencies because of the different economic systems and strong government intervention in developing countries. However, all countries generally lack specific descriptions of the scope of the right to data portability. Even if the GDPR and other laws state "conditionally permitted", the definition of "condition" itself is not clear. Therefore, this paper will study the scope of the right to data portability to provide a theoretical basis for the government to add specific descriptions.

Table 1. Comparison of the right to data portability provisions by country.

The Right to Data Portability	Scope of the Right to Data Portability	Definition of Personal Data	Applicable Subjects	Special Terms
Developed Countries:				
EU GDPR	prohibited in principle, allowed with conditions	wide range of protection	extraterritorial applicability	require companies to hire data protection officers
American CCPA	allowed in principle, conditionally prohibited	scope limitation and clarity	residents of California	have a prohibition of discrimination
Australian CDR	no clear description	wide range of protection	extraterritorial applicability	focus on the regulation of enterprises
Japanese APPI	no clear description	wide range of protection	exclusion of government agencies within the scope of other regulations	/
Developing Countries:				
Russian Federal Personal Data Law	no clear description	wide range of protection	exclude many government agencies	focus on the technical requirements, providing specific technical standards for data protection
Chinese Personal Information Protection Law	prohibited in principle, allowed with conditions	wide range of protection	extraterritorial applicability	prohibit big data price discrimination
Brazilian General Protection Law	no clear description	wide range of protection	exclude government agencies	excluding data explicitly disclosed by the data subject
Indian Personal Data Protection Bill	no clear description	wide range of protection	extraterritorial applicability	/

2.2. Literature Review of the Attribute of the Right to Data Portability

There is no unanimous academic opinion on whether the attribute of the right to data portability is a human right or a property right (Balsari et al., 2018; Borgogno & Colangelo, 2019; De Hert et al., 2018; Li, 2018). Supporting the right to data portability as a human right is mainly reflected in the following aspects: First, the right to data portability guarantees the basic human rights of individuals. By giving data subjects greater control over their personal data, the right to data portability can safeguard personal privacy and maintain personal dignity (Zhuo, 2019). Second, the right to data portability takes precedence over respect for the rights of people. India's Personal Data Protection Bill, for example, provides that when the data providing subject is unable to provide consent due to illiteracy, medical condition, etc., the choice should be in the interest of the data subject (Balsari et al., 2018). Finally, property rights should be widely available, but data portability rights are too limited in scope and not widely available (Borgogno & Colangelo, 2019).

Supporting the right to data portability as a property right is mainly reflected in the following aspects: first, users have the bargaining power, which brings property rights. The right to data portability gives users the right to allow platforms to transmit data to third parties, making the online market a "user market", which gives users bargaining power among platforms (Zhuo, 2019). Second, the right to data portability has the economic benefits of property rights. User data allows companies to make accurate recommendations, have precise marketing, and increase user stickiness and satisfaction (De Hert et al., 2018; Li, 2018; Van der Auwermeulen, 2017). Finally, the right to data portability is closely related to the intellectual property law. Therefore, it has property rights as intellectual property law does (Van der Auwermeulen, 2017).

3. Study on the Attributes of the Right to Data Portability Based on Property Rights Theory

A property right is a bundle of rights that includes three aspects: the right to use, the right to benefit, and the right to transfer. Among them, the right to transfer is the key to the contract, because only transferable property rights can achieve the matching of benefits and costs and ensure the professionalism of property rights usage (Alchian, 1965). The subject of data portability is users, and the prerequisite for the realization of the freedom of data transfer is that users must know and agree to the re-transaction and processing of data. Otherwise, it will inevitably lead to the problem of privacy leakage. Faced with the outstanding problems of personal information protection, it is necessary to regulate the boundary of the right to data portability and ensure the exclusivity of data. Any transaction is an exchange of property rights, and transaction costs are incurred due to the measurement and enforcement of property rights and are minimized within the transaction method (Williamson, 1989). The factors influencing transaction costs can be examined from the characteristics of the transaction, including uncertainty, frequency of transactions, and asset exclusivity (Mathur et al., 1979). Whether state-owned or private, Chinese firms are more likely to choose relational transactions which are significantly different from the market-based transactions commonly used in developed countries (Li, 2017). Therefore, based on China's relational transactions, this paper will analyze the governance of data portability from three aspects: transaction boundary, transaction frequency, and asset exclusivity. The research framework is shown in Fig. 1 below.

