
Research on personal information security in the era of big data

Zhi Liping^{1*}, Zheng Jiaxue²

School of Computer and Information Engineering, Anyang Normal University, Anyang, China

ABSTRACT

With the rapid development of the data era and the widespread application of cloud computing, information systems and other technologies, the amount of data increases exponentially. The wide application of data mining technology in personal information storage, digital analysis and information sharing brings convenience, but also poses severe challenges to personal privacy protection, trade secrets, national data security and other information. According to people's strong dependence on science and technology and the status quo of compulsory claims of each software platform, this paper focuses on the analysis of the problems facing personal information at present, as well as the factors that threaten information security, and puts forward relevant suggestions and measures for these problems and factors.

KEYWORDS

big data; data mining;
Information disclosure;
Information security

CORRESPONDING AUTHOR*

Zhi Liping

(1) INTRODUCTION

(1.1) Research Background

With the advantages of high efficiency, convenience and diverse choices, "Clothes and meals" has adapted to the fast pace of modern life and become a new life mode, which has been accepted and recognized by the public. "Clothes and Hands" -- an online shopping platform enables people to shop at home, experience the convenient service of door-to-door delivery, and satisfy their life while surfing. The surge of take-out users has promoted the rapid development of take-out industry and made users' daily life more convenient.

The convenience of the digital era, the rapid updating and iteration of science and technology, the highly open network space, the increase of Internet users, more and more people through the Internet to facilitate their life, enjoy the convenient services brought by the Internet. In China, the income of software and information technology service industry is increasing year by year in the process of social development. The vigorous development of software industry and information technology service industry has also sounded the alarm bell for the protection of our information security.

In this new mode of life, new problems arise. The development of data collection tools aggravates the situation of "no privacy at all in the Internet era". Everything has its advantages and disadvantages, and the coexistence of problems and convenience has raised requirements on how individuals, social enterprises and the state can solve this problem.

(1.2) Research Status

• Foreign research status

Personal information security is also known as personal privacy security in foreign countries. Western people have high-security awareness, which is related to their pursuit of individual rights. They call for human rights and pursue freedom. In terms of legislation, Germany is the first country in the world to pass the Privacy Protection Law, and its punishment for privacy disclosure is relatively strict. It will impose a high fine on enterprises that disclose users' information without their permission. America passed the Privacy Act in 1974; Japan is ahead of China in the implementation of personal information protection. In 1970, Japan implemented the protection of personal information, and then continued to improve the protection.

- **Domestic research status**

Since the era of big data, the continuous occurrence of personal information infringement events, so that the issue of personal information caused a hot social debate. Especially after the occurrence of "Xu Yuyu case", after the fermentation of network public opinion information, personal information security has become a key problem to be solved in the society.

To assess the public's awareness of information protection, the Center for The Rule of Law on the Internet and the Cover Think Tank jointly launched The Is Your Privacy Compromised? The number of questionnaires collected amounted to 1.04 million. According to the results of the questionnaire survey analysis, the problems faced by national information security for individuals has caused the attaches great importance to, but due to the lack of common sense and experience of how to protect information, then criminals against infringement of citizen's information still happen, but most of the information security threat for the vulnerable groups, inadequate maintenance of individual rights consciousness and ability is limited, After the information is violated can only choose to endure, so the protection of personal information security is still a top priority for the people.

In terms of legislation, China's earliest relatively complete information law started in the 1980s, but this law is mainly based on intellectual property rights, state secrets, network management and network security. The regulations based on personal information protection will be introduced on November 1, 2021, which is the official implementation of the Personal Information Protection Law. The introduction of this policy, to a certain extent, to ensure our information security.

(1.3) Research Significance

Part from the point of the present situation, the national consciousness of the protection of personal information as the strengthening of anti cheat strength has improved, for another part to integrate with The Times, not good for the people, the protection consciousness is still very weak, aware of the importance of personal information to yourself, don't know the personal information leak will bring what kind of impact to themselves or people around.

Based on existing facts, this paper summarizes the since into the digital era, information security problems caused by the individual events, and according to these problems, puts forward some advice to prevent similar events happening again, the purpose is to call for national consciousness to strengthen the protection of personal information, to realize the importance of personal information safety. At the same time, it is also hoped that the relevant departments of the state can pay attention to the protection of national information security, and there is a long way to go to crack down on information crimes.

