Industrial Policy Orientation and Mechanism Construction for Data Sharing and Utilization in the Internet of Things (IoT) Era

Xie Shen[1], *Bingying Zhou*[2*]

[1] *College of Marine Culture and Law, Jimei University, China*
[2] *School of Business Administration, Baise University, China*
shenxie@jmu.edu.cn, chow6117@alu.ruc.edu.cn

Abstract

Data sharing has gained significant prominence due to the emerging trends shaped by the Internet of Things (IoT), As a result, the rule of triple authorization as implemented by the judicial system has become popular, i.e. any data shared has to have the necessary approval from user for its collection and authorization from holders and user for its distribution. This rule has seriously affected data flow, impeding the growth of the big data industry. The mechanism of data sharing is in urgent need of improvement. In light of the big data industry's evolving demands, the detrimental impact of the existing frameworks on its development is examined from an industrial growth context. Then, from the perspectives of protecting personal data and sustaining the prevailing commercial interests, the control mechanism and benefit distribution mechanism for data sharing are reconstructed.

The realization of the potential of data and foster the growth and continuous improvement of the data market, there is a need to we must reassess the current model of comprehensive informational autonomy granted to data subjects and transition to an informed consent approach. This shift should include granting users the right to retrieve data in cases of unlawful collection, circulation, and utilization. Meanwhile, we should also make efforts in the following aspects: (i) encouraging active participation of data businesses in data sharing, (ii) improving the equitable distribution of benefits between data holders and users, (iii) clarifying and assigning the interests of data entities, and (iv) in the event of conflicting interests, the data holders' interests will be the priority.

Keywords: IoT technology, Cloud data, Data sharing, Legal mechanisms

1 Introduction

The Internet of Things (IoT) is a revolutionary technology that is shaping the collection and dissemination of data [1]. It utilizes terminal sensors that link to the internet or other data sources or storages, providing a mechanism to transmit data to the cloud or other available terminals [2]. This capability that allows for a free transmission of data creates and information network referred to as IoT [3]. The emergence and development of IoT rely on the interconnected network as the infrastructure, and the data transmitted through the sensors forming the circulatory link [4]. The interconnection of information networks and the sharing of data and information have decisive roles in the development of IoT.

However, contrary to the direction of data factor market circulation, data silos remain the most significant obstacle to the development of the data industry. The reasons for the existence of data silos are multifaceted: firstly, data possess informational value; while their use is not exclusive, the realization of their value is, leading to potential monopolization. Secondly, the data market still lacks effective norms and mechanisms that could ensure market participants gain fair value from data circulation and trust that their data rights will not be compromised, i.e., how to establish effective assurance mechanisms to facilitate efficient data resource circulation. This paper aims to explore these topics through extensive research. Admittedly, market mechanisms should not completely favor one party's interests over another's, but must instead balance interests to construct a market mechanism that equalizes the interests of all parties involved, thereby fostering a win-win situation.

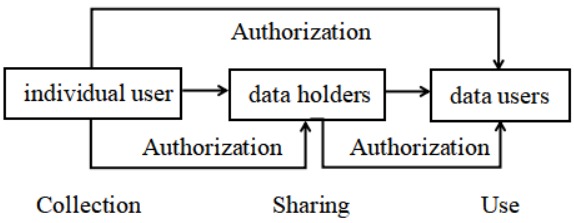

Figure 1. Triple authorization mechanism

Currently, data remain difficult to share and utilize across platforms and regions, significantly hindering the development of the digital economy industry. The root of this problem lies in the unclear rights associated with data resources and the absence of established mechanisms for data sharing and utilization [5]. Particularly, the "triple authorization mechanism" formed by the courts severely impacts data collection and circulation. Triple authorization mechanism is shown in Figure 1. Therefore, breaking down the barriers of data silos and establishing a robust legal

*Corresponding Author: Bingying Zhou; E-mail: chow6117@alu.ruc.edu.cn
DOI: https://doi.org/10.70003/160792642024072504010

mechanism for data resource sharing and utilization are essential for promoting the prosperity of the digital economy.

2 Process and Main Practical Obstacles of Data Resource Circulation

2.1 Participants and Steps in Data Resource Circulation

The process of data circulation and utilization essentially involves the exchange between information and data. This process is characterized by the flow of data in digital format, which is then decoded, interpreted, and applied by data users in the form of information. This process can be generalized as a cycle: Information → Data → Information.

