International Journal of Education and Humanities
ISSN: 2770-6702 | Vol. 6, No. 1, 2023

The Civil Law Protection of Internet Privacy

Liangliang Wang

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

Abstract: At present, with the rapid development of the network, the network has gradually become the main medium of people's communication, and it is inevitable to use the network in social life. When we shop in Taobao, when Tik Tok brushes short videos, and when we use search engines on websites, our personal information leaks on the network platform. In recent years, various network privacy infringement cases have been exposed, causing serious harm to network users and even affecting the security development of the network environment. There are two reasons for this situation: first, the law on network privacy protection in China is not perfect, and second, China's citizens lack the awareness of network privacy protection. We have strengthened the protection of the right to privacy, mainly through civil law, making it a civil right, and after being violated, we will provide relief through civil law. With the rapid development of network technology, we should pay more attention to the civil law protection of the right to privacy.

Keywords: Internet privacy, Tort liability, Civil law protection.

1. Right to Network Privacy and Infringement

1.1. The right to network privacy

1.1.1. The connotation of the right to network privacy

The rapid development of network technology has made people's privacy appear more and more frequently on the network. Nowadays, network users basically have no privacy in front of the network. Network privacy is developed on the basis of the vigorous development of network technology. Therefore, the right to network privacy can be roughly defined as a right that citizens enjoy in the network to enjoy peace of private life, private space, private information, etc. that is not infringed by others and is protected by China's laws. It also includes not illegally collecting, using or disseminating the privacy of others through the Internet, not maliciously slandering or slandering others on the Internet

1.1.2. Characteristics of network privacy

The ease of infringement.Against the background of the prevalence of the Internet, the network has developed rapidly, and more and more people are entering this field. The number of network users continues to rise, making the network environment mixed. Everyone has a different purpose, so that it is easier to cause citizens' network privacy to be constantly spying on, and the privacy of network users will be leaked out. The rapid development of the Internet makes citizens' network privacy more likely to be leaked and illegally used. Infringement of network privacy is more likely to occur.

The concealment of the infringing subject.The infringing subject of citizens' right to network privacy is generally individuals or organizations with superb network technology. They can leave no trace when illegally collecting the personal information of network users, and even they can use their own technology to change different identities in the network environment, so network users have no idea who illegally collected and used their own information. Even if these infringing subjects leave traces, network technology is constantly improving, and these traces may be erased by infringing subjects using advanced technology. When network users buy goods through Taobao and browse short videos on TikTok, their network privacy may have been leaked without knowing what happened. When the personal information of network users is stolen, because the thief has superb network technology, network users may not know that their privacy has been leaked, and even causing serious consequences, users are at a loss.

The seriousness of the consequences of infringement.With the rapid development and continuous updating of network technology, the privacy of network users in the network may spread faster and may spread to all corners in a short time. If citizens' network privacy is leaked, it will cause immeasurable losses. At the same time, it may cause serious consequences for network users, cause serious physical and mental harm to users, and even seriously undermine the stability of the security development of the network environment.

Multipleness of tort carriers.The right to network privacy takes the Internet as the carrier. With the vigorous development of Internet technology, various apps have also poured in, such as WeChat, QQ, TikTok, Taobao, Tmall, etc. When we use these software, our personal private information may be exposed to cyberspace and may even be illegally collected and used by some people to achieve their profit. Therefore, there are more and more carriers for criminals to violate citizens' online privacy, and it will become easier and easier for citizens to violate their online privacy.

1.2. Specific infringements of the right to network privacy

1.2.1. Provisions of the Civil Code on privacy infringement

The Civil Code stipulates the types of infringement of privacy rights. According to the understanding of the Civil Code, violations of the right to privacy have the following aspects: First, infringe on the peace of the private life of others. Daily peace includes not being disturbed in daily life, no spam advertisements, spam phone intrusion, etc. Personal choice of peace is mainly reflected in the ability to make self-determination in private life without being disturbed by others. For example, freely choosing a job, etc. Second, infringe on the private space of others. Private space mainly includes two aspects: real space and cyberspace. Realistic spaces include private homes and public spaces that citizens are using.

Cyberspace includes private email addresses, personal chat rooms, etc. Third, private activities that infringe on others. Private activities refer to daily activities that have nothing to do with others and only belong to your own. Life between husband and wife and communication with others belong to the scope of private activities. It is illegal to shoot, peep and disclose other people's private activities without their consent. Fourth, private information that infringes others. The content of private information is extremely rich, including personal health status, hobbies, physical privacy includes physical and mental health, etc. Family privacy includes family address, as well as family religious beliefs, communication processes with others and communication content. It is not possible to steal, spy or process other people's private information at will without the consent of the parties .

