ISSN: 1813-4890

Open Platforms and Personal Information Protection for College Students in the Digital Economy

Pinpin Cheng

School of Accountancy, Anhui University of Finance and Economics, Bengbu, Anhui 233000, China

535482129@qq.com

Abstract

In the era of digital economy, while college students enjoy convenience and convenience, it also brings a crisis of personal information protection. As the most active group in the information age, college students will undoubtedly face greater difficulties. The dissemination of information on open platforms has the characteristics of instant circulation and dispersion, making personal information face unprecedented risks of infringement. This article clarifies the boundary between open information and personal information on open platforms, and constructs a logically consistent open platform compliance paradigm from multiple dimensions, in order to balance the conflict of interests between deeply exploring the potential value of open information and fully ensuring the reasonable use of personal information, and to reconcile the practical contradiction between the sharing and utilization of personal information and security protection.

Keywords

Digital economy; Open platform; College students; Personal Information Protection.

1. Introduction

In recent years, the phenomenon of personal information leakage among college students has occurred repeatedly, making it difficult to ensure information privacy and personal and property security. Strengthening the awareness of personal information protection among college students and improving legal protection are important measures to maintain the safety and stability of schools and protect the legitimate rights and interests of college students. Currently, major internet companies both domestically and internationally are vigorously building open platforms. Information entities face not only direct and single connections with service providers, but also multiple interconnections with data intermediaries and subsequent users. If we focus solely on the comprehensive protection of college students' personal information and require that all personal information is obtained and used with strict authorization and consent from the information subject, information sharing becomes unsustainable, unable to provide substantive protection for college students' privacy, and becoming an important constraint on the development of data value. In the era of digital economy, how to internally reconcile the contradictions and conflicts between personal information protection for college students and data sharing on open platforms, and seek the best balance between the two, has become the key. As an emerging product, open platforms need to find a "shelter" within the existing legal track. In response to the problems existing in current open platforms, we need to explore solutions to reconcile the contradiction between personal information protection and information openness and sharing, in order to provide new ideas for the protection of personal information for college students.

ISSN: 1813-4890

2. Legality Inspection of Open Platform Open Information

2.1. Clarifying the Nature of Open Information

The establishment of an open platform aims to achieve a win-win situation for multiple entities and maximize the effectiveness of personal information through the reasonable sharing of personal information among some users. In the context of an open platform, personal information includes four types: basic personal information, extended information, behavioral information, and social background information. Compared with traditional semantic personal information, the scope is somewhat limited, emphasizing more on the sharing, liquidity, interactivity, and profitability of personal information. Within the framework of open platforms, user personal information is not static and unchanging, but gradually increases with the participation in online activities on open platforms, and user information also shows an increasing trend. The subject of obtaining personal information that is not shared on open platforms is limited, the utilization rate is relatively low, and the possibility of infringement on citizens' rights is relatively small. Therefore, the protection of personal information in the context of open platforms should be greater than that of ordinary personal information.

Open platforms are based on the sharing of user data, which is the digital display of user information and information. The academic community has varying opinions on how to define personal information, mainly including "identification theory", "privacy theory", and "value theory". "Identification" refers to the process from information to individuals, which means that information that can identify a specific subject is personal information. "Association" refers to the process from individuals to information, which means that information related to a specific subject is personal information. Personal information has a strong personal attachment, and without a specific subject, there is no attachment. Both paths emphasize the corresponding relationship between a specific subject and specific information, which are two aspects of a thing. "Identification" and "association" can be summarized as a whole using "identifiability". Overall, "identifiability" refers to the correlation and specificity between relevant information and specific citizens, through which specific subjects can be directly identified or indirectly identified by combining with other information.

2.2. Lack of user authorization requirements for personal information sharing

Both *the Cybersecurity Law* and *the Consumer Rights Protection Law* clearly stipulate that: "When collecting and using personal information, one should follow the principles of legality, legitimacy, and necessity, publicly collect and use rules, clearly state the purpose, method, and scope of collecting and using information, and obtain the consent of the recipient." The national standard "Personal Information Security Regulations" released in 2018 also stipulates the collection using personal information, explicit consent from the information subject and authorization from the information subject are required.

2.3. Risk of personal information leakage in the context of information exchange

The interaction and sharing of information is one of the most significant characteristics of the internet age. In the era of electronic exchange and massive utilization of personal information, there is a trend of massive sharing and rapid circulation of personal information. The separation of personal information subjects and information control subjects has become a normal phenomenon, gradually forming prominent characteristics of personal information that are not exclusive, easy to copy, and uncontrollable. Personal information is extremely easy to be transferred and used without permission, as a result, specific subjects lose autonomous control over personal information.