Data circulation is not merely the transmission of embedded information; it is also the process in which the value of data is created and realized. Several parties are involved in data circulation: data subjects, data holders, and data users. Data subjects are the originators of information and represent the starting point of data circulation, as well as the source of data generation. Data is produced by the subjects, typically collected by data industry entities and stored in digital form. Data holders then process, aggregate, and organize this data, which includes anonymization and the cleansing of sensitive information, to make it available for use. At this point, the data may be used by holders themselves or made available to other users, either for a fee or free of charge. This entire sequence of processes constitutes the circulation of data.

Data, as a resource, is fundamentally about the interests associated with information. These informational interests vary among different parties and at different stages. For instance, at the level of the data subject, the interests manifest in three ways: one concerns the personal interest from the perspective of personal information protection, and the other concerns the property value and benefits that can be derived from exchanging information resources in a commercial context. For commercial entities (data companies involved in collection, holding, processing, etc.), the commercial value of information is generated through its circulation. Lastly, from the perspective of industrial and social development, informational interests pertain to the added value generated through the movement and application of information on a larger scale, thereby advancing industrial development. Both the protection of personal information and the commercial and public interests in the development of the data industry are expressions of informational interests across various parties.

2.2 Participants and Steps in Data Resource Circulation

As discussed, data circulates due to its inherent informational value. However, it is this value that can lead to limitations on its circulation or even monopolization. The obstacles to data circulation stem from two main subjects: first, the information rights and interests of the data subjects. Data acts as a carrier of the data subject's information, which could potentially reveal details about the subject. Here, the data referred to can identify personal information, either alone or in combination with other data subjects' data, without anonymization. The current legislative framework for information protection affords substantial safeguards for the personal information of data subjects. The established right to informational self-determination allows subjects to restrict access to their information, prevent or impede its circulation, and even halt the use of data that may impact their informational rights and interests. Second, the control over data stems from data holders. In the information age, possessing information translates to having an advantage. However, as business entities naturally prioritize their own interests, information tends to be monopolized rather than shared. Exclusive control over valuable information or information monopolization can represent significant commercial value for data holders in the face of substantial informational interests.

Upon examining the current legislation, there has been a further emphasis on safeguarding personal information. The Personal Information Protection Law and the Data Security Law, both unveiled in 2021, delineate protective measures for personal information throughout data flows and establish security prerequisites for data transmission. Firstly, the right to self-determination of personal information has rendered data flows involving personal information contingent upon the consent and authorization of the individual concerned. Secondly, small-scale data enterprises face challenges in surviving within the surging tide of the industry, and these measures have significantly influenced data flows, leading to a tendency towards monopolization of data resources. Conversely, the current legal framework for data flows is inadequate, and a national data circulation mechanism has yet to be established. This, in another dimension, leaves data flows in a state of uncertainty, preventing the formation of a normalized data market [6]. China has proposed in the "Twenty Data Articles" to construct a compliant and efficient system for the circulation and trading of data elements that integrates both domestic and international markets, and innovative practices and mechanisms are currently under development in various regions.

The issues mentioned above pose unfavorable conditions for the practical circulation of data. As discussed earlier, data silos are a significant barrier to the development of the data industry. The progress of the digital industry necessitates the movement of data to maximize its information value. While industry development requires data fluidity, the protection of personal information and the constraints of commercial interests are impeding this flow, resulting in a conflict. Hence, the problem has evolved into a conflict between the development of the data industry and the protection of personal information and commercial value.

The essence of the legal relationship in data circulation is the management of the informational interests of various stakeholders. In the sharing and utilization of data resources, the issue primarily concerns the informational interests generated among different stakeholders. From an industry development perspective, these interests are realized through the circulation and utilization of data. From a commercial viewpoint, these interests are manifested as the data holder's interest in the exclusive control and use of information. From the standpoint of personal information protection, these interests are represented as the individual's interest in safeguarding their information. Therefore, resolving the

fundamental issues in data circulation involves managing the conflicts among these informational interests and addressing this balance of interest through legal institutions.