1.2.2. Infringement of the right to network privacy in life

Infringement performance of network users . The network user has the right to illegally disseminate or sell the private information of others on the network; copy the electronic information they are transmitting without the consent of the parties; and open the network user's private space to collect and steal private information without the consent of the network user.

Infringement performance of network service providers. Providers of network services must approve by the executive branch to provide services to the public, including network service providers and network service operators. Its infringing manifestations mainly include: providing information to intermediary companies, advertising companies, etc. without the consent of the parties concerned to achieve their profitability; infringencies on the network that infringe on the privacy of others's networks were not detected in time, and failure to take corresponding measures to prevent them, causing serious consequences for the lives of the infringed. Impact: modify the privacy of network users in the network or expose the personal privacy of network users to the network without the consent of the network user.

Infringement performance of commercial companies. After some commercial companies develop various network software, they will specially design functions to collect the private information of network users, resulting in infringement and losses to the rights and interests of network users. When network users use search engines provided by commercial companies, commercial companies can use network technology to detect the online activities of network users. Commercial companies will store the collected personal information and establish a huge personal information network. When someone needs the personal information of a specific person, they can search. Therefore, commercial companies achieve their purpose of seeking commercial interests.

Other forms of infringement. State organs and some social organizations may also violate citizens' right to online privacy. In order to pursue higher work efficiency, state administrative organs and some social organizations will count and use citizens' personal information. In the case of improper operation of staff, citizens' network privacy may be leaked. Such as communities, schools, hospitals, the judiciary, etc., and the personal information of citizens collected by these administrative departments will be more detailed and accurate. Once this information is leaked or used by relevant personnel, it will cause immeasurable damage to citizens and even affect the development of society.

2. Subjects Responsible for Infringement of Network Privacy Rights

2.1. Classification of infringing subjects of online privacy rights

With the continuous strengthening of China's national strength, the funds invested in network construction are increasing, and more and more individual users have entered the network. In this case, citizens' right to network privacy may be violated by multiple subjects. According to different nature, the infringing subjects can be divided into state organs and non-state organs.

The main body of a state organ refers to the organ exercising the public power of the state represented by government organs. Because these national institutions have to deal with the public affairs of society, they often have access to the privacy of many citizens and have the private information of many citizens. In this context, it is sporadicate that state organs and their internal personnel disclose and illegally use the privacy of others for profit. Specifically, it includes the following:

First, the People's Court and the People's Procuratorate. The people's court openly guarantees the fairness of justice on the Internet, and the public's right to know can be realized, so that the parties can believe and abide by the court's judgment. Relevant regulations have also been formulated to further regulate public content that may infringe on citizens' network privacy, which can well protect the parties' right to network privacy. However, there are inevitably some circumstances in which the privacy of the parties is leaked due to the mistakes of the staff. If some marriage and family disputes are all disclosed on the Internet without inspection due to the mistakes of the staff, the personal privacy of the parties will be disclosed on the Internet. If they are seen by others, it will have a negative impact on the life of the parties.

Second, other government departments and their staff. Government agencies have easier access to and access to citizens' private information due to the convenience of their powers. Staff of some state organs use their official convenience to sell citizens' personal information to obtain huge amounts of money. Nowadays, with the rapid development of network technology, most people are using the Internet to communicate. If the staff of government agencies sell the online communication information of the people they know to others, it will violate citizens' right to network privacy. Therefore, the newly promulgated Civil Code clearly stipulates that the staff of state organs have the obligation to keep the privacy of others.

The main body of a non-state organ is composed of network users, companies and other social organizations. Compared with the main body of state organs, the subject of non-state organs is the most important subject of infringement of the right to network privacy in daily life. It can be roughly divided into the following categories:

First, network service providers. Various websites and software developed and provided by network service providers can collect and store the personal privacy of network users. Due to the lack of self-management of network service providers, the outflow of personal privacy of network users is increasing. The personal information of network users is not well protected. After the personal information of network users is illegally obtained, criminals will use the

obtained information to harass the personal lives of network users, which will have a serious impact on the lives of citizens. In order to better protect citizens' network privacy, network service providers should strengthen their own management and construction and improve their technical level to prevent criminals from obtaining the personal information of network users on the platform.