(2) PROBLEMS OF INFORMATION SECURITY

(2.1) Information Disclosure

- **Research on information leakage**

According to official statistics, 78.2 percent of residents' information, including their names, residence, id numbers and mobile phone numbers, was leaked. It can be seen that our residents' awareness of security protection needs to be strengthened. Numerous information leaks caused by financial fraud, information bombing, telephone bombing, and the resulting loss of economic or time costs are enough to deepen our awareness of information security protection. Our dependence on technology increases the risk that our personal information will be illegally collected, sold and used. As shown in Figure 1 below, breaches have become more prominent, reaching 5,183 in 2019. According to publicly available information, about 1.127 billion personal information had been leaked by 2020. Among the information leaks in recent years, the number of information leaks in 2019 reached 7.995 billion pieces (as shown in Figure 2 below), which triggered endless thinking. If the national awareness of personal information security was improved, information leaks would not occur frequently and there would not be so much information leaked.

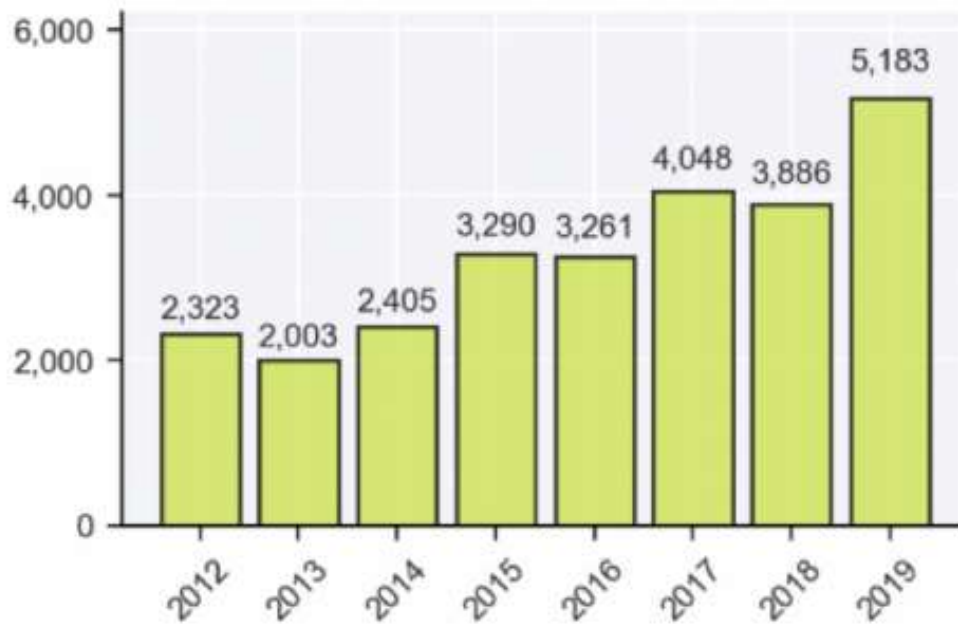


FIGURE 1: Statistics of data breach cases disclosed globally 2012 - 2019

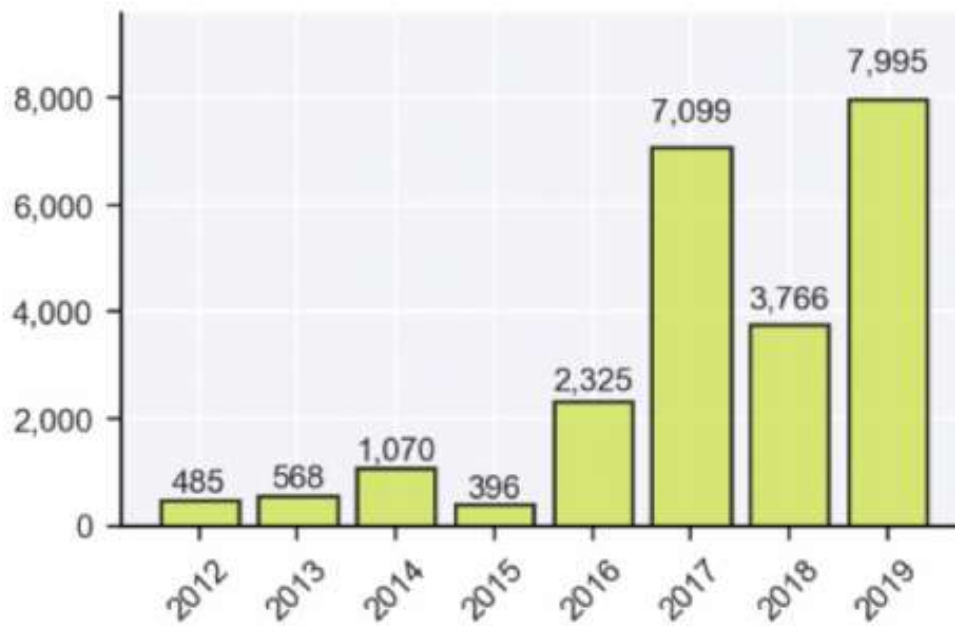


FIGURE 2: Data volume of information leakage 2012 - 2019 (unit: millions)

- **Main ways of information disclosure**

(1) Leakage of express bill