3 Conflicts and Balance of Interest in Data Sharing and Utilization Under Industrial Policy

3.1 Conflicts and Balance of Interest Between Personal Information Protection and Data Industry Development

The development of personal freedom necessitates the upholding of informational self-determination. However, the spread of personal information through data sharing raises concerns. Drawing on the European Union's General Data Protection Regulation (GDPR), the current Personal Information Protection Law ascribes personal information rights to the information agents, serving as a means to protect their right to informational self-determination. In the realm of data, this is specifically characterized by the information agents' absolute control over various stages of data handling, specifically, the implementation of a consent or authorization mechanism by data subjects (information agents) during the processes of data collection, transfer, and utilization. Without obtaining the consent or authorization of data subjects, data cannot be collected, circulated, or utilized [7]. The right to self-determination of personal information has also been implemented and affirmed in practice. The principle of triple authorization was first proposed by the appellate court in "Sina Weibo v. Maimai", i.e. user authorization to platform acquisition of data as the first authorization; user and the platform's authorization to enterprises for the use of that data as the second and third authorization. Based on this principle, when a platform shares the data with subsequent users, it still has to seek the authorization and consent of the platform user. Based on the requirements for personal information protection in different countries, to enhance privacy and prevent the leakage of personal information within the IoT infrastructure, countries are emphasizing the need for the user associated with the personal information to retain control over all processes involved post-data collection.

However, some scholars argue that that it is inadvisable to grant the individuals concerned absolute control of their personal information. There is an emphasis on the maintenance of adequate controls to protect personal information during its collection, sharing, and utilization within the IoT cloud data sharing. The main practice, currently, is to allow users to maintain "right of self-determination to personal information", which includes the regulation of data containing personal information. However such an approach creates a barrier to the free flow and use of data, which affects its value. Predictably, if a user decides not to share their personal information, then it creates a barrier that hinders the growth of the entire industry. Consequently, uncertainties emerge on the growth of the big data industry. Firstly, They highlight that prioritizing personal information protection over the development of the data business and it social value could lead individuals to withhold their information, which may hinder data circulation——this can happen even after information is collected, where they may subsequently disagree with its circulation. However, existing mechanisms for protecting personal information are solely focused on one aspect of protection and are not evaluated in a business context. If a value conflict arises between the need for data circulation for industrial development and personal information protection, current laws do not offer a resolution. Secondly, the public interest in data primarily encompasses the right to data development and its public value, whereas personal information protection is a private right concerning data. The interests reflected in personal data and the public value generated by data circulation are not comparable. As they are not mutually exclusive, both should be preserved [8]. The right to self-determination of personal information can, to some extent, affect the flow and use of data, creating a value conflict with data sharing and utilization. Thirdly, although users are naturally the subjects of the right to self-determination of personal information, they may not be the most suitable agents for this control. Users often lack the professional knowledge required to manage personal data effectively, which can lead to the proliferation of illegal means to acquire or disclose personal information [9]. Fourthly, data sharing and utilization do not necessarily result in the infringement of personal information rights. Promoting the development of the data industry without compromising the private interests inherent in personal information also signifies the advancement of society and individuals, and it can strengthen the protection of personal rights in the information society. Even if data sharing and utilization might lead to the infringement of data subjects' rights or there are risks associated with transmission security, the act of data sharing and utilization is not the root cause of these issues but rather the absence of effective market regulation and governance rules.

This paper argues for a balanced approach to the conflict between personal information protection and data industry development. Specifically, an effective balancing mechanism should be reconstructed to address the existing value conflict, rather than tilting in favor of one side over the other. Firstly, the need to reconstruct the mechanism stems from the fact that current personal information protection mechanisms cannot reconcile the value conflict between information protection and data circulation. A "strong control" model under the right to self-determination mechanism is not the optimal solution. Secondly, institutional design should appropriately reflect and emphasize an effective personal information protection mechanism that supports data circulation, ensuring that the mechanism can protect personal information effectively without unduly impeding data sharing and utilization. Lastly, while value conflicts are unlikely to be eradicated, it is possible to balance the conflicting values of both sides and develop towards a mutually beneficial equilibrium that favors both data circulation and information protection.

3.2 Conflicts and Balance of Interest Between Data Circulation and Data Monopoly in Data Industry Development

In the context of open or publicly accessible data, market

entities are generally entitled to use such data reasonably without needing consent or authorization from the data subjects or holders, provided they adhere to certain market acquisition norms. For instance, the practice of harvesting vast amounts of public data can still potentially be deemed unfair competition. However, the use of non-public or yet-to-be-released data currently requires the consent or authorization of the data holder; unauthorized acquisition and use are forbidden. This commercial practice was upheld in the appellate court's decision in the "Sina Weibo vs. Maimai" case, affirming that data utilization necessitates consent or authorization from data holders.