Second, private users of the network. With the rapid development of network technology, the network environment will generate more business opportunities, causing more and more people to enter the network, and the number of netizens will continue to increase. After some people commit certain behaviors on the Internet, due to age and cultural restrictions, they do not know that the act they have just committed has violated citizens' right to online privacy. Of course, in most cases, infringement of citizens' online privacy is intentional and purposeful infringement. Private users on the Internet have a variety of infringement purposes, some are based on envy and jealousy, maliciously tampering with and fabricating citizens' personal privacy, and leaking out citizens' privacy; some are based on curiosity, illegally entering other people's cyberspaces and peeping at other people's private information; some are based on hatred. Psychologically, in order to retaliate against each other, they leak their personal privacy into the Internet and expose them to network storms. Of course, in many cases, the invasion of the privacy of others is for economic interests. Criminals obtain personal information and sell them to organizations or individuals in need for huge economic benefits.

Third, other non-state organs. People have social attributes and cannot exist in isolation from society. In social life, they will inevitably intersect with others. In addition to the above subjects, the subjects that infringe on the privacy of citizens' network also include some social organizations. If community organizations fail to fulfill their due confidentiality obligations, the personal information of the community is leaked and obtained by criminals, it will seriously affect the stability of community life; hospitals and clinics do not effectively manage patients' personal information and disclose it to individuals or organizations selling medical supplies; there are also various funds. The organization did not manage the personal data of donors and Foundation staff, resulting in the disclosure of various information of the Foundation. There are many similar violations of citizens' online privacy in life practice.

2.2. The principle of attribution of the infringing subject of network privacy rights

2.2.1. Application of the principle of fault liability

Liability for fault means that it is not necessarily liable for damage. It must be seen whether the perpetrator is at fault. If there is fault, it will be liable, and if there is no fault, there will be no liability. It includes the following meanings: (1) the perpetrator has committed a certain act; (2) the perpetrator has committed a wrongful act; and (3) the victim's civil rights and interests have been damaged by the wrongful act.

There are several reasons: First of all, the right to network privacy is ultimately the right to privacy. The principle of attribution of the right to privacy adopts the principle of fault liability in judicial practice, so it is common sense to apply the principle of fault liability to the principle of attribution of the right to network privacy and can be well used in judicial practice. Moreover, because the principle of fault liability has a certain flexibility limit relative to the principle of no-fault liability, the application of this principle is more conducive to the development of the network and can provide a more relaxed environment for the rapidly developing network.

2.2.2. Application of the principle of no-fault liability

The principle of no-fault liability means that if the law should bear civil liability regardless of whether the perpetrator is at fault or not, the perpetrator shall bear civil liability for the damage caused by his actions .

In China, some experts have proposed that the principle of no-fault liability is more suitable for infringement cases of network privacy. Because compared with network users, network service providers have natural advantages. The technology and capabilities of network users cannot be compared with these network service providers. Therefore, network users will be at a disadvantage and cannot effectively protect their rights. The application of the principle of no-fault liability will put network users in an equal position as infringers when defending their rights. In the face of litigation cases on the right to network privacy, network users can normally protect their interests.

2.2.3. Application of the principle of presumption of fault

The essence of the presumption of fault is to presume that the perpetrator is at fault from the facts of infringement. There is no need for the defendant to prove the fault of the plaintiff's behavior and increase the burden of proof of the perpetrator. It should be emphasized that the law strictly stipulates the scope of use of the presumption of fault principle.

The reason for applying the principle of presumption of fault in network privacy infringement cases is that the infringing subject of network privacy is generally network service providers. When confronting in court, the infringed person is often at a disadvantage, because network users do not have the ability to extract evidence from highly skilled network service companies. This will cause the infringer to have enough evidence to be convicted. If the principle of presumption of fault is applied, the position of both parties can be balanced. However, applying the principle of no-fault liability will increase the burden on network service providers and cause the risk of instability in the network environment. Therefore, combining the above considerations, it is most reasonable to apply the principle of presumption of fault.

3. The Current Situation and Existing Problems of Civil Law Protection of Network Privacy Rights in China

3.1. The current situation of civil law protection of online privacy rights in China

Due to historical reasons and the limitations of lag in the development of science and technology in China. In the decades since the founding of New China, no special attention has been paid to the protection of online privacy. In the past two decades, due to the strengthening of China's comprehensive national strength and the rapid development of science and technology, the network has spread all over the streets and alleys. However, China has not yet established a law to protect the privacy of citizens' networks, and the protection of the privacy of our citizens' networks is reflected in some other laws.

