ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202204_5(4).0046

# Responsibility of Online Platforms from the Perspective of the Draft Personal Information Protection Law

Erjing Sun[1, a]

[1]Anhui University of Finance and Economics, Anhui, China

[a]937838534@qq.com

## Abstract

**With the development of science and technology, the protection of personal information on Internet platform has also changed from weak to strong. From the Personal Information Protection Act (Draft) of 2020 to the Personal Information Protection Act of 2021 (Draft II). We can see that the protection of personal information tends to improve. Not only does the definition of personal information protection become clearer, but also the obligation of the oversized Internet platform to protect personal information is increased, and the presumption of fault is clearly assumed as the principle of attribution for the infringement of personal information. On this basis, this paper thinks that we should pay more attention to the role of network service providers in it. Network service providers should follow the principle of opt-consent, the principle of a small amount of adequate use, the principle of transparency, the principle of ensuring security, the principle of clarity of purpose, and the principle of consistency of authority and responsibility in the collection and processing of personal information. These principles contribute to the development of the economy and social stability and can have a long-term impact.**

## Keywords

**Personal Information; Network Service Providers; Economic Development.**

## 1. Background of Personal Information Protection

Since the end of the twentieth century, information technology has begun to develop rapidly. With the continuous progress of the times and the rapid development of the network, people's speed of information dissemination and information processing ability have been greatly improved. In an increasingly progressive social environment, data is closely linked to life: in today's society, people use mobile phones to navigate, eat with mobile phone software to buy coupons, leave personal addresses and phone numbers on takeaway platforms, and use mobile phones and computers to buy groceries and shops. Today's lives have changed dramatically compared to twenty years ago, and most importantly, most people today have become dependent on a variety of online services.

However, while these software bring convenience to people's lives, they also bring endless hidden dangers. When people use various types of websites or software, they will fill in their personal information over and over again, and even when using some software, if they do not authorize their personal information to the software, such as reading their own address book, using their current location and reading information, then they cannot use the software normally, and their search records and IP addresses will also be recorded. When people open an account with personal information, it means that you send personal information to the corresponding institutions or companies, and some network platforms collect and classify and sort the citizens' personal information in the state of user authorization or unauthorized status, and many people can access these citizens' personal information. So criminals have many

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202204_5(4).0046

opportunities to obtain a lot of citizen information and sell it. Once citizens' information becomes a commodity that some people can buy and sell at will, the harm is infinite and irreversible.

According to relevant news reports, we can know that the leakage of personal information is very serious now. According to the data released by the China Internet Network Information Center in February 2021 and in the Statistical Survey on the Development of the Internet in China in the second half of 2020, netizens who experienced personal information leakage accounted for 21.9% of the total number of Internet users. Although this proportion is decreasing year by year, the proportion of personal information being leaked is still in a relatively dangerous state.

Personal information is related to a person's privacy, dignity, and other highly personal information. It is the foundation of a person's life. In such an era of information explosion, if personal information is not well protected, the direct consequence is that personal safety is not guaranteed, and the leakage or even abuse of personal information will produce a series of unpredictable and dangerous consequences. In the 2016 Xu Yuyu case, for example, criminals illegally collected citizens' personal information and accurately defrauded it, ultimately leading to the fall of a living life. Although the main offender was sentenced to a heavier sentence, the loss of life could not be changed. Therefore, the protection of personal information should be taken seriously, and the process of using personal information by enterprises should be limited.

## 2. Development of Personal Information Protection

The protection of personal information has always been a hot topic in academia. Since the 2020 Personal Information Protection Law (Draft) was promulgated in the whole society and widely solicited opinions from the public, it has aroused hot discussions in the whole society and academic circles. On April 29, 2021, Chinese Dawang also published the Personal Information Protection Law (Second Reading Draft). We can glimpse some trends in the protection of personal information from the revision of the draft. This article analyzes the draft as follows.

### 2.1. The Definition of Personal Information Protection Is Clearer

According to the comparison between the first edition of the Personal Information Protection Law (Draft) and the second review draft, it can be seen that in the second review draft, the definition of personal information that personal information processors can handle is more clear. According to paragraph 5 of article 13 of the Personal Information Protection Law (Second Reading Draft), in addition to the circumstances in which personal information processors can handle personal information such as obtaining personal consent and necessary for the conclusion or performance of a contract, a catch-all clause is added, that is, the personal information that has been disclosed is handled within a reasonable range in accordance with the provisions of the Personal Information Protection Law.

