Proceedings of the 5th International Conference on Computing and Data Science
DOI: 10.54254/2755-2721/15/20230804

Balance of rights in the protection of users' data interests in the era of big data

Chuanxiang Cong

Computer Science, dalhousie university, Nova Scotia, Halifax, Canada, B3H4R2

ch898183@dal.ca

Abstract. The protection of user data interests is of utmost significance in this day and age, when everyone's private life details and possessions are being digitised and stored in the cloud. Data now rules the world. This paper reviews the relevant literature in order to study the balance of rights in the protection of user data interests in the era of big data. It then suggests various countermeasures for the problem that it identifies. According to the findings of this study, the key factors contributing to the imbalance in the protection of user data rights are the progression of science and technology, the increase in the value of user data, and a lack of awareness regarding the protection of user personal data rights.

Keywords: data interest, big data, personal property, internet users.

1. Introduction

In the era of big data, with the continuous evolution of mobile terminal equipment technology and the development of mobile Internet applications, smart mobile terminals, such as smartphones and tablet computers, are gaining in popularity, and the number of Internet users worldwide continues to rise. Figure 1 displays that the number of Internet users in the globe increased by 4% between January 2021 and January 2022, reaching 4.95 billion.

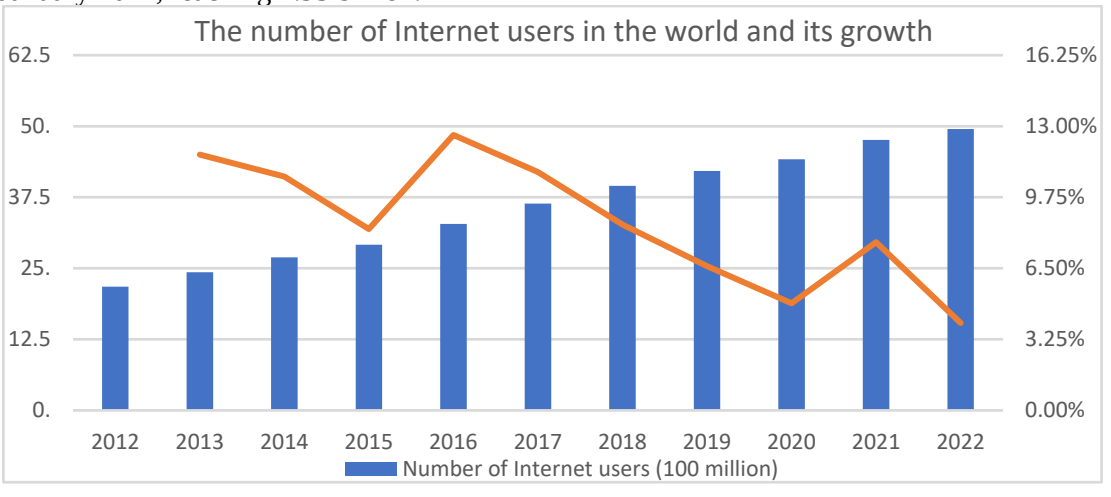

Figure 1. The number of internet users in the world and its growth [1].

DOI: 10.54254/2755-2721/15/20230804

A large number of users indicates that, in the era of big data, there are numerous types and quantities of user data. Moreover, the quantity of data left by Internet users is enormous. It is not difficult to conclude that, in the era of big data that we currently inhabit, the total quantity of user data has reached an astounding level.

Everyday network use necessitates the authorization of personal data. This can be reflected in a variety of privacy clauses in the application and a variety of login agreements. Personal information is utilised in virtually every aspect of daily existence. Through a review of relevant research, this paper examines the balance of rights in the preservation of user data interests in the era of big data and proposes a number of countermeasures. The paper intends to offer some helpful suggestions for this research field.

2. Performance of the imbalance of user data rights protection in the era of big data

The disparity in user data protection manifests itself in three ways: -It is the disclosure of fundamental personal information about the user. It refers to the personal name, age, and other demographic information involved in the dissemination of information, as well as the account information registered and utilised on the Internet. The second is the disclosure of personal behaviour data pertaining to users. In the process of information use and dissemination, real-time data such as users' clicking, forwarding, browsing, and sharing, as well as clothing, food, housing, and transportation, are at risk of being recorded, collected, used, and stored; these data reflect personal network communication behavior, information browsing behavior, entertainment consumption behavior, and other real behaviours. The third risk is the disclosure of an individual's predicted preferences. Using big data technology, personal preference information is summarised and predicted through the use of relational data, fuzzy calculation, and other methods in order to achieve the objectives of precise marketing, immediate analysis, and intelligent decision-making [2].

3. Reasons for the imbalance of user data rights protection in the era of big data

3.1. The value of user data has been continuously improved

In the current era of big data, any user data may become valuable and provide people with benefits. However, when criminals steal user data through improper means and misuse it, it will cause irreparable damage to the body and mind of the individual, as well as threaten the security of personal property and even the stability of the entire society. With the development of online media, the use value and exchange value of user information data have significantly increased in the era of big data, while the disclosure of user privacy information has become more lucrative [3].