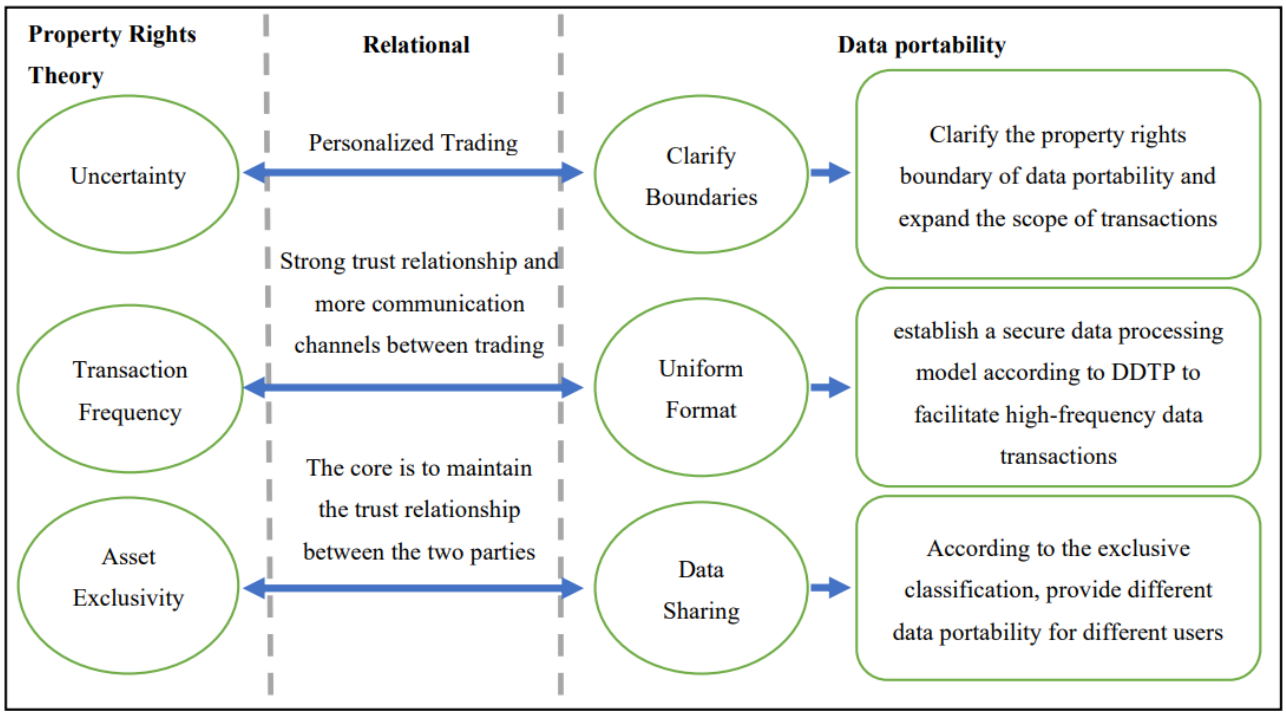

Fig. 1. Study of Data Portability Based on Property Rights Theory.

First of all, from the perspective of the uncertainty of the transaction, as China currently does not have a clear attribute of the right to data portability, the boundary of the right to data portability is vague and the scope of the transaction is unclear. The problems of generalization of rights and personal data trafficking are serious. In China, relational transactions mean that both sides of the transaction have significant personality characteristics, bound after investment, and market competition cannot automatically eliminate immoral behavior (Chen et al., 2010; Li, 2017). If the right to data portability is extended to the transferable data, it will potentially induce enterprises to buy and sell personal data for relational transactions, thus causing personal privacy leakage. From the perspective of commercial credit, to compensate for the adverse effects of commercial credit, enterprises may buy and sell personal data in the case of unclear regulations on the right to data portability. Therefore, it is necessary to clarify the scope of traded data and define the boundary of property rights based on the context of relational transactions in China. The right to data portability is a manifestation of the conflict between access to information and personal privacy. As a result, the scope of the right to data portability transactions needs to be clarified to balance the conflict between digital economy development and personal privacy (Li, 2018). Article 20(1) of the GDPR limits the scope of the right to data portability to "the personal data concerning him or her, which he or she has provided to a controller". However, the GDPR's provisions on data portability itself are somewhat contradictory, emphasizing the non-mandatory obligations of platforms while regulating "machine-readable". Platforms are encouraged but not

obligated to build interactive data transfer formats, giving them the possibility to refuse to enforce the right to data portability (Wong & Henderson, 2019).

