



# Balance Between Data Circulation and Personal Information Protection

## Based on the Analysis of the Development of the Digital Industry in the Internet of Things Era

Shen Xie<sup>1</sup> and Cheng Chen<sup>2</sup>(✉)

<sup>1</sup> Department of Law, Jimei University, Xiamen, China

<sup>2</sup> Xiamen Institute of Technology, Xiamen, China

chengchen\_cy@yeah.net

**Abstract.** In the era of the Internet of Things, data sharing has formed a trend. Judicial practice has clarified the “triple authorization rules”, that is, data sharing and sharing requires users to obtain the authorization of data collection and the authorization of users and data holders for data circulation and utilization, which seriously affects the data circulation. Starting from the needs of the development of the big data industry, to reflect on the hindering impact of the current authorization mechanism on the big data industry, the data control mechanism of data sharing should be rebuilt. In order to fully tap the potential of data and further promote the development and improvement of the data factor market, the existing data subject should change the complete right of self-determination of data, change the consent authorization mechanism into the informed mechanism, supplemented by the user’s right of data retrieval under the circumstances of illegal collection, circulation and utilization.

**Keywords:** Internet of Things technology · Internet of Things · Cloud data sharing

## 1 Introduction

The Internet of Things technology is a new technology for connecting various sensors and the existing Internet. It uses various terminal sensors to collect user information, and transmit the information to the cloud or other information terminals in the way of data. Using smooth network transmission, the world can form an interconnected information network, namely the Internet of Things. The development of the whole Internet of Things. The Internet of Things technology is booming, the interconnected network is the infrastructure, and the “data and information” collected, transmitted and shared by sensors is the “blood” of the boom of the Internet of Things technology. The interconnection of information network and the sharing of data and information play a very important role in the development of the Internet of Things technology.

IoT cloud data refers to the production data that can identify user information when identified and collected by terminal devices that use the Internet of Things technology

and collected in the form of data. IOT cloud data is formed by collecting user information by the terminal equipment on the user end, and then the Internet of Things information network transmits the user data back to the information processing center, and screened, analyzed, processed and sorted out the data. Finally, the processed data is stored in the cloud for subsequent utilization. The whole Internet of Things cloud data, from collection to storage, and then to utilization, involves the data subject (i. e., user), data holder (i. e., Internet of Things technology provider or operator) and data user respectively. The data can be used for self-use, shared to other subjects, or sold to other subjects.

Based on the protection of personal information in the data circulation, Three mechanisms have been established: whether the data is anonymized, Deplete personal information from individuals, No personal identifiability; Second, if the data can not be completely anonymized, Then the data involving personal information shall be agreed to and authorized by the individual corresponding to the information; Third, in the use process, If there is an abuse of data containing personal information, Individuals have the right to exercise the “right to carry personal data”, The EU General Data Protection Regulation is based on the data subject’s right of self-determination of their personal data, It clearly stipulates the “right to carry personal data”, That is, the data subject has the right to obtain the personal data provided to the data controller in a structured, common, and machine-readable format, Or have the right to freely transmit such data from the data controller that it provides to another data controller.

Iot cloud data sharing involves personal information protection, which lies in the collection, sharing and utilization. Currently, it is common practice to grant users “self-determination on personal information”, including users taking control over data containing personal information. In the case of “Sina Weibo v. Mai Mai”, the court of second instance in the case initiated the “triple authorization principle”, that is, the first authorization for users to obtain data from the platform; the second and third authorization for the user and the platform to use the subsequent data acquisition. Based on the “triple authorization principle”, the platform still needs to obtain explicit authorization or consent from users when sharing data with subsequent users. Based on the requirements of various countries for the protection of personal information, to avoid and prevent the leakage of personal information and privacy directed by the Internet of Things cloud data, various countries tend to leave the whole operation process after data collection to the users corresponding to the personal information for control.

This leads to a value conflict between user data control and the free circulation of data. It is conceivable that if users do not agree to share the data, the data flow will be limited, and the development potential of the entire industry should also be affected. In other words, the development of the entire big data industry will be presented with various uncertainties. Then, from the perspective of industrial policy, how to further weigh the value conflict between personal information protection and the development of big data industry, so that the two can obtain the optimal solution in the value combination, is the problem to be discussed and solved in this paper. It can be seen that although the sharing and sharing of IOT cloud data is a simple process of data transmission and utilization, the subject relationship involved is relatively complex and involves the construction of many mechanisms.

