CSCanada
**Studies in Sociology of Science**
Vol. 4, No. 4, 2013, pp. 32-35
**DOI:**10.3968/j.sss.1923018420130404.2878

ISSN 1923-0176 [Print]
ISSN 1923-0184 [Online]
www.cscanada.net
www.cscanada.org

# Internet Privacy

ZUO Yujia[a],*; JIANG Xiaohang[a]

[a]School of Law, Changchun University of Science and Technology, Changchun, China.
*Corresponding author.

Received 19 September 2013; accepted 20 November 2013

## Abstract
With the rapid development of electronic technology, new changes have emerged in people's lifestyles. The development of the Internet, in particular, is changing people's lives subtly. The Internet provides us with common knowledge that we need but that we don't know. We can fully share resources on the Internet. This improves work efficiency and at the same time avoids the waste of resources. However, the Internet has its own characteristics. The Internet has three main features: openness, identity concealment and information timeliness. Once individual privacy is infringed, it is difficult for the victim to find the infringer or request compensation from the infringer. Can the latest judicial interpretation be applied to individual Internet privacy infringement? Can it lead to lasting solutions? How is the protection of Internet privacy regulated in foreign countries? I believe research on Internet privacy still has meaning and I will put forward my own humble opinions.

**Key words:** Privacy; Internet; Protection model

ZUO Yujia, JIANG Xiaohang (2013). Internet Privacy. *Studies in Sociology of Science, 4*(4), 32-35. Available from: URL: http://www.cscanada.net/index.php/sss/article/view/j.sss.1923018420130404.2878
DOI: http://dx.doi.org/10.3968/j.sss.1923018420130404.2878

## INTRODUCTION
According to authoritative statistics, to June 2013, the scale of China's Internet has become the first in the world. The number of Internet users has reached up to 591 million and the number of mobile Internet users has reached 464 million. If we count 1.6 billion as China's total population, about every 4 out of 10 people are using the Internet and every 3 out of 10 are using mobile Internet. It is on such a huge scale. If the society is simplified into families formed of 3 or 4 people, basically every family has Internet users. The Internet has become an indispensable part of our lives. The Internet has its advantages such as a huge amount of resources, fast delivery of global news and information, and convenient online shopping, etc. which benefit people in all aspects of life. However, the Internet is a double-edged sword. In order to maintain its timeliness, Internet service providers cannot check whether each user's behavior or remarks constitute privacy infringement or not. Or even the victims do not know the fact of infringement. This situation often occurs in cases of privacy violations. Recent social hot issues including Internet rumor infringement cases, the group event of city management workers beating a watermelon farmer to death, and the prism affair involving Snowden have one thing in common, the Internet's violation of citizen's privacy (i.e., a violation of Internet privacy).

## 1. INTERNET PRIVACY PROTECTION MODELS IN FOREIGN COUNTRIES
The occurrence of Internet infringement cases has become a common problem in all countries. Because of different local emphases on historical background and value protection, Internet privacy protection models vary. Some countries providing distinctive Internet privacy protection in law mainly include the European Union, the United States, South Korea and Japan.

The European Union is a typical country which uses legislation as the primary means to protect Internet privacy for its people. In order to make its people follow Internet privacy protection principles, the EU keeps enacting laws and regulations, and even, in order to complement this

implementation, it also enacts administrative regulations and judicial relief in particular. The EU as a whole, in order to improve efficiency and reduce hassles due to inconsistencies between the rules, makes a lot of common laws and regulations. Due to its own characteristics of virtual network, the EU member countries have reached a consensus foe this legislation. For example, in 1981, the council of Europe member states signed the "Personal Protection Convention of Automatic Processing of Personal Data". On October 24, 1995, EU member states passed "EU Personal Data Protection Direction". After that, the EU has successively promulgated a series of regulations, such as the "General Principles of Internet Privacy Protection" and so on.

The United States is a case law country. In protecting Internet privacy, it typically adopts industry self-regulation model. The industry self-regulation model can be divided into three kinds: the first one is to regulate the behavior of Internet service providers, Congress provides suggestions for Internet service providers by developing relevant laws and regulations, requires them to develop Internet privacy protection rules, and reviews the rules they have developed to achieve Internet privacy protection. The second one is to allow users to better identify the scope of others' personal information. Enterprises in compliance with Internet privacy protection standards can post a Internet privacy protection certification after authorized to make sure their users are under Internet privacy protection. The third one is to conduct technology protection in order to respect users' right to choose. The Internet community takes a large number of privacy platforms as a carrier, allowing individuals to decide which information can be made public and which cannot from the information presented by the carrier. Ultimately, users can decide to post information and adopt methods provided by Internet technology. This can prevent users from losing confidence in Internet security.