Article 27 of China's Personal Information Protection Law defines the scope of data portability as "the processor of personal information may, within a reasonable range, process personal information that the individual has disclosed on his own or has otherwise legally disclosed, except when the individual expressly refuses to do so". This definition excludes anonymized data or data unrelated to the data subject, i.e. data processed by the platform (De Hert et al., 2018). This definition is legally supported by the 2011 case of Dianping.com against AiHelp.com and the 2016 case of Dianping.com against Baidu Maps for unfair competition. The court held that the online data of Dianping.com was the result of its operation of a huge cost. AiHelp and Baidu Map's obtaining the data directly from Dianping.com constituted unfair competition. From the perspective of data portability, the information of user reports and reviews produced by the platform are not related to the data subject, not within the scope of protection of the right to data portability. However, the "within a reasonable range" in the article makes the boundary of data portability blur again. Article 27 of the Personal Information Protection Act states that the scope of the right to data portability shall include data involving multiple persons, such as telephone calls, interpersonal interactions, or network communication records, provided that the rights and freedom of third parties are not adversely affected. However, the definition of third-party rights and freedom is again a blurred line. The ultimate right to transmit group photos of multiple people (Urquhart et al., 2018) and whether users' friend information data is allowed to be transmitted together (Tolmie & Crabtree, 2018; Van der Auwermeulen, 2017) are both at the fuzzy boundary.

In determining the boundaries of the right to data portability, the differences between the draft GDPR and the official document, viewed from international legal experience, show that the right to data portability under GDPR is restrictive. The scope of the right to data portability is defined in the draft as "data being processed", while in the official document it is limited to "the personal data concerning him or her, which he or she has provided to a controller". As for the data format, it is "electronic, structured and commonly used format" in the draft, but reduced to "machine-readable" in the official document. These points limit the scope of GDPR data portability (De Hert et al., 2018). China's data portability law can appropriately expand the scope of the right to data portability by removing the limitation that data should only be provided by the data subject. That is, if user B wants to transfer data related to user A, he can do so with user A's consent. The government can require that users' consent as a third-party data subject should be sought before using the platform. If user A consents for his/her data to be transferred before using the platform, then when his/her friend B requests exercise of the right to data portability to transfer friends list, user A's data can be transferred directly without the need to ask for consent again. If user A does not consent, any of user A's friends will not include user A's data when transferring their friends list. Certainly, the right to data portability should not infringe upon a person's legal rights. In case of suspected infringement, the individual has the right to request the platform to delete the data.

Secondly, from the perspective of transaction frequency, due to urbanization transformation, enterprises have accelerated the process of digital transformation, and the frequency for data transactions has increased significantly. The lack of data transfer norms results in the excessive use of personal data. The big data model also makes data storage control more complicated (Ellis & Leek, 2018; Peisert et al., 2018; Van der Auwermeulen, 2017). In the context of relational transactions in China, there is a strong relationship of trust and more channels of information communication between the parties. Relational transactions allow China to have more frequent transactions than developed countries, because it is only profitable to establish relational transactions if the frequency of transactions is high enough (Li, 2017). However, the data processing mode has not been gradually standardized as the frequency of transactions increases, making data transmission extremely difficult. In the future, a more detailed specification of the data processing mode is needed to reduce transaction costs. GDPR gives three different rights to data subjects: receiving the personal data concerning him or her, which he or she has provided to a controller, having the personal data transmitted directly from one controller to another and receiving machine-readable data. The first two have small technical requirements, but the third right relies on technical operability (Borgogno & Colangelo, 2019). Chapter 5 Articles 44-46 of China's Personal Information Protection Law gives data subjects three different rights: individuals have the right to know and decide on the processing of their personal information and the right to restrict or refuse the processing of their personal information by others; individuals have the right to access and copy their personal information from the personal information processor and the transfer route shall be provided when individuals request the transfer of their personal information to the designated processor; individuals have the right to request the deletion of information that has not been deleted by the information processor. In order to make data transfer possible, data format specifications are needed to reduce exchange costs (Haile & Altmann, 2018). The data processing mode needs to ensure both security and efficient data transfer. If the data processing mode is too complex, there will be too many formats conversion steps, severely reducing the efficiency of data transmission (Courbier et al., 2019). If the data processing mode is too simple, it is vulnerable to successful theft by hackers, resulting in large data leakage. GDPR requires the data format to be "structured, commonly used and machine-readable". The Personal Information Protection Act does not explicitly mention format requirements, stating only that "processors of personal information shall provide a means of transfer". The GDPR defines "machine-readable" as "a format that

enables software applications to easily identify, recognize and extract specific data"(Ding, 2020). It means that the platform should develop software with an "import-export" module, but this requires more data connect points, making it easier for third-party platforms to access user data and a greater possibility of exposing user data (Zhuo, 2019).