## 2 Conflict and Balance of the Interests of All Parties in the Data Sharing and Sharing Under the Industrial Policy

Information self-determination is seen as an important sign of the free development of personality. The sharing of data may cause the dissemination and diffusion of personal information. The data control right belongs to the subject of digital rights is a means to protect the right of information self-determination of the data subject. In the specific mechanism, it is the consent or authorization mechanism of data collection and use.

However, more and more scholars believe that it is undesirable to give information subjects absolute control over personal information. First, from the perspective of personal information protection, without considering the development of data industry and data public value, the private interest of data is not comparable to the public value, and the right to self-determination of personal information will more or less affect the circulation and utilization of data, and produce value conflicts. Second, users are not the appropriate subject of the decision power of personal information. Users have no industrial foundation, and can only control the data through consent or authorization, which will also lead to more illegal means to illegally obtain or disclose personal information.

From the value orientation of data sharing and sharing, data development and personal information protection should not be ignored. The public interest of data mainly includes the data development right and the public value, while the protection of personal information is the private interest right of data. This paper holds that the conflict between the two should be balanced, rather than biased on one side, especially in the case that industrial policy does not affect personal information and private interests, starting from social development, maintaining social welfare means human development. Second, the possible infringement of the rights and interests of data subjects or the existence of transmission security risk caused by data sharing means that the cancellation of sharing sharing, is not the way to solve the problem. Data sharing is not the root cause of the problem. The root cause of the problem lies in the legal relationship of multiple parties in sharing. We should not give up eating for fear of choking. We should explore and find a suitable path for development and sharing, and find a balance limit and a reasonable scale between sharing and sharing. The author believes that in the process of data sharing and sharing, the personal information contained in the data should be reasonably protected, and the data sharing should be carried out on the basis of personal information protection. However, based on the development of the data industry, it is also necessary to reduce the personal absolute control of the information to some extent. Since it is inevitable that personal information will be used and gain value in the industry, what we should solve instead is how to build a reasonable mechanism to avoid abuse for the use of personal information.

What is the reasonable premise for the reduction of the information self-determination of the data subject? This article thinks there are two: one is the data containing personal information will be used for public purposes, such as epidemic prevention and control of personal whereabouts flow, will involve personal positioning information, such as annual statistics in the annual data may involve personal income, etc., these use alone or collection, more or less will cause certain impact on personal information, but based on public purposes, should be given to a certain extent. Second, based on the development needs of the big data industry, a reasonable data circulation

mechanism is established to exempt the authorization and consent procedures of the data subjects to a certain extent. Advocate the whole society to form an efficient and orderly data circulation factor market, promote the free circulation of valuable data, and meet the needs of the development of big data industry. However, the data protection related to personal information should still be adhered to. This paper believes that there should be several standards and principles: first, the protection of personal data in the process of data circulation; second, based on the use of data resale and illegal profits; third, the data subject can exercise the “right to carry personal information” to retrieve the data at any time based on the abuse in the data circulation. Fourth, take the corresponding data security protection measures.

### **3 Control and Utilization Mechanism of Data Circulation Under the Background of Data Sharing**

#### **3.1 Conform from Prior Consent Mechanism into “PRior Knowledge + post Control” Mechanism**

Based on the consideration of industrial base and effect, data control party and utilization party are the backbone of promoting data circulation control. From the point of view of the data subject, holder and utilization subject, because the data information is generated by the Internet of Things service provider, the data control subject of the data information is more professional than the user private, so the control of the data information should belong to the data holder; this essentially forms the right of self-determination of the data subject information.

First, the reduction of the right to self-determination of data subjects does not mean denying the personal information protection mechanism, but this protection should be changed from the original consent authorization mechanism to the informed mechanism. This paper holds that for the protection of personal information, passive restriction mechanism rather than active restriction mechanism, that is, for the collection and circulation of personal data, in principle, only the user knows without full consent or authorization of personal information; moreover, the cost of collection and circulation, consent or authorization and monitoring of personal data is high. In principle, as long as there is no illegal operation and abuse of personal information, the restrictions on the collection and circulation of data should not be increased. At the same time, the collection and circulation for public purposes can exempt users from personal knowledge, as long as there is no abuse of information.