The rapid development of online shopping platforms has opened the market of express delivery industry, as shown in Figure 3 below, which shows the development of express delivery industry in China from 2015 to 2020, and the volume of express delivery business in China in 2020 is up to 83.36 billion pieces.

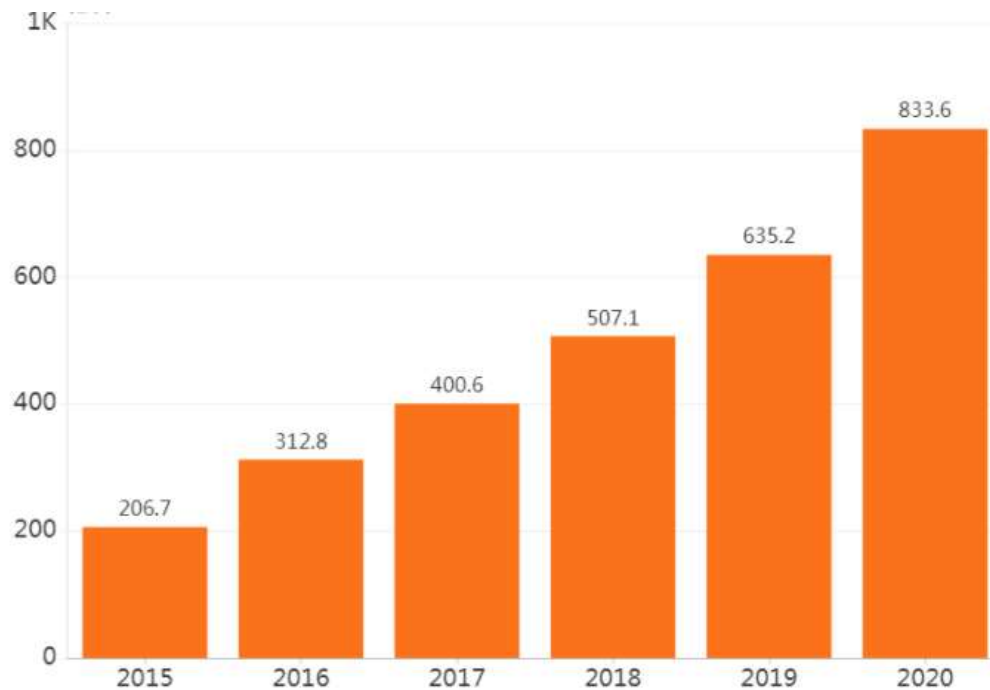


FIGURE 3: China's express Business volume 2015-2020

People enjoy the joy of unpacking the express but ignore the processing of the express bill. The most common way to dispose of packages or boxes is to throw them into the trash can, and pay no attention to the personal information on the packages. As a result, in recent years, the disclosure of personal information by the Courier has become common news. An investigation by a journalist reportedly found that some express delivery orders containing users' names, contact information, shipping addresses and other private information were being sold in batches with marked prices.

Based on the timeliness of the express receipt, the criminals divide it into "historical" and "real-time". On this basis, they further refine the classification, such as judging the user's gender and consumption level according to the type of product purchased by the user, so as to achieve the purpose of precise selling of user information. Purposeful and planned sales in accordance with this standard constitute a set of industry "rules". When fraudsters get personal information, they often contact users with the identity of the "business", and there are not a few cases of fraud caused by this.