This article argues that it has been difficult to have a reasonable definition of the handling of personal information until now. Because in different situations, the location of personal information is different. For example, in the current outbreak of new crown pneumonia, if you are unfortunate enough to be infected with the new crown virus, although their travel trajectory and related information are in the category of personal privacy in normal times, they need to be strictly subject to the law Protection; however, after being infected with the new crown virus, the trajectory of his personal journey belongs to the category of public information, because this involves the prevention and control of the epidemic and the implementation of corresponding policies, which are in the public interest, and when the public interest and personal interests cannot be taken into account at the same time, the individual Rights should then give way to the public interest and ensure that the public interest is not compromised. In

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202204_5(4).0046

this case, personal information should be published and must be unreserved to ensure that it can be known to the public.

Article 5 defines the information that personal information processors can handle, and establishes a bottom-up clause, so that the scope of personal information is clearer than in the past, and the bottom clause provides a legal basis for the processing of information by information processors. When an enterprise needs to process information, it may use and process the personal information in its possession within the scope of the provisions of this clause. However, the bottom clause is not the only criterion for online platforms to collect and process personal information. The handling of personal information by online platforms is also subject to other factors, such as public order and good customs.

## 2.2. Increase the Obligation of Super-Large Internet Platforms to Protect Personal Information

The large Number of Internet platform users and the huge amount of information carried, therefore, the protection of personal information should also have a stricter protection obligation than that of ordinary enterprises. For example, Alibaba Group, according to relevant reports, Alibaba Group's monthly active users reached more than 900 million, it can be said that in China, Alibaba Group has the largest number of users and the highest degree of user activity. Users of the Internet platform use the Internet for daily activities such as buying, selling, consuming, and investing. In these activities, a large number of personal information is recorded, including the age, occupation, address, and interpersonal relationships and other personal information of the individual. Therefore, the obligation of Internet platforms to protect personal information should be fully taken seriously.

According to Article 57 of the Personal Information Protection Law (Second Reading Draft), Internet platforms shall establish a third-party organization to supervise the protection of their personal information, and service chambers that have not fulfilled their obligations to protect personal information are suspended from providing services to restrict the development of their business. In addition, reports on the protection of personal information shall be published periodically and subject to public supervision. This provision stipulates the obligations and responsibilities of network service providers for the protection of personal information from the legislative level, adding to the protection of personal information on the network platform.

## 2.3. Explicitly Make the Presumption of Fault the Principle of Attribution of Personal Information Infringement

According to Article 65 of the Draft Personal Information Protection Law, the principle of personal information processors assuming responsibility is the principle of fault liability. If the personal information processor can prove that he or she is not at fault in the process of collecting and processing personal information, the personal information processor may mitigate or exempt himself from the infringement of personal information liability. This provision seems to be very reasonable, but it invisibly increases the burden of proof on the victim and increases the cost of the victim's litigation. The victim bears the burden of proof not only to prove that he or she has been harmed, but also to prove that the person handling the personal information is at fault. This undoubtedly increases the difficulty of the victim's proof. Due to the unequal status of the parties to the lawsuit, the infringed party is usually the inferior party, the difficulty in obtaining evidence, the delay in litigation, the relatively long litigation time and other factors All are obstacles that prevent the infringed party from safeguarding its legitimate rights and interests through legal means.

The Personal Information Protection Law (Second Reading Draft) makes up for this shortcoming. According to Article 68 of the Personal Information Protection Law (Second Reading Draft), where citizens' personal information rights and interests are infringed, if the

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202204_5(4).0046

personal information processor cannot prove that he is not at fault at the stage of collecting, using, storing, etc., he shall bear the corresponding responsibility Tort Liability. Reversing the burden of proof not only imposes a tight curse on enterprises that use citizens' personal information, but also reduces the burden of proof on victims and reduces litigation costs. If the infringing enterprise cannot produce evidence to prove that it is not at fault, it is presumed to be at fault and needs to bear corresponding liability. To a certain extent, this measure balances the unequal litigation status between the infringer and the infringed, and opens up a shortcut for citizens to protect their rights.

## 3. Responsibilities to be Borne By Network Service Providers in the Protection of Personal Information

In summary, personal information is easily infringed in the current era of big data. In the process of legislation, legislators have given full consideration to the role that legislation should play in view of this phenomenon. While providing necessary legal protection for citizens' personal information, we also emphasize the protection of personal information by enterprises that provide network services. However, it is not enough to protect citizens' personal information by law alone, and enterprises should also follow certain rules and principles to protect personal information from infringement while conducting business. This article believes that as a responsible enterprise, it should follow the following principles in the protection of citizens' personal information.

### 3.1. The Principle of Selective Consent

Now when we use most of the mobile phone APP or computer programs, we need to register or log in. This process involves the authorized use of citizens' personal information on the online platform. Now most APPs have their own privacy terms, although most network service users will not click to check whether there are any standard terms that harm their privacy, but this principle still needs to be observed by network service providers, because Network service providers do not have the right to use and process users' personal information without authorization, and the processing of users' personal information must have the user's authorization.