3.2. Rapid development of technology in the era of big data

Rapid advancements in information technology have unquestionably made people's lives more convenient. The increasing sophistication of information technology has always been a double-edged sword for the general public. If the user's mind is impure, information technology will become a Damocles' sword dangling from the ceiling. Increasingly sophisticated network programmes and covert systems make it easier to capture user data in the background. Under big data, the background cloud storage is also practical for querying user behaviour data. Moreover, as a result of the above-mentioned extensively utilised characteristics of user data, user data has become more transparent and the protection of personal privacy data has become increasingly difficult.

3.3. Weak awareness of data rights among users

In the Internet age, the protection of others' privacy is exceedingly rare, and the awareness of network congestion's impact on the protection of personal privacy data is still quite low, so people cannot pay sufficient attention to privacy violations in everyday life. First, individuals do not know how to safeguard their own and others' privacy. Some individuals believe that privacy violations are common and have not been punished, so they invade the privacy of others. In addition, the public is unaware of how to safeguard their privacy from intrusion. When individuals' privacy is violated, they do not know

DOI: 10.54254/2755-2721/15/20230804

how to halt it. They cannot ensure that their privacy will not be violated through formal legal channels, which contributes to the frequent and intractable theft of the public's personal information. People's lack of awareness regarding personal privacy protection not only contributes to the development of China's legal system, but also encourages the recurrence of violations, making it impossible to guarantee their safety.

3.4. The lag of privacy protection regulations leads to inadequate supervision

In the context of big data technology, the absence of privacy protection regulations makes data utilisation supervision fraught with hidden dangers, resulting in a privacy conundrum. Existing laws and regulations regarding network privacy protection are merely formalities, are overly general, and lack practical application. The majority of them protect only personally identifiable information, and their protection scope is limited. The original privacy protection principles, including "precise purpose, prior consent, use restrictions, etc., are challenging to implement in the context of big data technology. The legal system for the preservation and use of online personal data is imperfect, resulting in a lack of robust countermeasures for data use oversight [4].

4. Countermeasures to ensure the balance of rights in the protection of user data interests in the era of big data

4.1. Constructing relevant laws to ensure users' data interests

It is of the utmost importance to strengthen the legislation governing the preservation of personal information. Within the framework of extant laws and regulations, the first objective is to strengthen criminal law provisions. Expand the scope of the crime in question. Except for the personnel of state organs or relevant divisions, it is proposed that ordinary individuals with criminal responsibility be included, so that the subject of the crime is the general subject. As long as the crime continues to be committed, all severe offences will be punished. Clear the judgement of serious circumstances, serious circumstances will only exist when the act of unlawfully providing or obtaining other people's information is sufficient to pose a serious threat or cause serious losses to the personal personality rights and property rights of citizens. To assess the severity, it is necessary to consider four factors: the quantity of information, the significance of information, the influence of information, and the timing of behaviour [5]. The second objective is to enhance the tort liability law. It is proposed to change the rules of proof so that the infringer must prove that he is not at fault, and if he cannot do so, he is presumed to be at fault, thereby reducing the burden of evidence for the infringed. Providing punitive damages; If the infringer sells or illegally provides personal information to others, or steals or purchases, collects, stores, processes or uses personal information illegally, it is difficult to determine the infringer's loss, and if the infringer gains from it, compensation shall be made at twice the profit; thereby expanding the infringer's compensation range. Third, the Personal Information Protection Act should be promulgated as soon as feasible. Numerous departments involved in the protection of personal information should actively promote legislation or establish special institutions to promote legislation, introduce a special and unified law on the protection of personal information as soon as possible, standardise and coordinate the implementation of other relevant laws and regulations, and establish a comprehensive protection system for personal information security.

4.2. Constructing a powerful multi-subject supervision system

In the current era of big data, all subjects should do their part to safeguard the security of users' data rights and interests.

First, the government should do a good job with the design of the user data system repository, establish and develop a prevention and control mechanism for user data privacy that is compatible with the current era of big data, and play its leadership role to the fullest. Both central and local government agencies should increase their oversight of privacy protection in order to prevent the disclosure of personal information. The government should establish a mechanism for online notification and

DOI: 10.54254/2755-2721/15/20230804

feedback regarding abrupt privacy incidents. According to the division of responsibilities, government departments must respond swiftly to sudden, significant privacy breaches or leaks and implement efficient coordination and emergency response mechanisms across departments, regions, and systems [6]. Multiple departments collaborate to address the privacy disputes of citizens caused by unethical businesses or institutions, to closely monitor the progress of significant issues, to continuously report the staged progress of investigations, and to promptly address a variety of privacy concerns. Expose the punishment results to companies or institutions with inadequate privacy protection, and effectively improve the service quality and work efficacy of online politics.