3.1.1. " Protection of the right to network privacy in the Civil Code

The Civil Code compiles the right to personality independently and clearly stipulates the right to privacy. It not only strengthens the protection of citizens' right to privacy, but also makes up for the meaning and protection of the right to privacy in China. Blankness is regarded as a highlight of the Civil Code. Article 111 stipulates that the personal information of natural persons shall be protected by law. Article 1032 stipulates that natural persons have the right to privacy. And this clause covers most of the violations of the right to privacy in daily life, and also provides a bottom clause. At the same time, this provision also adds a provision "provisioned by law otherwise", through which other laws can impose the necessary restrictions on rights if the purpose is legitimate.

China's current Civil Code clearly stipulates the liability for network tort in Part VII. It clarifies the legal status of the right to network privacy, which reflects that the state pays more attention to the protection of the right to network privacy. Moreover, this law establishes a notification and removal system and a counter-notification system to protect citizens' right to network privacy.

3.1.2. " Protection of the right to network privacy in the Cyber Security Law

The current Cyber Security Law of the People's Republic of China clearly stipulates the protection of the personal information of network users [see Articles 41, 42, 43 and 44 of the Cyber Security Law of the People's Republic of China]. It reflects the importance of online privacy to citizens in today's society. The Cyber Security Law protects citizens' network privacy in two aspects. The first is to regulate from the perspective of network operators. Articles 41 and 42 of the Cyber Security Law stipulate the tort liability of network operators: After infringement, network operators shall take corresponding measures to prevent network users from being subjected to secondary infringement. They shall also notify network users and relevant departments in time when they know that the infringement occurs or there is a tendency to cause infringement, so as to prevent Occurrence of violations. Second, it is stipulated from the perspective of network users. Articles 43 and 44 of the Law stipulate that if a network user finds that the network operator collects and uses his or her network privacy without his or her consent, he may require the network operator to delete his or her network privacy and stop the infringement.

3.2. Problems existing in the protection of civil law on the right to network privacy in China

3.2.1. The content and legislation of the right to network privacy are unclear

In the current network environment, the emergence of the right to network privacy makes us pay more attention to the protection of the right to privacy, which is derived from the right to privacy on the basis of the rapid development of the network. Although the Civil Code in force today provides targeted provisions on the right to privacy, it does not specify the right to network privacy, and the provisions on the right to network privacy only exist in some judicial interpretations and the Cyber Security Law.

The content of network privacy is unclear . Neither the Civil Code nor the Tort Liability Law and other relevant laws and regulations clearly stipulate the content and object scope of the right to online privacy. This keeps citizens in a vulnerable position in the infringement of the right to network privacy, because citizens do not know what content the right to network privacy should include and how to violate their right to network privacy? In the end, citizens can only use ex post facto relief to exercise their right to cyber privacy.

The legislation on the right to network privacy is not targeted. Judging from the current laws and regulations in China, the legislation on citizens' online privacy is not targeted. China's current laws and regulations on the protection of citizens' right to network privacy are basically scattered in various judicial interpretations and administrative regulations. There is no special legislation on citizens' right to network privacy, let alone a complete legal protection mechanism. In addition, China adopts the principle of indirect protection. The protection of citizens' network privacy is mainly by strengthening citizens' awareness of network security. The law does not provide for the direct protection of citizens' right to network privacy.

3.2.2. The principle of attribution for online privacy infringement is unreasonable.

The infringement of the right to network privacy is more complicated than the infringement of the right to privacy. The method and path are very different. Netizens' awareness of the protection of network privacy rights is already weak. Coupled with their unfamiliarity with the network environment and the complexity of the network environment, netizens are infringed on their right to network privacy without knowing it.

In cases of infringement of network privacy, netizens are obviously at a disadvantage for network service providers. The network technology of network service providers is professional and has great technical advantages. In practical judicial practice, the determination of network tort liability adopts the principle of "whoever claims to give evidence". Generally, the plaintiff bears the burden of proof, including the proof of the facts of infringement and claims. Because the plaintiff may not be able to collect evidence or the evidence collected is limited due to network technology, the plaintiff may lose the lawsuit and the defendant will not receive due sanctions by law. Cases in which the infringed person loses the case due to the unreasonable distribution of the burden of proof often occur in real life. In judicial practice, there are the following manifestations of the failure of the infringer due to his insufficient ability to prove.