Therefore, when the relevant business in life is conducting business, it is necessary to collect, store, process, use, transmit, provide, disclose, and other business-related activities such as the collection, storage, processing, use, transmission, provision, and disclosure of citizens' personal information Users who are collected, processed and processed personal information should generally have the right to choose, and citizens have the right to refuse enterprises to use their personal information, this right is not to provide a small amount or a certain amount of information hypocritically, but to ensure that the user's own right to refuse can be fully exercised. The legal basis for this principle comes from the provisions of Articles 14 to 16 of the Personal Information Protection Law (Second Reading Draft). According to these three legal provisions, when using personal information, enterprises should ensure that the user consents to the use of personal information by the enterprise under the circumstances of full knowledge and voluntariness, and when the premise of using personal information changes, it should also inform the user and obtain the consent of the user again, and at the same time fully protect the right of revocation of the user, that is, the user has the right to withdraw his personal information authorized to use. However, it should be noted here that before the user withdraws his right to use his personal information, the business carried out by the online platform for the user's personal information is not affected by the user's withdrawal of his right to use his personal information.

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202204_5(4).0046

## 3.2. The Principle of Sufficient Use of Small Amounts

According to relevant reports, in June 2018, some consumers said that when they opened the browser of a network platform, the lifting camera of their mobile phones would automatically open, and later after inspection by the relevant departments, it was found that many mobile phone programs required sensitive permissions that had nothing to do with the services they provided. This phenomenon has caused great social repercussions. A large part of the protection of personal information on online platforms lies in the network platform itself.

This article believes that when an enterprise collects the user's personal information, in order to perform the contract or successfully conclude the contract, it generally involves a considerable part of the personal privacy, but in the past, the scope of the personal information that the enterprise should obtain was not clearly defined. According to relevant reports, the mobile phone software developed by some enterprises reads the mobile phone address book and tracks the location of the mobile phone without the authorization of the user, which seriously violates the privacy of the user. According to Article 6 of the Personal Information Protection Law (Second Reading Draft) in April this year, enterprises should not only be clear when collecting and handling personal information and reasonable business purposes, and should be limited only to the minimum necessary to achieve the purpose of processing and ensure that this act has minimal impact on the rights and interests of individuals and, most importantly, that personal information unrelated to the purpose may not be carried out processing and collection.

According to this provision, an important principle that enterprises should follow when collecting and handling personal information is the principle of small amounts being sufficient. That is to say, when an enterprise conducts business, the personal information that an enterprise should collect and process should not exceed the scope of personal information required by the business, and the business must be legitimate and have a reasonable purpose. Under the premise of collecting the personal information at least, it is possible to meet the business needs of the personal information, so as to achieve the results of the purpose of the contract. For personal information unrelated to business, enterprises should not only not collect and process it, but should also promptly destroy or take confidentiality measures to protect the information after obtaining it.

## 3.3. The Principle of Openness and Transparency

According to Article 7 of the Personal Information Protection Law (Second Reading Draft), the handling of personal information shall be open and transparent. That is to say, the processing process after enterprises collect citizens' personal information should be open and transparent. In the absence of internal affairs and trade secrets involved, the enterprise shall disclose the process of collecting and processing personal information and comply with the purpose of the contract, that is, the personal information collected and processed and the realization of the purpose of the contract are necessary.

First of all, when collecting personal information, companies are required to disclose the purpose of collecting personal information, the method of processing it, and the scope of the personal information collected in a public manner, so as to ensure that the person being collected can clearly understand the whereabouts of their personal information and whether it is used for the intended purpose of the contract.

Secondly, the process of publicly using personal information is not only disclosed to the person being collected, this article believes that the network platform as an enterprise entity collects and collects within the scope of business The use of personal information shall be subject to the supervision of relevant agencies and the public, so the process and purpose of collecting and processing personal information by enterprises shall also be disclosed to the public. Transparency in the relevant processing processes can increase the sense of responsibility of

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202204_5(4).0046

the company, and accepting the supervision of society and relevant institutions can make the collected person feel that the personal information is protected, thereby increasing trust in the company. This initiative can enable both the enterprise and the counterpart to obtain the protection of benefits.

### 3.4. Ensure Safety Principles

After citizens' personal information is collected by network service providers, the most worrying thing is security. Therefore, articles 9 to 11 of the Personal Information Protection Law (Second Reading Draft) stipulate that the information collector has the responsibility to ensure the security of the personal information of the person whose information is collected. According to the provisions of Article 9, the processor of personal information shall be responsible for the entire activity of handling personal information, and shall take necessary measures to ensure the security of the personal information they process.