The data processing mode needs to find a balance between security and speed. First, platforms of the same data type should develop their own industry specifications. For example, image type data and location type data each have their own internal compatible specifications. Second, different data types use common open format data between platforms and unify the format of data output. The format depends on the specific scenario and technical level, enabling the circulation of data between platforms. Finally, a decentralized data processing system should be established by imitating the decentralized recommendation system (Casino & Patsakis, 2020; Urquhart et al., 2018). Compared to collaborative recommender systems, decentralized data processing systems decentralize the placement of data and reduce data exposure, thus better protecting data. Data transfer guidelines can also be established based on Distributed Data Transfer Protocol (DDTP) and blockchain technology. Data security can be ensured through verifiable digital credentials "digital fingerprints", thus better facilitating high-frequency data transactions.

Finally, from the perspective of asset exclusivity, data sharing should be carried out accordingly for different users, balancing the relationship between user privacy and data sharing. If personal privacy is overly protected, it is not conducive to the economic utility of personal data. If sharing is overly encouraged, it brings an impact on personal privacy (Guo et al., 2018; Wang, 2019). The core of relational transactions in China is the asset exclusivity that maintains the trust between the parties, because its counterparty identity is derived from exclusive investments made in the transaction, and the value of this exclusive asset is sufficient to guarantee automatic compliance by both parties (Li, 2017). Relational transactions exclusive assets can correspond to data portability asset exclusivity, and simplify the data portability classification by classifying the existing exclusive assets. The right to data portability should allow a certain range of data sharing, promote trust between users and data controllers, and achieve a win-win situation for both users and data controllers (Urquhart et al., 2018). In fact, under the premise of privacy protection, users are often willing to authorize part of their personal data to reduce the transfer cost in exchange for more convenient services. The transfer cost refers to the fact that when users switch between platforms, the corresponding personal data, such as friends list, search history, etc., cannot be transferred, which brings great inconvenience to users (Ramos & Blind, 2020).

The right to data portability can be classified by exclusivity. On the one hand, the "one-size-fits-all" model of data licensing should be eliminated and categorical licensing should be used (Waithira et al., 2019). Currently, there are only two models, full authorization and no authorization which are too extreme and will bring economic losses. Hence, partial authorization options are needed. China's Notice on Information and Communication Service Perception Enhancement Action stipulates that "embedded SDKs shall not start themselves or start associated with each other when they are not necessary for the service or have no reasonable application scenarios". SDKs cannot obtain any data when unnecessary, so the collaborative recommender systems cannot work and the platform cannot make accurate recommendations. The user purchase rate decreases, leading to the decline of enterprise revenue and the national economic downturn. Therefore, classification authorization should be used to set three types of data: unconditionally open, conditionally open, and non-open. For different categories of data, users can be given different levels of protection, and different levels of identity verification can be stipulated to ensure data security. For transmission of high privacy data containing ID information, users can be required to provide ID photos or face recognition to confirm their identity; for transmission of medium privacy data such as frequently visited web pages and frequently visited locations, users can be required to answer pre-set secret security questions; for transmission of low privacy data such as personalized signatures, users can merely provide account numbers and passwords. For the boundary determination of high, medium, and low sensitivity data, the platform can collect the user's priority for the sensitivity level of different data. When users request wielding the right to data portability, different levels of identity verification are conducted according to the pre-collected sensitive data table to ensure that no others impersonate the user's identity for data transmission and therefore guarantee information security. On the other hand, the platform data processing mode possesses exclusivity. For different platforms, data information is important in different degrees. For map navigation software, the user geolocation information is more important than the age information (Ramos & Blind, 2020). Platforms can set up the exclusive data processing mode based on high, medium, and low privacy data, using the complex processing mode for high privacy data and the simple processing mode for low privacy data. When there is inconsistency in privacy classification between platforms like when the private part of one platform is released as public by another platform (Urquhart et al., 2018), platforms can complete the interconversion of high privacy and low privacy data through transcoding to achieve accessible data transmission.