South Korea is so far the only country that enforces the use of a real-name system to protect Internet privacy. South Korea formally implemented this system in 2005. It is special because when Internet users conduct business (except browsing behavior) online they must confirm their basic resident information. This includes, for example, online posting, replies to other postings, or making comments on certain current events. "Basic Protection Law of Information and Communication" and other relevant regulations clearly define the scope of Internet privacy violations. The combination of the two has achieved the purpose of protecting Internet privacy.

South Korea's practice is similar to that of European Union's, but there are differences: EU law only polices behavior that has already occurred. They first develop laws. Once a violation occurs, the perpetrator is called to account afterwards, with an emphasis on a variety of laws cooperating with one another. South Korea is a pro-active law. It develops regulations before Internet users commit violations which give certain deterrence and make the perpetrator think before he acts.

Japan uses the developed protection principles to protect Internet privacy. Since the end of the 20th century, Japan Private Life Research Society has proposed to develop basic principles related to Internet privacy protection. The principles are divided into 5 aspects and they are collection, usage, storage, full public participation and division of responsibilities.

Japan's Internet privacy protection model falls somewhere between the self-regulatory model of the United States and the legal regulation model of the EU. Compared with the protection model of the United States, Japan's Internet service providers have the same free space to take actions as long as they are not against the principles. However, Japans protection model has differences. Japan's protection model is compulsory, meaning that violation is invalid. The industry self-regulation system in the United States is a recommendation or a contract between the users and providers. Violation of the nation's recommendations is not necessarily invalid. Comparing Japan's protection model with that of EU's, although Japan's basic principle model has a legal effect, it is primarily only a set of vague general principles and regulations, while the EU has developed specific regulations to handle violations of Internet privacy.

Every country places different emphasis on Internet privacy protection, but each of them has some drawbacks. The EU's legislative protection is prone to loopholes in the law when new violations occur because of the lag time between new forms of violation and the development of new laws and these results in legal but unreasonable results. The United States' industry self-regulation protection model relies on Internet service providers' cooperation with law enforcement. How can the Internet service providers' industry self-regulation protection be monitored? Relying on legislation to solve the problem, when legislation and industry self-regulation are in conflict with each other, which should have priority? Can South Korea's real-name system limit freedom of expression? How can we regulate those who fraudulently use another people's identities? Japan's principal protection is too general. Is it possible that the judge's discretion appears too large or cannot be used specifically?

There can be a defect or another in a system, but if it is migrated to our country, the most important factors that we should comprehensively measure are our national conditions, lifestyle, and national culture and so on.

## 2. CHINA'S INTERNET PRIVACY PROTECTION STATUS

At present, China has no clear legislation on Internet privacy protection, but Internet privacy belongs to

the extension of privacy; therefore we can appeal to traditional privacy protection regulations. The existing laws of privacy protection are too general and fragmental. The Constitution just makes general provisions on Internet privacy, stating that a citizen's personal dignity should not be violated, a citizen's residence is protected from unlawful infringement and privacy of correspondence is protected by law. Civil Law does not make clear statements on privacy protection. The Supreme Court has made expansive interpretations in relevant judicial interpretation of the protection of reputation, and takes the violation of privacy as a violation of the right to reputation. In judicial practice, this judicial interpretation has been followed to judge cases. Behaviors whether in written, oral or other forms of publicizing other people's privacy and causing certain impacts should be recognized as a violation of the citizen's right to reputation. In the field of criminal law, there is a separate chapter in the Criminal Law about citizens' civil and democratic rights, but there is no provision on invasion of privacy. Protection of privacy is scattered in a few single laws. For example, "Protection of Minors Law" stipulates that any organization or individual shall not disclose the personal privacy of minors. On Internet privacy protection relevant specialized laws and regulations, China's legislation appears weak and most of them are just general principle requirements. In the December of 1997, the Ministry of Public Security issued the *Computer Information Network and Internet Security Management Approach* and the spirit of this document is: any subject shall not use the Internet to endanger national security or leak state secrets, and is prohibited against violating the interests of the state, the society and the public or the legitimate rights of citizens, and is prohibited from engaging in illegal and criminal activities; any subject is not allowed to violate laws or regulations to use the Internet to violate users' freedom and privacy of correspondence. On December 13 1998, the State Council Informatization Leading Group issued the *Computer Information Network and Internet Management Interim Provisions Implementation Method* and the spirit of the Article 18 is: do not allow fraudulent use of another person's name on the Internet to send information such that it violates the privacy of others or distribute false information against the privacy of others. These legislative provisions constitute our Internet privacy protection system, but there are still some problems. Firstly, with the rapid breakthroughs in science and technology, new Internet privacy violations occur, such as deliberately fabricating information about others, or distributing false information to others while knowing the information is false or tampering with the original information of others and so on. So far there is no legal distinction on the Internet about what information a person is allowed to publicize, what information can be publicize without the person's permission, and what specific methods must be applied in the use of certain kinds of information or how such use should be authorized. Law cannot give a definite answer. In judicial practice related to Internet privacy violation, only traditional privacy protection regulations can be applied to. Secondly, when Internet privacy violations occur, because of the characteristics of such violations such as their ubiquity, the speed with which they happen, and difficulty of redacting statements, etc., still only the Supreme invasion of privacy provisions on violations of the right of reputation can be referred to. Such protection is probably inappropriate.