The justification for insisting on consent or authorization is twofold: firstly, drawing upon John Locke's "labor theory of property", data holders have invested significant labor in the collection, compilation, organization, and processing of data, and thus their proprietary rights over the data should be acknowledged. Secondly, the consent or authorization framework helps to effectively prevent opportunistic behaviors such as free-riding that can disrupt market order [10]. Imagine if data users could access data without consent or authorization from the data holders and compensation, this could disincentivize enterprises from investing in the creation of industries and would likely dampen the enthusiasm of data-driven businesses, leading to a decline in developmental impetus and slowing industry progress.

It is essential to recognize that this mechanism serves a necessary and reasonable purpose for data holders. Data holders are distinct from data subjects, and so is the rationale behind their consent or authorization mechanism. With their specialized knowledge and experience, data holders can effectively control data circulation through this mechanism, thereby securing their data-related profits. Furthermore, the informational interests of data holders diverge from those of data subjects; data holders are more invested in the property benefits they can accrue both when they possess the data and when it is circulated. Therefore, the consent or authorization mechanism can effectively regulate data usage for holders, allowing them to maximize the potential for value creation.

However, it is widely acknowledged that data sharing and utilization hold significant functional value for industrial development and societal economic progress [11]. Sharing and utilizing data resources can unlock the potential of big data and yield positive externalities [12]. Yet, the current state of data circulation remains subdued, and it has not become standardized. This is not due to the existence of a consent or authorization mechanism, but rather because data circulation faces various market-level challenges, such as an underdeveloped circulation environment. Firstly, the current extent of data circulation is insufficient to evolve into a standardized and efficient market. Secondly, the data circulation market lacks effective safeguard mechanisms that ensure data holders can reap necessary profits from data circulation and reduce the uncertainties associated with profiting from such circulation.

Even as we recognize the current market's imperfections, does this mean we must solely concentrate on safeguarding the interests of data holders while the market remains underdeveloped? The answer is not straightforward. The interests of data holders represent the private interests of commercial entities, but the circulation of data benefits the entire industry and its practitioners, offering significant social value. This paper contends that in promoting data sharing and utilization, it is necessary to strike a balance between the social benefits of data circulation and the protection of private interests through industry policy. Here, it is pointed out that, firstly, in view of the social and industrial benefits, we should promote organized data sharing, implement data sharing at the policy level, and even take the corresponding measures to restrict or prohibit data monopoly (unless there are clear reasons, one cannot refuse to give authorization). Secondly, while promoting data sharing, we should protect and respect the interests and rights of data holders and provide the appropriate compensation for labor [13]. In light of the importance of developing the big data business, it is imperative that we promote the shared flow and use of aspects of the data market, creating a shift from an industrial policy that promotes data sharing to one that advocates for free flow of data from controllers to users.

Still, from an industry policy standpoint, achieving data sharing between data controllers and data users requires tackling the pain points in data sharing. To achieve an optimal relationship between the data holders and the users, it is important to address the main issues impeding the data sharing, namely: first, from the perspective of the data controllers, how to achieve the appreciation of data circulation and use while protecting data security and their own interests; for the data users establish mechanisms to ensure that they receive correct, complete, and useful data.

If there is merely a consent or authorization mechanism without subsequent normalized mechanisms for benefit exchange and pricing, the consent or authorization mechanism itself becomes deficient, essentially becoming a mechanism of refusal. Merely holding data implies no revenue, but also no risk. Furthermore, effective mechanisms for data circulation should be established to explore data circulation practices and promote an optimized circulation environment, thereby providing the market with more opportunities and space for circulation. A more relaxed circulation environment will encourage data holders to allow their data to circulate freely.

4 Control Mechanism for Personal Information within the Context of Data Sharing and Utilization

4.1 Transforming the Control Mechanism for Personal Information Related to Data

This study advocates for a change in the mode of exercising the right to self-determination of personal information by data subjects, shifting from a model of "prior consent" to one of "control during and after the event". When data begins to circulate, it should not be necessary to obtain the prior consent or authorization of the data subject. However, data holders and users must, in accordance with personal information protection requirements, do their utmost to safeguard the data subject's informational interests and information security.