4. Exploring the Path of Smart City Development from a Data Portability Perspective

4.1. Government

First, the government should strengthen the training of legal knowledge for the public and enhance their awareness of the law. After introducing relevant regulations, the government should publish an explanatory document that converts legal language into everyday language and uses everyday examples for explanations when necessary. The government should also provide community outreach services for people who have difficulty using the Internet (Lytras & Serban, 2020). Next, the government should build the transmission platform regularly, requiring the platform to send monthly data transmission reports to users to address the public's concerns about data leakage of data portability (Urquhart et al., 2018). The report should state the number of data transfer requests, the number of successes, and the object of the transfer platform, so that users can grasp the flow of their personal data. Next, the government should provide policy support to the technology related to data portability. International data portability is basically non-mandatory. For example, the law states that "where technically feasible", i.e., it is not mandatory for corporate data to be machine-readable, and companies are encouraged instead of obliged to use interactivity formats (De Hert et al., 2018). These statements give companies the possibility to delay and not cooperate with the right to data portability. The government needs to introduce policies to encourage companies to develop appropriate technologies. Given that large companies have more time and money to develop relevant technologies (Borgogno & Colangelo, 2019), the government can start with large companies and promote the development of related technologies through financial subsidies, tax reduction, and other policies to better realize the right to data portability. Finally, the government should focus on the boundary issue of the right to data portability. The exclusive classification does not mean indulging in data sharing. The government still needs to restrict profile authorization, and the platform needs to obtain another user's authorization when sharing data again to ensure that the platform uses the data within the scope of authorization (Wang, 2019).

4.2. Company

From the perspective of enterprises, first of all, competitive market enterprises should build a transparent transaction information network. Competitive market enterprises will strengthen data innovation to attract users or even third-party platform users to their end. They are more willing to make the data processing mode easy to read so that they can easily read user data. Competitive market enterprises can record and track transaction information within the scope of the right to data portability, constitute a transparent transaction information network, and achieve the equilibrium effect in the Stackelberg game to implement a win-win situation for both the data output and input enterprises, helping the construction of smart cities. Secondly, the winner-takes-all market should develop technological innovation. Companies in winner-take-all markets are inert to innovation because it increases the possibility of user abandonment (Ramos & Blind, 2020). Therefore, they do not want their own data to flow out and want to raise the market entry barrier and put obstacles in the way of the other party's access to information. As large companies, winner-takes-all type of companies can undertake technological innovation. According to the frequency of transactions, develop "machine-readable" data transmission technology to better promote high-frequency data transactions under the premise of ensuring data security (Bagloee et al., 2021; Guo et al., 2018). Finally, enterprises should be elastic in setting data portability boundary issues. According to asset exclusivity, different data carrying rights should be established for different users, and the scope of data sharing should be flexibly scaled. For users with a high trust level, the company should provide large-scale data sharing, and for users with a low trust level, small scale data sharing.

4.3. Society

From a social perspective, on the one hand, the right to data portability needs individual consciousness to be truly implemented. Data subjects need to use the right to data portability actively and consciously in order to maximize the role of the right to data portability (Turner et al., 2021). Although the right to data portability provides people with the right to access their own information, users often have no incentive to exercise the right to data portability because of data access cost, personal benefits, etc. (Graef & Prufer, 2021). On the other hand, individuals are also able to regulate whether companies are enforcing the right to data portability regulations. Relational transactions in China do not only exist between enterprises, but also between users and enterprises. Companies need to build their reputation and increase user trust. Users usually provide data to the companies they trust (Urquhart et al., 2018). Users choose regulated enterprises to provide data, pushing non-compliant enterprises to rectify, which implements the function of regulating enterprises.