As a second step, it is important to promote the development of a multi-agent coordination and linkage mechanism for privacy protection. Multiple stakeholders, including the government, data corporations, and the general public, are involved in protecting individual privacy in the context of big data technology. Consequently, the government should direct multiple stakeholders to participate in the development of a collaborative governance linkage mechanism for privacy protection. Government departments should establish a linkage mechanism for privacy protection with data companies and other relevant institutions, share information, accept responsibility, collaborate, and coordinate services. At the same time, individuals are encouraged to actively contribute to the development of an interactive privacy protection mechanism. The operation of an effective multi-agent linkage mechanism will aid in the formation of a joint privacy protection force and reduce the likelihood of public privacy disclosure. Moreover, it is significant to construct a public privacy disclosure complaint platform and enhance the network complaint, reporting, and monitoring platform construction and privacy problem resolution service mechanism. Government departments should incorporate citizens' privacy protection into the government network supervision system, combine the specific requirements and application characteristics of privacy protection, and construct a public complaint reporting platform for privacy leakage in collaboration with businesses. Improve the privacy protection expression mechanism by utilising a stable and dependable platform for reporting complaints. The government should take the initiative to solve problems for the people, implement strict information supervision and a reward-and-punishment system for related industries that have customers' personal information, and end the bad behaviour of related industries or companies that disclose public privacy [7].

4.3. Strengthening the protection of users' data rights by technical means

In the age of big data, flexible technical means are an essential supplement to government oversight. The advancement of science and technology can also bolster the protection of user data rights to some extent. First, institutions need to increase capital investments in science and technology. Countries and businesses must increase capital investment in research and development of essential technologies for big data security, increase the proportion of capital investment allocated to research and development, or establish dedicated research funds. Encourage the research and development and innovation of personal information security technology, ensure information security at the technical level, enhance the quality of China's big data security technology products, and seize the opportunity to develop security technologies based on big data. The second goal is to enhance technical means. In the era of big data, a significant amount of individuals' personal information is stored and transmitted over computer networks. Technical means are the most effective method to close both human and technological loopholes [7]. It is necessary to strengthen the research, development, application, and promotion of new products and technologies, to continuously improve the performance of information system security equipment such as the firewall, intrusion detection system, anti-virus system, and authentication system, and to adopt technical means such as access filtering, dynamic password protection, login IP restriction, and network attack tracking method to enhance the access and audit functions of applications. The third step is to bolster technical specifications. Encrypt and safeguard the sensitive and vital data, and restrict access and viewing to only those who have been granted identity authorization or who have decrypted the data. Simultaneously, the system of multi-person management of important and key information is stipulated, and the authority of personal information holders is restricted, so that a single person cannot

DOI: 10.54254/2755-2721/15/20230804

master all information and relevant personnel at each level can only master the corresponding limited information.

5. Conclusion

To balance the rights in the protection of user data interests in the era of big data, it is necessary to understand the characteristics of user data, which are numerous and widely used, leading to an imbalance in the protection of user data rights and interests, which are embodied in the basic data of users, personal behaviours of users, and user preferences. Through research, this paper concludes that the primary causes of the imbalance in the protection of user data rights are the advancement of science and technology, the increase in the value of user data, and the lack of awareness regarding user personal data rights protection. In this regard, if people want to better safeguard the rights and interests of users' data in the era of big data, the government must take the lead in macro-control, establish and strengthen relevant institutions, and implement and strengthen relevant legal systems. The second step is for all social disciplines to develop their own multi-subject supervision mechanism. Lastly, it is necessary to give priority to the application of science and technology; on the one hand, it might as well to use scientific and technological means to improve the security of user data. On the other hand, it is also a good way to break criminals' technical means and prevent user data leakage.

The literature chosen for this paper cannot encompass all ages and is insufficiently exhaustive, and this research methodology is immature. In addition, the contemporary data era is still evolving rapidly, and the data security industry will continue to improve.

References

[1] Consulting Research Report on Industry Competition and Investment Strategy in cmnet from 2022 to 2028, 2022. https://zhuanlan.zhihu.com/p/536700394

[2] The realistic dilemma and path choice of personal information protection in the era of big data, Journal of information, (12),155-159+154, 2019.

[3] User data: as privacy and as assets? -legal and ethical considerations of personal data protection, Editorial friend, (10), 74-79, 2019.

[4] On the disclosure of citizens' privacy under the network media environment-taking the disclosure of Facebook user data as an example, Research on Communication Power, (15), 221-222, 2020.

[5] Thinking about privacy dilemma facing big data technology, Jianghan Forum (08),65-70, 2020.

[6] Troy Segal, What is Big Data? Definition, How it works and uses, 2022. https://www.investopedia.com/terms/b/big-data.asp

[7] Tankard, C. Big Data Security, Network Security, 5-8, 2012.