Second, emphasizing the data holder’s control over the data information does not mean that the subject enjoys complete control over the data information. Data subjects still have the requirement to protect personal information. The control interest of the data control subject means that the control subject can occupy and use the data information, and also undertakes the security obligation of the data control and transmission and the protection obligation of the data information. At the same time, the digital power subject, the user, can exercise the right to retrieve the data information, or the illegal utilization of the data control subject, or the purpose of personal protection of the data information. The data retrieval right of the trigger data subject only comes from the protection of personal information data (Table 1).

**Table 1.** Premise of personal information protection for table data sharing

User informed	Identification mechanism of user information	Whether public use	Data circulation
yes	yes	yes	can
deny	yes	yes	
deny	deny	yes	
deny	deny	deny	cannot
yes	deny	yes	can
deny	yes	deny	cannot
yes	yes	deny	can
yes	deny	deny	can

### 3.2 Control Mechanism at the Common Level of Data Sharing

Data sharing and sharing under the condition of personal information protection is essentially a dispute over the control rights and interests of data, that is, the control right of the data subject, the data controller and the data user over the data. The control mechanism of data generation and utilization is formed, which includes three parts: authorization mechanism (data flow direction, dynamic), utilization mechanism (data possession and use, static) and confrontation mechanism. Among them, the authorization mechanism is the data control mechanism between different subject (this is the generation of data control), using the mechanism is the subject of data utilization of independent decision-making mechanism (the exercise of data control), confrontation mechanism is a main body based on some reason against the data control of another subject (data control to eliminate or pause).

First, data control does not absolutely belong to a certain subject, which is the characteristic of data different from traditional objects, its control rights can be shared, and the actual control of data does not mean the control of equity level.

Second, data control for the different entities. First, the control right of the data subject includes: a) the data generation level, that is, to independently decide whether to form the data; b) the data subject shall be informed of the collection of the data; or requires that the collected data will not affect the subsequent utilization of the data. At the same time, based on the smooth and efficiency of commercial data utilization, this knowledge should usually be a package, rather than such case or personalized processing. Second, the control right of the data holder includes: a) the decision at the data circulation level, that is, the data holder can decide whether to share the data; b) the data utilization level, that is, the data holder has the right to decide whether and how the data is used, including the right of the authorized data user to use the data, of course, the utilization level should comply with the laws and regulations and the authorized content of the data subject. Third, the control of the data user, that is the decision power at the data utilization level. After obtaining the shared data, the data user can decide to use the data independently according to the authorized content. However, the data user cannot exercise the decision

power on the data circulation, that is, when the data user can only use the data and use the data within the authorization of the data holder.

Third, the data utilization level, such as the confrontation subject's control over data. Control is not completely free, or based on authorized restrictions, or based on public interest industrial policy restrictions, produce a confrontation mechanism. In essence, the confrontation right is generated by the control right. Under the premise that the control right is multi-oriented, the right of confrontation should also be multi-oriented and can be exercised by different subjects. First, the control right of the data holder is not completely unrestricted. At the level of decision power at the utilization level, the data subject returns the control when it makes illegal use. At the data utilization level, the data is also based on the balance of interests between the data subject, data holder and data user. The data subjects oppose the control rights of other subjects based on their control rights. Although the data subject should not control the use of the data in the whole chain, the data subject can only control the illegal use of the data, that is, it can exercise the right to retrieve or be forgotten when the data is illegally used. Second, based on the needs of industrial development, the improper interference of the data subject in the subsequent circulation and utilization is opposed. If the data user uses the data under the authorization of the data holder, the improper interference of the data subject and the data holder can be excluded. The behavior of the data user is limited to the utilization purpose, and cannot be similar to the data holder enjoying the control of the data circulation level.

## 4 Conclusion

In the era of the Internet of Things, data sharing has become a balance of power. Based on the needs of the development of the big data industry, the data sharing and sharing mechanism needs to be improved urgently. In order to fully tap the potential of data and further promote the development and improvement of the data factor market, the existing data subject should change the complete right of self-determination of data, change the consent authorization mechanism into the informed mechanism, supplemented by the user's right of data retrieval under the circumstances of illegal collection, circulation and utilization.