ISSN: 1813-4890

Data is regarded as the new oil, and its importance and value are self-evident. While enjoying the convenience and progress brought by the Internet, people face unprecedented risks of personal information infringement due to the real-time flow and dispersed and difficult to control characteristics of online information dissemination. Participants in the cyberspace can only obtain corresponding services after providing a large amount of personal information, The imperfect information security prevention mechanism puts personal information in a dangerous state that may be leaked at any time. The potential value temptation of personal information and the widespread application of big data analysis technology further exacerbate the risk of infringement.

3. Problems with Personal Information of College Students

3.1. College students lack awareness of personal information protection

In the era of big data, the learning and life of college students are filled with various APP software, membership registration, and information registration scenarios that require personal information to be provided. If one is not careful, personal information leakage or even account theft may occur, causing varying degrees of personal and property damage to college students. At this stage, college students generally lack the awareness of personal information protection, freely connect to free WIFI, easily allow all kinds of software to read personal information, often scan the QR code to pay attention to the official account for small gifts, etc. These are very common behaviors of college students, making the cost of obtaining personal information extremely low, resulting in frequent telecommunications network fraud cases such as campus loans, network loans, swipes, account theft, etc.

3.2. High vulnerability in student information management in universities

The vast majority of units and departments in universities have a requirement to collect student personal information in their daily work, which is undeniable. This is a basic condition for normal work, but it also poses a huge challenge to the protection of personal information for college students. At present, comparative activities such as university awards and evaluations require a public disclosure process, which inevitably requires the disclosure of students' personal information, providing opportunities for unscrupulous individuals to take advantage of. Many university teachers rely on student assistants for their work, and various statistical tables are spread freely among students, making it difficult to avoid risks. The imperfect information management mechanism for university students can easily lead to group information reselling and damage the legitimate rights and interests of university students.

3.3. Imperfect laws and regulations on personal information protection for college students

At present, the frequent occurrence of account theft and fraud among college students due to personal information leakage and other reasons has become a hot social issue. Although *the Cybersecurity Law* issued in 2016 and *the Interpretation on Several Issues Concerning the Application of Laws in Handling Criminal Cases of Infringement of Personal Information of Citizens* issued by the Supreme People's Court and the Supreme People's Procuratorate in 2017 have begun to focus on the legal protection of online public relations information, more emphasis is placed on maintaining the national and social cybersecurity, not on personal information legal protection, nor on college students. In terms of current laws and regulations in China, it is necessary to establish specialized and targeted information protection laws for college students, strengthen daily legal supervision and assistance relief, and provide a good social environment for campus security, stability, and the growth and development of college students.

ISSN: 1813-4890

4. Pathways to Protect Personal Information of College Students

4.1. Open Information: Introducing the "scenario based" standard to define personal information

Openness is an inherent label of the Internet, and it is inevitable for open platforms to open personal information. Clarifying the boundaries of "personal information" is the logical starting point for building a reasonable open platform system. As mentioned earlier, the extension of personal information in the context of open platforms is somewhat limited compared to ordinary personal information, and it is more fluid and difficult to protect. Therefore, the protection of personal information in the context of open platforms should be greater than that of ordinary personal information. We should fully consider the unique characteristics of open platforms and distinguish them from the traditional "recognizable" personal information recognition standards. We should introduce a "scenario based judgment" method for personal information recognition on open platforms, and construct a dynamic and changing path for personal information recognition on open platforms, rather than a fixed, rigid, and unchanging one.

(1) The shortcomings of traditional standards for defining personal information. Defining personal information from the perspective of "identifiability" is a common practice in various countries. Among them, the information that can identify a specific subject alone has a strong personal dependence, while the information that needs to be combined to identify a specific subject is unrelated to the specific subject or has weak personal dependence. However, with the rapid development of technology and the improvement of big data mining and integration capabilities, more and more information that appears to be unable to identify a specific subject can become "identifiable" through multiple media or when combined with multiple pieces of information, The ability of information to identify specific subjects is increasing, and the boundaries between identifiable and unidentifiable, as well as privacy and disclosure in cyberspace are becoming increasingly blurred. More and more information has the dual attributes of "public information" and "personal information", and the scope of "identifiable" personal information is constantly expanding. The dynamic and situational nature of defining personal information poses obstacles to judicial recognition. The dilemma of defining personal information as "identifiable" has attracted the attention of some scholars. From the perspective of relevant laws and regulations in China, the definition of personal information is constantly expanding. However, the scope of legal protection cannot be expanded without limitation. In the current context of "data being generated anytime and anywhere", it is worth considering whether "identifiability" can continue to be the single standard for defining personal information.