On September 10 2013, The Supreme Court and the Supreme Procuratorate issued *An Interpretation in Applicable Law on A Number of Issues on Handing Criminal Cases by Using Confidence Internet to Conduct Defamation* (hereinafter referred to as judicial interpretation) which makes protections of Internet privacy from the perspective of criminal law.

It is divided into three levels and they are: the aspect of libel, the aspect of disturbing the peace and the aspect of extortion and illegal business.

First, the spirit of Article 1 Section 1 of the judicial interpretation is: knowingly and deliberately fabricating facts that may damage other people's reputations and distributing them on the Internet, causing serious effects; or fabricating facts which may harm the reputations of others and spreading or organizing them by using the Internet as a carrier; or instructing others to spread or tamper with original information to a violation of laws protecting personal reputation. One of the above three behaviors can be completely identified as a libel. Thus, one of the three behaviors violates other people's Internet privacy by damaging their reputation and now people's Internet privacy is under criminal law's protection. However, if the violation level does not reach the extent of the judicial interpretation, should this behavior be punished? Should it be identified as libel? Should they take civil liability for compensation or administrative responsibility for punishment? There is no specific provision in the judicial interpretation.

Second, the spirit of Article 5 Section 2 of the judicial interpretation is: spreading purposely or knowingly rumors or false information on the Internet, or organizing, instructing others to spread rumors or false information as to create a disturbance, causing serious public disorder, should be condemned as disturbing the peace and be punished. If the fabricated information infringes the privacy of others and some criminals deliberately create public disturbances by this means, it can constitute a crime as long as it reaches the degree of disturbing public order.

Third, Article 6 and 7 of the judicial interpretation states, using ways to delete postings or post information for threats or profits, that reaching a certain level, will constitute a crime. I will not repeat this again here.

The judicial interpretation remedies the legal consequences of new Internet privacy violations, but there are still shortcomings. Internet privacy protection

is essential for the life of each person and no person shall have the right to violate it. It is indispensable for each person to live with dignity, freedom, and choice. Even if some violations do not reach a criminal level, they still should fall under the provision of the law. I hope legislators can introduce relevant policies to implement privacy protection from a civil perspective in the near future, and refine its scope to fully protect people's privacy.

## REFERENCES

Liu, D. T. (2011). On China's construction of Internet privacy protection system. *Legal Space*, (01). (In Chinese).

Liu, M. D. (2007). Special factors in the jurisdiction of online infringement cases. *Law*, (04). (In Chinese).

Sun, S. S., & Luo, C. X. (2006). Civil protection of personal information. *The Journal of Beijing University of Posts and Telecommunications (Social Sciences Version)*. (04). (In Chinese).

Wang, W. H., & Zhang, G. (2000). The deceased's post right and privacy's conflict and its protection. *The Journal of Shandong Institute of Business*, (05). (In Chinese).

Xu, J. H. (2008). The United States' Internet privacy's industry self-regulation's enlightenment to China. *Intelligence Theory and Practice*, *32*(06). (In Chinese).

Zhao, L. N. (2009). On China's legal protection to Internet privacy. *Legal Forum*, (01). (In Chinese).