5. Conclusions

This study focuses on the attributes of the right to data portability based on property rights theory. Firstly, the right to data portability is extended by using industrial economics theory. Based on relational transactions in China, this study enriches the results of personal information protection in developing countries. It provides a theoretical basis for the government to manage data, helps promote the definition of personal digital asset boundaries, and advances the digitalization process of cities and sustainable economic development. Secondly, this study elaborates on three aspects: transaction boundaries, transaction frequency, and asset exclusivity. From the perspective of transaction uncertainty, the scope of the right to data portability needs to be clarified in the future, and the property rights boundary needs to be defined. From the perspective of transaction frequency, a more standard data processing mode is needed in the future, imitating distributed data transfer protocols or decentralized recommendation systems to find a balance between security and speed. From the perspective of asset exclusivity, the future should establish a categorized data sharing database for different users, prevent a "one-size-fits-all" mode, and find a balance between user privacy and data sharing. Finally, the government, enterprises, and society should choose the path of smart city development. The government should introduce policies to encourage people to use the right to data portability and encourage enterprises to develop related technologies; enterprises should flexibly choose the boundaries of the right to data portability according to their own characteristics to promote data sharing; individuals in society should take the initiative to exercise the right to data portability and regulate the enterprises' protection of personal data.

Author Contributions: conceptualization, M. Chen; methodology, M. Chen; resources, M. Chen and X. Chen; writing—review and editing, M. Chen; visualization, M. Chen; supervision, M. Chen and X. Chen. All authors have read and agreed to the published version of the manuscript.

Funding: This research did not receive external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alchian, A.A. (1965). The basis of some recent advances in the theory of management of the firm. *Journal of Industrial Economics*, *14*(1), 30–41. https://doi.org/10.2307/2097649
2. Bagloee, S.A., Heshmati, M., Dia, H., Ghaderi, H., Pettit, C., & Asadi, M. (2021). Blockchain: The operating system of smart cities. *Cities*, *112*, 103104. https://doi.org/10.1016/j.cities.2021.103104
3. Balsari, S., Fortenko, A., Blaya, J.A., Gropper, A., Jayaram, M., Matthan, R., Sahasranam, R., Shankar, M., Sarbadhikari, S.N., Bierer, B.E., Mandl, K.D., Mehendale, S., & Khanna, T. (2018). Reimagining Health Data Exchange: An Application Programming Interface-Enabled Roadmap for India. *Journal of Medical Internet Research*, *20*(7), e10725. https://doi.org/10.2196/10725
4. Borgogno, O., & Colangelo, G. (2019). Data sharing and interoperability: Fostering innovation and competition through APIs. *Computer Law & Security Review*, *35*(5), 105314. https://doi.org/10.1016/j.clsr.2019.03.008
5. Casino, F., & Patsakis, C. (2020). An Efficient Blockchain-Based Privacy-Preserving Collaborative Filtering Architecture. *IEEE Transactions on Engineering Management*, *67*(4), 1501–1513. https://doi.org/10.1109/tem.2019.2944279
6. Chen, D.Z., Fraiberger, S.P., Moakler, R., & Provost, F. (2017). Enhancing Transparency and Control When Drawing Data-Driven Inferences About Individuals. *Big Data*, *5*(3), 197–212. https://doi.org/10.1089/big.2017.0074
7. Chen, Y.Y., Yuan, Y.J., & Wang, L.L. (2010). Intermediary, Rent-seeking Network, and Corruption Deal: Empirical Research Based on Provincial Panel Data of China. *Nankai Economic Studies*, 2, 3–16. https://doi.org/10.14116/j.nkes.2010.02.003
8. Colangelo, G., & Maggiolino, M. (2019). From fragile to smart consumers: Shifting paradigm for the digital era. *Computer Law & Security Review*, *35*(2), 173–181. https://doi.org/10.1016/j.clsr.2018.12.004
9. Courbier, S., Dimond, R., & Bros-Facer, V. (2019). Share and protect our health data: An evidence based approach to rare disease patients' perspectives on data sharing and data protection-quantitative survey and recommendations. *Orphanet Journal of Rare Diseases*, *14*, 175. https://doi.org/10.1186/s13023-019-1123-4
10. De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, *34*(2), 193–203. https://doi.org/10.1016/j.clsr.2017.10.003
11. Deng, L.B. (2020). Unscrambling of Data Security Law of P.R.C. (Draft) and Countermeasure Suggestions of Library & Intelligence Circles in China. *Journal of Information*, *39*(12), 83–87.
12. Ding, X.D. (2020). On the Properties, Impact and Application of Data Portability in China. *Studies In Law and Business*, *37*(1), 73–86.