Therefore, in order to ensure the security of the personal information taken and processed by network service providers, they should improve their own technology to ensure that they can have enough technical skills to resist the illegal infringement of the amount of personal information, and to protect the security and confidentiality of personal information with the greatest ability.

### 3.5. The Principle of Clear Purpose

The purpose of network service providers to collect and process personal information should be clear, legitimate, reasonable and lawful. According to paragraphs 2 to 6 of article 13 of the Personal Information Protection Law (Second Reading Draft), the purpose for which network service providers collect and process personal information should be within the scope provided by the contract or law.

The information collected by the network service provider must be necessary to meet the needs of the contractual purposes, or as required by the relevant legal provisions, or for maintenance purposes The need for public interest. In the case of the epidemic, when the epidemic was at its most serious, most communities required people to stay at home, and there would be community or village committee staff who came to the door to ask to use the Alipay app to fill in the health status and population of family members, which involved a lot of personal information. However, as required by the public interest, network service providers collect personal information within a reasonable and lawful scope to ensure that the public interest is not harmed, and its purpose is legitimate.

### 3.6. The Principle of Consistency of Powers and Responsibilities

The principle of consistency of rights and obligations requires online platforms to have corresponding obligations while collecting and using users' personal information. In the provisions of Article 11 of the Personal Information Protection Law (Second Reading Draft), we can know that the state has actively established and improved it We will protect personal information and actively prevent infringement of personal information and punish acts of infringement against personal information.

The centrality of this provision is to require online platforms to have an obligation to protect while collecting and processing citizens' personal information. After personal information is infringed, corresponding liability shall be borne.

This article believes that the infringement of personal information in this article should be determined that the existence of network service providers in this regard is a kind of negligence rather than intentionality. According to the above, according to the relevant provisions of the Personal Information Protection Law (Second Reading Draft), when personal information is infringed, the principle of presumption of fault is adopted for the burden of proof. If the web service provider cannot prove that it is not at fault throughout the process of collecting and

ISSN: 2637-6067 DOI: 10.6918/IJOSSER.202204_5(4).0046

using the personal information of citizens, then it is presumed Where online platforms have certain faults for infringing citizens' personal information, the online platforms shall bear corresponding liability for compensation or other civil or administrative liabilities. According to this provision and the connotation of the principle of attribution, when a network service provider suffers damage to personal information in the case of negligence, the network service provider shall bear corresponding civil liability or administrative punishment, and where the intentional crime is committed, it shall be given an administrative punishment, civil punishment or criminal punishment depending on the circumstances.

## 4. Conclusion

Personal information concerns the privacy of individuals and other public or undisclosed information about the person's person. According to article 2 of the Personal Information Protection Law (Second Reading Draft), citizens' personal information is strictly protected by law, and any person or organization is organized Citizens' personal information shall not be harmed. Therefore, we can know that in the relevant legal provisions, personal information has been attributed to the fundamental rights of individuals. With the eager discussion of the Personal Information Protection Law, the role of network service providers in the protection of personal information has also become more and more valued. The protection of personal information is inseparable from the joint role of individuals, society, state agencies and related enterprises. While developing themselves, network service providers should also shoulder the heavy responsibility of protecting personal information, and escort the security of personal information within the scope of their capabilities.

The country vigorously develops the economy, and with the rapid development of science and technology, more and more enterprises have begun to pay attention to the Internet's shadow of their own development sound. But the Internet, an efficient and convenient platform, is a breeding ground for criminal acts that infringe on personal information. Therefore, the responsibility of network service providers to protect personal information is more stringent than that of traditional enterprises, but it also reduces the harm of economic development. Therefore, this article believes that on the basis of citizens' increasing attention to personal information, emphasizing the responsibility of network service providers has a certain role in promoting economic development and social stability.

## References

[1] QIU Xiaoling. Research on the Legal Protection of Personal Information in the Era of Big Data[J].Journal of Chongqing University of Science and Technology (Social Science Edition), 2016(12).

[2] Ren Hiromi. Business Model Innovation and Enlightenment Based on "Big Data"[J].Modern Commerce and Trade Industry, 2013(20):171-172.

[3] Ministry of Science and Technology of the People's Republic of China. International Science and Technology Development Report.2013[M].Science and Technology Literature Press,2013.

[4] Mao Rong. Legal Methods and Modern Civil Law[M].Beijing:China University of Political Science and Law Press,2001:52.]

[5] Qi Aimin. Draft Model Law of the People's Republic of China on personal information protection[J].Hebei Jurisprudence.2005,23(6).2005,6:2-5.

[6] Yan Xiaoli. Research on Personal Information and Privacy Protection Legislation in the Era of Big Data[J].Secrecy Science and Technology, 2015(9):22-25.