(2) The identification standards for personal information in open platforms. The goal of personal information protection in open platforms is to prevent the indiscriminate use of personal information, while advocating for the rational use of personal information by open platforms. Open platforms have their own unique attributes, and opening up information such as product names and prices is essential and unavoidable. The scope and boundaries of personal information should be dynamic. In the era of big data, the usage scenarios of personal information are complex and ever-changing, beyond the scope of legislation that can be standardized and foreseen. The idea of dynamically defining personal information protection based on user centeredness and result orientation has increasingly become a trend in national legislation, gradually advocated and recognized by the international community.

Open platform personal information can construct a "scenario based" identification model. Jump out of the traditional single identification standard, start from the principle of "specific problem specific judgment", and conside multiple factors comprehensively and fully in specific scenarios for imagination, in line with the general understanding and reasonable expectations

of the public. The advantage of adopting the "scenario based identification" model is that it improves the predictability of personal information judgment, with prior judgment. It only considers whether it can be independently or combined into personal information in the current scene and current technological background, without considering whether it can be combined with other fragmented information, and without considering whether it can become personal information with the further development of big data mining and analysis technology, This greatly reduces the compliance cost of open platforms, which is conducive to achieving a balance between personal information sharing and protection.

4.2. Open approach: constructing data desensitization rules with the "proportionality principle" as the core

At present, the vast majority of open platform open information has not undergone technical processing such as fuzzification and anonymization. In order to reduce the infringement of personal information and fully leverage the effectiveness of open platform information exchange, the principle of proportionality should be upheld, and data masking (also known as data bleaching) should be carried out on open platform intended open information at the technical level. Data desensitization needs to follow a set of scientific and reasonable rules. If data is excessively desensitized, the value of the data will be lost. If the degree of desensitization is low, it will pose a threat to personal information security. Therefore, data desensitization needs a unified and appropriate set of standards to regulate it. However, currently, China has not introduced relevant standards. China urgently needs to establish a standardized set of data desensitization standards, dividing the degree of desensitization into different levels, and using the degree of coupling between this information and personal life as the standard to apply different desensitization standards.

Article 41 of *the Cybersecurity Law* stipulates that the collection and use of personal information of natural persons shall follow the principles of legality, legitimacy, and necessity. Article 814 of *the Draft Parts of the Civil Code* also has similar provisions. In addition to the principles explicitly stipulated in the above laws, information sharing on open platforms should also follow the principle of proportionality. The principle of proportionality originated in administrative law and has always been known as the "imperial clause" in the field of public law. Although it originated in the field of administrative law, it has long crossed the boundaries of specific departmental laws and become a universal and fundamental guiding principle in modern rule of law society. There is a contradiction between the efficiency of information sharing and the protection of personal information in open platform information sharing, and there is also a dilemma in data desensitization to prevent privacy leakage and reduce information loss. In order to maximize the economic utility of personal information on the basis of protecting personal information, data desensitization of open platform information should be carried out within the framework of the principle of proportionality, Adopt a solution that minimizes damage to interests and preserves other interests. Specifically, first of all, data desensitization requires retaining the characteristic conditions of the original data while exchanging sensitive information. Only management personnel or authorized users have the authority to access data for statistical purposes, ensuring the security of data sharing and usage. Data desensitization can continuously expand the scope of user use while ensuring security. Data desensitization is the most effective method for protecting data in the context of big data.

Secondly, the current technological processing of personal information mainly adopts the methods of "anonymization" and "fuzzification", but it has many drawbacks. For example, the fuzzification of certain sensitive information may actually attract others' attention. In the context of big data mining technology, as long as there is enough data and advanced technical support, specific entities can be identified. Admittedly, desensitization of data cannot completely block the identification of specific subjects. However, identifying specific subjects

through desensitization information requires sufficient data and advanced technology as the primary prerequisite. Data desensitization shields sensitive information and preserves its original data format and attributes to ensure that applications can operate normally during the development and testing process of using desensitized data, improving the level of personal information protection. It is more conducive to achieving the goal of balancing data security and data usage.

Finally, data desensitization does not mean desensitizing all information, but rather classifying personal information in a "ladder like" manner. The famous German case "Drugstore Judgment" refined the principle of proportionality, and its establishment of the "three tiered" analysis model is considered the most important contribution of the judgment to the fundamental theory of basic rights, with strong exemplary significance. The data desensitization rules for personal information can refer to the "pharmacy judgment". When it comes to personal sensitive information, as it is closely related to the peace of personal life, the level of protection for it should be higher than that of general personal information. When sharing, the explicit authorization of the information rights subject should be fully obtained to achieve a high degree of data desensitization. The correlation between personal information other than sensitive personal information and personal life is relatively low, and its protection can be relatively weakened. The conditions for data sharing can be relatively relaxed, and the degree of desensitization can be relatively low. Different scales of desensitization rules can be adopted based on the importance of personal information, which can achieve proportionality between means and purposes.