First, the plaintiff could not provide evidence. Nowadays, network technology is booming, making network content ever-changing and the network environment quite complex. It is very difficult for plaintiffs to find evidence of infringement in such a large network environment based on their own ability.

Second, the evidence provided by the plaintiff is not enough to prove his claim. The plaintiff did not comply with the provisions of laws and regulations when looking for the selected evidence, or because there was too little evidence for technical reasons, the evidence was insufficient to prove and there was no additional evidence to prove it, which led to the plaintiff to lose the lawsuit.

Third, the plaintiff's ability to collect evidence is limited. In judicial practice, the infringing subject of network privacy infringement cases is generally the provider of network services or the operator of network services. In the face of such infringement subjects, network users have no ability to

obtain data from within the infringing subject to prove. Because of the plaintiff's limited ability to prove, the infringing subject will not be punished by the law, and the interests of the infringed person will not be effectively relieved, which will cause the network environment and its unfair situation.

3.2.3. The remedy of the ex post facto rights of online privacy is inappropriate.

Many cases of infringement of the right to privacy on the Internet cause serious damage to the spiritual life of the infringed. Therefore, when dealing with such cases, the judiciary usually remedy the rights of the infringed by stopping the infringement, removing obstacles, eliminating the impact, apologizing, and restoring the reputation. However, in judicial practice, we find that these remedies are not appropriate to the damage suffered by the infringed person. The reasons are as follows: first, the network spreads extremely fast and covers a wide range. Once citizens' privacy is violated on the Internet, it may spread all over the Internet in a very short time, the suffering of netizens will be doubled, and the impact of the incident will continue to expand; second, the infringer may It is a provider of network services. Such infringing subjects have a natural advantage in the network environment. It is difficult for the infringed to obtain evidence to prove their infringement, so that the infringer does not receive the original punishment. Third, in the case of infringement of the right to network privacy, the infringement not only damages the spiritual life of the infringed, but also It will cause serious damage to his person and property .

4. Suggestions for Improving the Protection of China's Network Privacy Civil Law

4.1. Formulate laws and regulations on the right to network privacy

The meaning of Chinese citizens in protecting network privacy is relatively weak. The state has not enacted specific laws and regulations to protect citizens' network privacy, which will cause citizens to do not have good remedies after their right to network privacy is infringed, and even cause instability in the network environment. Therefore, the state should incorporate the right to cyber privacy into the law on the basis of existing laws. First of all, we should clarify the content of the right to network privacy. We can learn from the legislative experience of Western countries on the right to network privacy. The content of the right to online privacy can be roughly divided into: the right to know, the right to modify, the right to restrict use, the right to self-determination and the right to compensation. Then, we should expand the object scope of network privacy. Because network technology is constantly developing, emerging things in the network are constantly emerging, and the damage to network privacy infringement is so serious. The objects of network privacy should include private cyberspace, independent network behavior and personal private information, etc. However, due to the continuous development of the network, these objects should be further expanded and detailed on the original basis.

4.2. Establish the principle of attribution of reasonable liability for tort

China adopts a single principle of attribution in privacy infringement cases, that is, the principle of fault attribution. However, in judicial practice, it is difficult for the infringed to find evidence at the time of the violation, or because the evidence provided is limited to prove that it is not enough to convict the infringer. Therefore, a single principle of attribution cannot be applied in network privacy infringement cases.

Using different rules and principles in different situations is conducive to protecting citizens' right to network privacy. Therefore, when dealing with cases of network privacy infringement, we should apply different principles to different situations. For acts committed by ordinary infringers that infringe on the privacy of others, the principle of attribution of fault liability should be applied; but when the infringing subject of network privacy is a special infringing subject such as network service provider or government agency, the principle of presumption of fault should be adopted.

4.3. Refine the remedies for tort liability

Several remedies for rights stipulated in the Civil Code are the most commonly used remedies for tort liability in China, but when these remedies are used in the right to network privacy, there are some unreasonable and inappropriate places, which should be further refined in the infringement cases of the right to network privacy.

First, further refinement of "stop damage". After committing an infringing act, the infring subject should immediately delete or modify the network privacy of the infringed person when receiving the notice of the infringed person, or cause a negative social impact after improper information collection and processing by the infringing subject, and the infringing subject actively deletes and modify to prevent the infringed person. Private information spreads rapidly on the Internet, causing a more serious impact .