13. Ellis, S.E., & Leek, J.T. (2018). How to Share Data for Collaboration. *American Statistician*, *72*(1), 53–57. https://doi.org/10.1080/00031305.2017.1375987
14. European Society of Radiology (ESR). (2017). The new EU General Data Protection Regulation: what the radiologist should know. *Insights into Imaging*, *8*(3), 295–299. https://doi.org/10.1007/s13244-017-0552-7
15. Fang, H.X., & Zhang, Y. (2016). Supplier /Customer Relationship Transaction, Earnings Management and the Auditor's Decision-Making Behavior. *China Journal of Accounting Studies*, 1, 79–86. https://doi.org/10.3969/j.issn.1003-2886.2016.01.011
16. Graef, I. (2015). Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union. *Telecommunications Policy*, *39*(6), 502–514. https://doi.org/10.1016/j.telpol.2015.04.001
17. Graef, I., & Prufer, J. (2021). Governance of data sharing: A law & economics proposal. *Research Policy*, *50*(9), 104330. https://doi.org/10.1016/j.respol.2021.104330
18. Guo, B.Y., Deng, X.F., Guan, Q.S., Tian, J., & Zheng, X.W. (2018). An Incentive Mechanism for Cross-Organization Data Sharing Based on Data Competitiveness. *IEEE Access*, *6*, 72836–72844. https://doi.org/10.1109/access.2018.2882233
19. Haile, N., & Altmann, J. (2018). Evaluating investments in portability and interoperability between software service platforms. *Future Generation Computer Systems—The International Journal of Escience*, *78*, 224–241. https://doi.org/10.1016/j.future.2017.04.040
20. Hesse, M., & Teubner, T. (2020). Reputation portability - quo vadis? *Electronic Markets*, *30*(2), 331–349. https://doi.org/10.1007/s12525-019-00367-6
21. Javed, Y., Salehin, K.M., & Shehab, M. (2020). A Study of South Asian Websites on Privacy Compliance. *IEEE Access*, *8*, 156067–156083. https://doi.org/10.1109/access.2020.3019334
22. Kolasa, K., Redekop, W.K., Berler, A., Zah, V., & Asche, C.V. (2020). Future of Data Analytics in the Era of the General Data Protection Regulation in Europe. *Pharmacoeconomics*, *38*(10), 1021–1029. https://doi.org/10.1007/s40273-020-00927-1
23. Kramer, J., & Stallein, N. (2019). Data portability, data disclosure and data-induced switching costs: Some unintended consequences of the General Data Protection Regulation. *Economics Letters*, *181*, 99–103. https://doi.org/10.1016/j.econlet.2019.05.015
24. Li, W.L. (2018). A tale of two rights: exploring the potential conflict between right to data portability and right to be forgotten under the General Data Protection Regulation. *International Data Privacy Law*, *8*(4), 309–317. https://doi.org/10.1093/idpl/ipy007
25. Li, Z.Q. (2017). The Governance Role of Accounting in Relationship-based Transactions:Paradigm Exploration of Internationalized China's Accounting Research. *Journal of Finance and Economics*, *43*(2), 4–33. https://doi.org/10.16538/j.cnkij.fe.2017.02.001
26. Lytras, M.D., & Serban, A.C. (2020). E-Government Insights to Smart Cities Research: European Union (EU) Study and the Role of Regulations. *IEEE Access*, *8*, 65313–65326. https://doi.org/10.1109/access.2020.2982737
27. Mathur, S., Williamson, H.O., Landgrebe, S.C., Smith, C.L., & Fudenberg, H.H. (1979). Application of passive hemagglutination for evaluation of antisperm antibodies and a modified coombs-test for detecting male auto-immunity to sperm antigens. *Journal of Immunological Methods*, *30*(4), 381–393. https://doi.org/10.1016/0022-1759(79)90020-6
28. Mercille, J. (2021). Inclusive Smart Cities: Beyond Voluntary Corporate Data Sharing. *Sustainability*, *13*(15), 8135. https://doi.org/10.3390/su13158135
29. Peisert, S., Dart, E., Barnett, W., Balas, E., Cuff, J., Grossman, R.L., Berman, A., Shankar, A., & Tierney, B. (2018). The medical science DMZ: A network design pattern for data-intensive medical science. *Journal of the American Medical Informatics Association*, *25*(3), 267–274. https://doi.org/10.1093/jamia/ocx104
30. Polatidis, N., Georgiadis, C.K., Pimenidis, E., & Mouratidis, H. (2017). Privacy-preserving collaborative recommendations based on random perturbations. *Expert Systems with Applications*, *71*, 18–25. https://doi.org/10.1016/j.eswa.2016.11.018
31. Ramos, E.F., & Blind, K. (2020). Data portability effects on data-driven innovation of online platforms: Analyzing Spotify. *Telecommunications Policy*, *44*(9), 102026. https://doi.org/10.1016/j.telpol.2020.102026
32. Stalla-Bourdillon, S., Pearce, H., & Tsakalakis, N. (2018). The GDPR: A game changer for electronic identification schemes? The case study of Gov.UK Verify. *Computer Law & Security Review*, *34*(4), 784–805. https://doi.org/10.1016/j.clsr.2018.05.012
33. Tolmie, P., & Crabtree, A. (2018). The practical politics of sharing personal data. *Personal and Ubiquitous Computing*, *22*(2), 293–315. https://doi.org/10.1007/s00779-017-1071-8
34. Turner, S., Galindo Quintero, J., Turner, S., Lis, J., & Tanczer, L.M. (2021). The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment. *New Media & Society*, *23*(10), 2861–2881.
35. Urquhart, L., Sailaja, N., & McAuley, D. (2018). Realising the right to data portability for the domestic Internet of things. *Personal and Ubiquitous Computing*, *22*(2), 317–332. https://doi.org/10.1007/s00779-017-1069-2
36. Van der Auwermeulen, B. (2017). How to attribute the right to data portability in Europe: A comparative analysis of legislations. *Computer Law & Security Review*, *33*(1), 57–72. https://doi.org/10.1016/j.clsr.2016.11.012
37. Waithira, N., Mutinda, B., & Cheah, P.Y. (2019). Data management and sharing policy: the first step towards promoting data sharing. *BMC Medicine*, *17*, 80. https://doi.org/10.1186/s12916-019-1315-8