4.3. Authorization Mode: Establish a cross model between "triple authorization" and "reasonable expectation"

The Cybersecurity Law and *the Consumer Rights Protection Law* require the consent of the recipient when collecting and using personal information, but there are no clear and detailed provisions on the form of such consent and whether it can be in the form of "implied" consent. In the operating mode of open platforms, authorization should include both consumer authorization and open platform authorization. The characteristic of big data applications is the need to obtain massive amounts of individual information data for application analysis. With the rapid development of big data mining and analysis technology, everyone is constantly producing data and information. In this context, we should pay more attention to the protection of personal information. The reason why data sharing requires personal authorization is that data sharing includes the transmission and collection of personal information, which may pose a certain threat or even infringement to personal information and privacy during the sharing process. The "express authorization" mode should be adopted to let users clearly know which information will be collected and utilized, reducing the risk of information infringement. From the perspective of the information subject, it is actually a "dual authorization", Article 817 of *the Draft of the Civil Code of China* coincides with the paradigm of "dual authorization", requiring information subjects to authorize information sharing, not limited to authorizing information collection behavior. When information is shared again by the sharer, they should still be authorized by the information subject again.

In the context of the explosive growth of big data, although each authorization mode of triple authorization is rooted in different scenarios and prerequisites, for example, in "User Authorization 1", users only know that the open platform will obtain their information, but do not know which third party the information will be transmitted to. In "User Authorization 2", users clearly know that the information will be transmitted to a specific third party, and the "authorization" will be provided for users to choose again Considering the opportunity, based on their own situation, the information they agree to authorize may be limited compared to the information authorized during "User Authorization 1". The two "User Authorizations" provide

ISSN: 1813-4890

dual protection for personal information protection. However, the "triple authorization" model may incur huge authorization costs, which is not conducive to more convenient sharing of data resources among various entities, creating greater social benefits, and maximizing the acquisition of "data gold mines". Helen Nissenbaum, who has had a significant impact on the legislation of the Consumer Privacy Act in the United States, can consider drawing on the theory of "reasonable expectations" in US law. She once stated that in determining whether there is an infringement of data privacy, "reasonable expectations" in different scenarios should be considered. The theory of "reasonable expectations" is not only in line with the inherent meaning of the "scenario based" identification model of personal information, but also can compensate for the inherent shortcomings of the high cost of data collection in the "triple authorization" model, and properly balance the relationship between data sharing and the protection of personal information and data rights.

5. Conclusion

College students, while enjoying the benefits of the digital economy era, also face the risk of personal information being violated. The "openness, equality, collaboration, speed, and sharing" of open platforms is a clear manifestation of the spirit of the Internet. However, openness should not touch the red line that infringes on personal information, and a balance should be sought between information sharing and personal information protection. Enrich the identification criteria for personal information based on the traditional "identifiability" benchmark, explore the cognitive "scenario based" judgment mode, and reconstruct the open platform from the triple perspectives of open information, open means, and open mode, so that personal information can not only maximize its function as data, but also receive the due respect and protection, in order to promote the long-term protection of personal information for college students in the Internet era.

Acknowledgments

This research is funded by Research project of Anhui University of Finance and Economics, "Research on the Value and Path of Strengthening Personal Information Security Education for College Students in the New Network Era" (No.: ACKYC22071).

References

[1] Mei Shaozu. Legal Norms for E-commerce [M]. Beijing: Tsinghua University Press, 2000.

[2] Tan Xiaoqing. Research on the Theory and Judgment of Intellectual Property Protection in the Digital Era [M]. Suzhou: Suzhou University Press, 2005.

[3] Kong Lingjie. Legal Protection of Personal Data Privacy [M]. Wuhan: Wuhan University Press, 2009.

[4] Qi Aimin. Research on the Principles of Personal Data Protection Law and Its Cross border Circulation Legal Issues [M]. Wuhan: Wuhan University Press, 2004.

[5] Cheng Xiao On Personal Data Rights in the Era of Big Data [J]. Chinese Social Sciences, 2018, (03).

[6] Peng Litang, Rao Chuanping. The attributes of online privacy: from traditional personality rights to information self-determination [J]. Legal Review, 2006, (01).

[7] Xu Jin. Legal Protection of Internet Privacy in the United States [J]. Modern Intelligence, 2005, (06).

[8] Qi Aimin. Draft Model Law of the People's Republic of China on the Protection of Personal Information [J]. Hebei Law, 2005, (06).

[9] Wang Liming. On the Status of Personal Information Rights in Personality Rights Law [J]. Journal of Suzhou University (Philosophy and Social Sciences Edition), 2012, (06).

[10] Wang Liming. On the Legal Protection of Personal Information Rights - Centered on the Boundary between Personal Information Rights and Privacy Rights [J]. Modern Law, 2013, (04).