To strike an effective balance between the protection of personal information and the informational benefits of data circulation, it is crucial to construct a reasonable mechanism that balances these interests correctly. Such control should be established through regulation during and after data processing, rather than before. In the context of industrial policy, it is crucial not to overlook the private interests associated with personal data. Social development hinges on maintaining social welfare and promoting individual advancement. Merely discontinuing data sharing due to potential infringements on data subjects' rights or security risks is not a comprehensive solution. The main issue is on managing the legal relationships in data sharing. Instead of "throwing away the apple because of its core", a balanced approach to data sharing, considering both personal information protection and industry development, is advocated [14]. While personal information requires reasonable protection during data sharing, absolute control by individuals may impede industry growth. Hence, establishing mechanisms to prevent the misuse of personal information is imperative, given its inherent value.

Lessening the right to informational self-determination does not negate the mechanism for protecting personal information. The difference is the shift from the triple authorization mechanism to an informed approach. It is believed here that with respect to personal information protection, a passive restraint mechanism should be adopted in legislation instead of an active one, that is, the acquisition and distribution of personal information should only require fundamentally the individual user to be informed, but not his/her consent or authorization for the personal information. In addition, in cases of collection and circulation of personal data, the costs of consent or authorization and monitoring are usually high [15]. If there is no illegal utilization of private information, in principle, we shouldn't further restrict data collection or circulation. Similarly, there should be an exemption if the data sharing is for public purposes and there is no abuse of the data.

A key question to consider is what are the appropriate grounds to reduce the absolute control to personal information held by subjects? This paper finds two: one is when personal data is used to improve public welfare. For example, the epidemiologic investigation of individual whereabouts in epidemic prevention and control will involve personal GPS information; annual statistical data may involve the annual income of individuals. The use of such data, whether alone or collective, will have a certain impact on personal information. But considering the purpose of the use of such data, the weight of the informational right of self-determination should be reduced to a certain extent. The other is that to foster the growth of the big data industry, it's imperative to establish a rational data circulation mechanism that, to some extent, exempts from the strict requirement of the triple authorization principle. Encouraging the development of an efficient and regulated data market would facilitate the free flow of valuable data, aligning with the demands of the big data sector [16]. In the meantime, we must stick to the securing personal information, as this is the premise for the adjustment of the mechanism. In other words, the initial default position should change from obtaining the data subject's "specific consent" to an assumption of the data subject's consent or default agreement. Here, the following standards and principles are proposed: first, protect personal information from being used illegally during data circulation; second, follow the principle of "acquire for use", prohibit the use of illegal use of data to generate a profit; third, the subjects of data may initiate the "personal information carrying right" on top of the acts of abuse in data circulation and retrieve the data if a need arises; fourth, adopt corresponding measures for data security protection.

4.2 Return to Data Subjects' Right to Self-determination of Personal Information

Data subjects may not have given prior consent or authorization for the circulation of their data or the manner in which it circulates. Nonetheless, they retain the right to be informed about this circulation and should be able to fully understand the entire process of data utilization. When data holders or users circulate or utilize data in an unlawful or non-compliant manner, data subjects can exercise their right to self-determination of personal information to control the use of their data resources during and after the fact. They can intervene in the illegal or non-compliant circulation and use of data, canceling the qualifications of the data holder or user to circulate or use the data, thus protecting their informational interests [17]. Data users should confront against data subjects' improper interference with subsequent distribution and use of data considering the needs of industrial development. For example, a data user's use of data with the approval of the holder of the data can exclude irregular use of the data use from third parties like the owner of the data and its controller. The behavior of users of data should be only for the purpose of use, and it should not be deemed as similar to the control held by the data handler at the level of distribution. Relying on their control, data stakeholders confront the control of the other parties. But data subjects should not have chain-wide control over the use of the data, they can only exercise their right if there is evidence of abuse of the information. The control mechanism at the data sharing is shown in Figure 2.