38. Wäljas, M., Segerståhl, K., Väänänen-Vainio-Mattila, K., & Oinas-Kukkonen, H. (2010). Cross-platform service user experience: A field study and an initial framework. In Proceedings of the 12th International Conference on Human Computer Interaction with Mobile Devices and Services, New York, NY, USA, September 7, 2010; pp. 219–228.
39. Wang, C.H. (2017). Analysis of six legal systems on Cyber Security Law. *Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition)*, *37*(1), 1–13. https://doi.org/10.14132/j.cnki.1673-5439.2017.01.001
40. Wang, L.M. (2019). Data Sharing and Personal Information Protection. *Modern Law Science*, *41*(1), 45–57.
41. Wang, L.M., & Ding, X.D. (2021). On the Highlights, Characteristics and Application of Personal Information Protection Law. *The Jurist* 6, 1–16. https://doi.org/10.16094/j.cnki.1005-0221.2021.06.001
42. Williamson, O.E. (1989). Transaction cost economics. *Handbook of Industrial Organization*, *1*, 135–182.
43. Wohlfarth, M. (2019). Data Portability on the Internet An Economic Analysis. *Business & Information Systems Engineering*, *61*(5), 551–574. https://doi.org/10.1007/s12599-019-00580-9
44. Wong, J., & Henderson, T. (2019). The right to data portability in practice: exploring the implications of the technologically neutral GDPR. *International Data Privacy Law*, *9*(3), 173–191. https://doi.org/10.1093/idpl/ipz008
45. Wu, Z.D., Li, G.L., Liu, Q., Xu, G.D., & Chen, E.H. (2018). Covering the Sensitive Subjects to Protect Personal Privacy in Personalized Recommendation. *IEEE Transactions on Services Computing*, *11*(3), 493–506. https://doi.org/10.1109/tsc.2016.2575825
46. Zhang, J.P. (2016). International Regulation of Cross-border Data Transfer and the Response of Chinese Law--A Concurrent Review of the Rules on Restriction of Cross-border Data Transfer in China's Cybersecurity Law. *Political Science and Law*, *259*(12), 136–154. https://doi.org/10.15984/j.cnki.1005-9512.2016.12.014
47. Zharova, A.K., & Elin, V.M. (2017). The use of Big Data: A Russian perspective of personal data security. *Computer Law & Security Review*, *33*(4), 482–501. https://doi.org/10.1016/j.clsr.2017.03.025
48. Zhuo, L.X. (2019). Right to Data Portability: Concept, Problems and China's response. *Administrative Law Review*, *118*(6), 129–144.