Second, further refinement of "compensation and apology". The remedy of compensation and apology in the right to network privacy should be refined as follows: the infringing subject can apologize to the victim in the form of a website website, email or face-to-face apology to apologize to the infringed person. However, such an apology method may cause secondary damage to the infringed. Therefore, it is up to the infringer to decide how the infringer should make apology, and other organizations or individuals do not have the right to interfere.

Third, further refinement of "compensation for losses". The infringement of the right to network privacy will cause moral and material damage to network users, so the liability should include moral and material compensation. Material damage compensation for direct losses caused by infringement, such as litigation costs, missed work expenses and other necessary expenses, also include indirect losses caused by the social impact caused by the infringement. Compensation for moral damage shall be compensated according to the degree of damage caused. The compensation for moral damage corresponding to the degree of mental damage caused by network infringement can be divided into three types: general moral damage compensation, serious moral damage compensation, and especially serious mental damage compensation. General moral damage compensation refers to the serious psychological discomfort caused by the infringed, and the scope of impact is large. Compensation for serious mental damage refers to the serious damage to the aggrieved person's daily life and work state, mental depression, mental disorder, etc. The impact is rapidly spread on the Internet, and it cannot make up for the mental state of the infringed by

means of relief. Particularly serious mental damage compensation refers to the extreme depression, suicide and self-inflicted behavior of the infringed person.

To sum up, although China has carried out significant legislative protection in the protection of the right to network privacy in recent years, there is still a long way to go to improve the protection of the right to network privacy. Based on the actual situation in China, pay attention to the development trend of network technology, learn from relevant relevant foreign legislative experience, and then continue to improve the civil law protection of citizens' right to network privacy.

5. Conclusion

With the rapid development of the Internet industry in today's society, the Internet has become the main medium of communication between people, and people's daily life is inseparable from the Internet. The rapid development of the Internet has also exposed citizens' personal privacy to the Internet. All kinds of online privacy infringement cases are coming, and China has not carried out special legislation on the right to network privacy. There is still a long way to go to improve China's legislation on the right to network privacy.

As a powerful country in network science and technology, when legislation on the protection of the right to network privacy, we should learn from the successful experience of Western countries in the protection of the right to network privacy, and then summarize the methods of civil law protection suitable for the right to network privacy in China according to the specific situation of China's network environment. When improving the civil law protection of the right to network privacy, we should adhere to the following two aspects at the same time. On the one hand, we should strengthen the legislative construction of network privacy protection to ensure the normal exercise of the right of network privacy by network users; on the other hand, to improve the public's awareness of network privacy protection. The improvement of the protection of online privacy and civil law is conducive to the construction of a perfect civil law system and the formation of a socialist country under the rule of law with Chinese characteristics.

References

[1] Yimeng Wang .Research on Legal Protection of Network Privacy [D]. Master's Thesis of Hebei Normal University, 2018.

[2] Chen Jiang .On Legislative Perfection of Civil Law Protection of Network Privacy [D]. Master's Thesis of Anhui University, 2020.

[3] Xiuwen Yu.Empirical Study on Legal Protection of Network Privacy [D], Master's Thesis of Nanchang University, 2018.

[4] Liyuan Zhang.Research on Privacy Infringement in the Network Environment [D], Master's Thesis of Heilongjiang University, 2019.

[5] Zhangzhang Hao. On the Confirmation and Protection of Network Privacy [D], Master's Thesis of Shanxi University of Finance and Economics, 2018.

[6] Yun Wang.On the Protection of Privacy in the Age of Big Data [D], Master's Thesis of Shandong University, 2019.

[7] Haijiao Yang. Research on Civil Law Protection of China's Internet Privacy [D]. Master's Thesis of Shanghai University, 2013.

[8] Yujie Li. On the Perfection of China's Civil Law Protection of Network Privacy [D]. Master's Thesis of Anhui University of Finance and Economics, 2018

[9] Hao Sun. Civil Protection of China's Internet Privacy in the Big Data Environment [D]. Master's Thesis of Anhui University, 2016

[10] Meng Wang. On Legal Protection of Network Privacy [D]. Master's Thesis of Heilongjiang University, 2017

[11] Jia Li. Research on Civil Law Protection of Network Privacy [D]. Master's Thesis of Dalian Ocean University, 2020