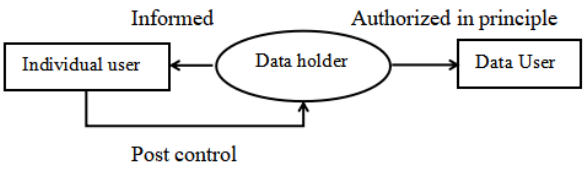

Figure 2. The control mechanism at the data sharing

5 Benefit Distribution Mechanism in Data Sharing and Utilization

5.1 Benefit Confirmation Mechanism during the Circulation and Utilization of Data

It is essential to acknowledge the interests involved in the distribution and use of data. At the outset, it is important to

note that data, in its raw form, does not inherently generate profits therefore, data subjects, namely the users themselves, claim a share of the profits derived directly from the data. From a rights perspective, individuals are the rightful owners of data rights, albeit restricted to personal rights and interests and not business rights. An individual cannot purport to sell their personal information since such a benefit only manifests in users that find a business value of the data. However, protecting personal rights and interests from infringement is crucial when utilizing personal information for commercial purposes. Personal information cannot generate benefits on the individuals' side; it only produces possible property interests by circulating. Such rights and interests are actually benefits generated by the use of data, preventing individuals from financially capitalizing on personal data. Additionally, the generation of property rights stems from the value generated by the data holder incurring labor costs; users, however, provide their information for IoT to enhance the experience of life services, for which it cannot be a source of such value. Secondly, data can bring profit at the level of utilization. As postulated in Locke's labor theory of property, the profit from data should reflect the costs incurred for innovation and data refining. For data holders, there are two primary ways they can use the data in their possession to generate property rights: by packaging the data for sale to other businesses; or by analyzing and processing the data to generate value. From the perspective of balancing optimal use of data assets with securing personal information, data sharing should be limited in terms of utilization and profitability. It is proposed here that there should be a limitation to the sharing of data based on domain, that is, the collected data can only be used for IoT services; second, limited ways of making a profit, the data can only be shared, not sold in packages to transfer the right of use; after sharing, the sharer remains the controller and should be obliged to control and secure the data. Therefore, the property rights and interest in data stem by the data controller stem from value they add to it and not the data in its raw form. Data users usually can only use the data authorized for use, only as allowed during authorization and the consideration paid for its acquisition. Moreover, it is prohibited to transfer IoT data for profit.

5.2 Pricing Mechanisms in Data Circulation

The determination of appropriate prices for data to avoid data holders' seeking illegal or unjust profit, which negative affects the growth of the big data industry, the possible gains to the data holders from data sharing should be limited to a specific degree. The current foundations of data value include the information contained within the data (potential profits it may yield), its processing value (such as screening and aggregation methods), and the intrinsic value inherent in the user. The proposition here is that data pricing should primarily consider its processing value, instead of the assumed additional value to the user or the implied value of the data.

5.3 Mechanisms for Resolving Conflicts of Interest in Data Usage

Conflicting interests in data utilization, i.e. the distribution and use of data may witness conflicts of interests between different subjects. The competing interests of data controllers are affected by data sharing, which might affect the financial benefits for the controllers from the use of the data. A possible situation is where the controller and the user similar enterprise, creating a competitive business position. In that regard, the industrial policy should incorporate a mechanism for evaluating the competing interests between the data holder and the data user. Benefit distribution mechanism for data sharing is shown in Figure 3.

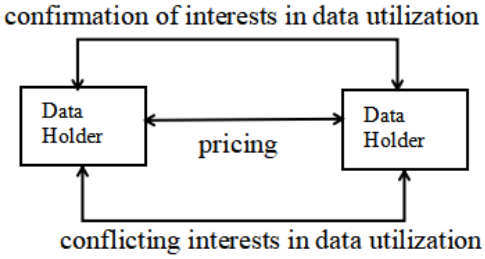

Figure 3. Benefit distribution mechanism for data sharing

Generally speaking, if a monopoly is formed in data collection, normally, there cannot be a refusal of the sharing of data. If there is not a monopoly, data users may find data sources by themselves or through other channels if they can. However, if there is no proof that the utilization of the data will affect the competitive advantage of the data controller, then they should share it with the data user. The data controller should only be able to withhold sharing if they prove that: (i) there is the likelihood of illegal data uses or an infringement on public welfare; (ii) the use of the data might be against the interests of both parties; (iii) there is grounds for competitive interests between the parties; (iv) the data user might share the data with unauthorized persons; (v) there might be the above circumstances in affiliates of the data user, etc.