(2) APP software leakage

In this Internet age, our personal data are viewed by various apps. Some software, we need to open a variety of permissions, including: address book, read mobile phone storage, read information, read geographical location, read photo albums and so on, without authorization, can not normally use the software, personal data has become an important asset for the strategic development of enterprises. However, not all enterprises can stick to the bottom line of morality, forced access, secretly stealing user behavior information, simple account registration difficulties and other problems emerge one after another, which not only seriously threaten the interests of users, affect the healthy development of society, and even threaten the national security.

Until the first half of 2021, Didi Chuxing was a ride-hailing app with both reputation and safety. The next day after its launch in the US, Didi Chuxing was censored by the Cyberspace Administration of China, and was forced to be removed from the market after reports emerged that it had seriously violated laws and regulations in collecting user information. There are also some programs that maliciously read user privacy information, such as: WeChat's WeChat powder application privacy profit of 8 million yuan, in the program development, have made clear to steal user information function, illegally obtained information, the data will be uploaded to a "transit site", as long as become a VIP of the site, you can use the site's information mass brush "single" "thumb up" service. Such incidents are not rare, and the state has therefore intensified the management of major software, requiring that no software can have excessive collection of user information.

(2.2) Software Monitoring

With the rapid development of the digital wave and the continuous integration of big data and real economy, we may encounter the following situations: just ordering takeout, we will receive a drink push; After chatting with friends about something, the next second you turn on your mobile phone and major browsing software pushes relevant content. After searching for a product on the Web, the shopping website will recommend it to us. It's as if our lives are being "watched" by apps.

Many apps mine user value and define and categorize users by surreptitiously collecting information about our location, shopping habits, mobile web browsing, reading preferences and more. In the age of big data, our mobile apps may know us better than we do: shopping platforms recommend our favorite styles; Online social platforms are pushing our favorite videos or articles; Video entertainment software push is like watching TV...

Data mining technology has given full play to its role in obtaining valuable information, understood the habits of users, mastered the preferences of users, and successfully expanded the user group. But it also brings some new problems, such as big data killing -- the same software, the same goods, different prices for different users, platform companies try to maximize their own profits. If we don't pay attention when shopping, we may become one of the targets of big data.

(2.3) Monitoring Vulnerability

Monitoring products are widely used in roads, offices, shopping malls and families, etc., the original intention is to facilitate management, convenient life. But with the diversification of monitoring products, their quality is uneven, and even some monitoring products can not be guaranteed safety performance. Some people cracked all kinds of cameras or surveillance video according to the vulnerability of its product security performance, and published its cracked methods as a tutorial on the Internet, more lawbreakers openly sell stolen video or audio. Monitoring information security involves many levels, such as the security performance of the device itself, the security of the monitoring platform and the security of the monitoring content in the process of synchronization. Any level of attack may lead to our personal information being exposed to the public.

(2.4) Rampant "rogue software"

"Rogue software" for lawbreakers, its role is to constantly pop up advertising information, and benefits from its binding software development enterprises and promotion costs. It fully grasped the user's dependence on the installation of the guidance of the psychology, through unclear prompts, bundled software installed on the user client, so as to infringe the legitimate rights and interests of users.

A kind of rogue software appears on the computer, showing as forced installation, difficult to completely uninstall and spread spam, malicious binding of other software installation and so on; Another kind of rogue software appears on mobile apps, such as forcibly demanding permissions, illegally selling user information, and killing users with big data. According to relevant statistics, in the first half of 2019, more than 1,000 software were forced off the shelves, all due to excessive collection of user information and forced user authorization.

(3) INFORMATION SECURITY PROTECTION MEASURES

(3.1) Improve the awareness of information security protection

Improve the national awareness of personal information security protection is not achieved overnight, the society should actively take measures to strengthen anti-fraud efforts, create an environment conducive to improving the awareness of information security protection, information security will be rooted in the hearts of the people, from the root to protect personal information.

- **Properly handle information**

Develop good behavior and proper handling of personal information. In daily life, Courier orders, bank access vouchers, take-out orders and other small receipts containing our identity information should be properly disposed of, leaving no room for those who collect bills to obtain personal information.

- **Develop good Internet habits**

There are often free WiFi in public places, so try not to connect. Although some are set up by businesses for the convenience of customers, it is inevitable that some criminals will also set up some phishing WiFi. Once we connect to the WiFi, our device information and file security may not be guaranteed, or be illegally used.

Try not to leave personal information on the website and contact information, the Internet era of corporate earnings have been associated with the user information, the user data volume, the more the more help to corporate earnings, so some sites will want to leave the user's personal information as much as possible, especially some profitable website, after the users personal information, Enterprises will contact users to marketing, to achieve the purpose of profit.

(3.2) Strictly control "rogue" software

Should as far as possible when downloading software from the official sources, most are "rogue software" is derived from advertising site, the site's software contain bundled software, in the process of our installation, slightly do not pay attention to some useless get we installed the computer software, this software will be timing pop-up ads or contain Trojan virus, even if we didn't use the software, But it doesn't prevent our data from being stolen.

The country should strengthen the management of each big software, prevent "rogue software" to run amuck in social life. In the 30th session of the 13th session of National People's Congress standing committee, the software for excessive collect user information, "big data kill cooked" behavior such as a clear stipulation, for a serious breach of regulations, will place below 50 million or 5% penalty in accordance with the previous year turnover, this is after the law, the second law of administrative punishment in turnover percentage. The policy partly cracks down on software that collects excessive user information, slams e-commerce platforms for discriminating against users, and shows how seriously China attaches importance to personal information.

(3.3) Increase penalties for information disclosure

There are financial fraud, spam SMS bombing, advertising telephone harassment and other events, warning us of the urgency of personal information security protection, but also requires us to start from the little things, from the source to protect our information is not illegal elements to obtain; On the other hand, it is also necessary for the state to increase the punishment for those who leak information and continue to improve the Tort Liability Law. When the punishment is far greater than the benefits brought by the crime, there will be no profit and no one will take risks, thus reducing the frequency of information leakage events.

(3.4) Improving network management

In today's era, the protection of personal information security not only depends on providing residents with protection awareness, but also needs to improve the level of system management. Trojan incursion leads to information outflow, hacker attacks computer system intentionally leads to computer security system paralysis and other problems are not an individual case, which requires us to constantly strengthen prevention technology, so that Trojan virus can be invaded nowhere, hackers can attack nowhere, so as to protect personal information security.

(3.5) Continue to improve laws and regulations

To some extent, laws and regulations restrain and regulate illegal behaviors. The ever-changing information age, personal information security problem and the rights of contradictions increasingly prominent, in order to solve this problem, our country officially introduced in November 2021 the personal information protection act, the law is the first dedicated to personal information protection in China at the head of the law, the implementation of the policy means that our information protected by the policy.

Information security issues are complex and changeable, and only by constantly supplementing and improving laws and regulations can we truly protect personal information security from infringement from the root.

(4) CONCLUSION

With the comprehensive development of informatization, information security has become a national issue, which is related to national interests, social stability and national security, and its importance is self-evident. The country should strictly control market behaviors, improve the public's awareness of protection, constantly improve laws and regulations, and create a secure network environment to further promote the development of the era of data and add more bricks to the convenient life.

REFERENCE

- [1] Dong Hao. Poll: About 64% Americans worry about personal information security [N]. China Daily,2021-09-17.
- [2] Xu Fu, Yu Tao, Zhu Liming. Protection and perfection of personal information -- analysis from xu yuyu case [J]. Journal of huaibei vocational and technical college,2019,18(01):72-74+82.
- [3] China Youth Daily. The grim situation of personal information security and privacy protection. https://www.edu.cn/info/ji_shu_ju_le_bu/wlaq/201611/t20161129_1471361.shtml.2021.11.19
- [4] Liu Y. Discussion on information security in the era of big data [J]. Journal of Information Record Materials, 201,22(10):68-69. (in Chinese)
- [5] Zhang S N. Research on Personal information protection of Online Consumers in China in the era of big data [D]. Dalian University of Technology,2021.
- [6] Ning Hua, WANG Yanhong, Wang Yuxiao. Current situation and countermeasures of APP personal information security [J]. Quality and Certification,2020(04):33-35.
- [7] Liu Dandan. Consumer Rights Protection under Network Precision Marketing [D]. Southeast University,2020.
- [8] HAO Dongmei. Malware Governance must prevent resurgence [N]. China Business Daily,2019-08-20(P02).
- [9] Pu Yeqing, Zhang Baowen. Iso27001-oriented Ontology modeling and its application: A case study of enterprise malware protection [J]. Communications technology,2017,50(02):307-314.