6 Conclusion

The two principal barriers to data circulation, whether stemming from human nature or commercial logic, inherently arise within the business process. As the Internet of Things continues to gain significant popularity, it creates a demand for data sharing. However, the sharing mechanisms require urgent improvement to unlock the potential of the big data industry. The impediment to data circulation is rooted in the mechanisms, particularly the current issues with data control rights systems. Existing personal information protection mechanisms or commercial logic endow data subjects and controllers with control over data and its circulation. Our circulation mechanism aims to resolve these control rights and balance them. An urgent change is to shift from the right to informational self-determination for data principals and transform the mechanism of consent and authorization to an approach of informed consent with the right to retrieve the consent if there is evidence of illegal gathering of the data, distribution, or use. At the same time, we should fully

mobilize businesses in the data industry to participate in data sharing, further improve the mechanism of benefit distribution among data holders and data users, pay attention to the confirmation and distribution of the interests of data business entities, and prioritize the protection of the interests of key stakeholders like data controllers in the event of a conflict of interest.

Acknowledgements

This work was supported by Xiamen Social Science Research Project (No. 2024C22) and Fujian Province Science and Technology Innovation Strategic Research Project (No. 2022R0053).

References

[1] D. J. Deng, R. S. Chang, A Priority Scheme for IEEE 802. 11 DCF Access Method, *IEICE Transactions on Communications*, Vol. E82-B, No. 1, pp. 96-102, January, 1999.

[2] D. J. Deng, C. H. Ke, H. H. Chen, Y. M. Huang, Contention window optimization for IEEE 802.11 DCF access control, *IEEE Transactions on Wireless Communications*, Vol. 7, No. 12, pp. 5129-5135, December, 2008.

[3] D. J. Deng, K. C. Chen, R. S. Cheng, IEEE 802.11ax: Next generation wireless local area networks, *10th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness* (OSHINE), Rhodes, Greece, 2014, pp. 77-82.

[4] D. J. Deng, Y. P. Lin, X. Yang, J. Zhu, Y. B. Li, J. Luo, K. C. Chen, IEEE 802.11ax: Highly Efficient WLANs for Intelligent Information Infrastructure, *IEEE Communications Magazine*, Vol. 55, No. 12, pp. 52-59, December, 2017.

[5] W. Kerber, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, *Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil (GRUR Int)*, No. 11, pp. 989-998, November, 2016.

[6] J. Drexl, Designing Competitive Markets for Industrial Data- Between Propertisation and Access, *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 8, No. 4, pp. 257-292, January, 2017.

[7] E. Fialova, Data Portability and Informational Self-Determination, *Masaryk University Journal of Law and Technology*, Vol. 8, No. 1, pp. 45-55, June, 2014.

[8] B. Engels, Data Portability among Online Platforms, *Internet Policy Review*, Vol. 5, No. 2, pp. 1-17, June, 2016.

[9] P. Samuelson, Privacy as Intellectual Property, *Stanford Law Review*, Vol. 52, No. 5, pp. 1125-1169, May, 2000.

[10] G. Hardin, The Tragedy of the Commons, *Science*, Vol. 62, No. 3859, pp. 1243-1248, December, 1968.

[11] K. Pistor, Rule by Data: The End of Markets?, *Law & Contemporary Problems*, Vol. 83, No. 2, pp. 101-124, July, 2020.

[12] C. M. Rose, Surprising Commons, *Brigham Young University Law Review*, Vol. 2014, No. 6, pp. 1257-1282, December, 2014.

[13] P. D. Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, I. Sánchez, The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services, *Computer Law & Security Review*, Vol. 34, No. 2, pp. 193-203, April, 2018.

[14] P. K. Yu, Data Producer's Right and the Protection of Machine-Generated Data, *Tulane Law Review*, Vol. 93, pp. 859-929, October, 2019.

[15] D. J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, *Harvard Law Review*, Vol. 126, No. 7, pp. 1880-1903, May, 2013.

[16] O. Lynskey, Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability, *European Law Review*, Vol. 42, No. 6, pp. 793-814, December, 2017.

[17] N. Isaacs, Book Reviews: Fundamental Legal Conceptions as Applied in Judicial Reasoning and Other Legal Essays by Wesley Newcomb Hohfeld, Walter Wheeler Cook, *Harvard Law Review*, Vol. 36, No. 8, pp. 1038-1042, June, 1923.

Biographies

Xie Shen is a lecturer at the College of Marine Culture and Law, Jimei University. He earned his Ph.D at the Law School of Tsinghua University of China. His areas of research include data and artificial intelligence law, civil and commercial law and sports law.

Bingying Zhou is an associate professor of Baise University. He earned his Ph.D. at the Law School of Renmin University of China. His areas of research include competition law, regulating digital platforms, intellectual property rights, and commercial law.