Personal Information Security in the Era of Big Data

YE SUN

ABSTRACT

The advent of the era of digital information, vast amounts of data is gradually affect people's way of life, work and study habits, etc., bring convenience to people at the same time, also make people face a lot of information security threats and challenges, so the information security problems faced by big data era is of great significance. This paper first analyzes the current big data era background, on the basis of the key problems of personal information security, analysis of information security risks at the same time, put forward the issue of information security strategy.

KEYWORDS
Big data, personal privacy, information security.

INTRODUCTION

The advent of the big data era has digitized paper documents that were previously not easy to carry, store and share. The Internet has become a necessary tool for modern people to process data, communicate and work. Such as WeChat, drops, taobao and alipay APP, brings people a convenient way of life, but people on the Internet behavior will be recorded by system, including personal basic information, purchase records, daily habits and so on. For businesses, the data can be used to tap into the needs of users, so as to improve the corresponding products and services and achieve accurate marketing, thus generating more economic benefits. But at the same time, these data also reveal personal privacy, and personal information security is very risky. Once unscrupulous people dig into this information and use it for online fraud, it will bring great disruption and even significant economic loss to our lives.

Ye Sun, 13488381492@163.com, Shaanxi Guohua Jinjie Industrial Park Shaanxi Guohua Jinjie Energy Co., LTD. Maintenance Department, Shaanxi, 719319, China
ANALYSIS OF THE STATUS QUO OF PERSONAL INFORMATION SECURITY IN THE BACKGROUND OF BIG DATA

In the age of high-speed information, people use new tools, new models and new systems to excavate a wide variety of data to obtain new value information. When big data merged with traditional industries, new businesses and new business models were born, and in the process, personal information was applied. But there have been frequent breaches of personal privacy at home and abroad, such as the fact that the hacking attack on Anthem, America's second-largest health insurer, has affected 80 million user data. The domestic 360 browser infringes on user privacy and so on, which seriously infringes the client's privacy and damages the legitimate rights and interests of the client. So how to protect individual privacy becomes the question that every citizen or even whole society thinks seriously.

Personal information is ubiquitous, and data processing and mining threaten privacy

In business, personal information can be accurately recorded and stored. For example, the name, time and place of the goods purchased by the consumer will be preserved. In the medical field, personalized treatment can be achieved through the recording of personal information. In the social field, with the increase of social software, people's social needs are greatly enriched. At home, the most representative is the WeChat tencent launched in 2011, the user in the process of using WeChat, personal information will be keep records, such as Location Based services (Location-based Service, LBS), can make a circle of friends of friends know exactly how the user released the information in any position.

Now a lot of information analysis tools, people's identity information, web surfing traces and geography information collection, storage, conversion, after induction, statistic analysis, make the system data to confirm and explain each other, each other between various database will also arises at the historic moment. To a certain extent, privacy is no longer private.

Data storage is no longer suitable for big data environment, and the risk of data leakage is increasing

In the context of big data application, data types and data sources are diversified, and a large number of structured and unstructured data are continuously generated, and many storage systems cannot meet the requirements of big data applications. At present, most privacy protection technologies and algorithms are aimed at traditional relational data and cannot be transplanted directly into big data applications.

Data resource disclosure, sharing and privacy protection are contradictory

In the age of big data, information disclosure and sharing are beneficial to business development and government administration. Because personal information can bring commercial value, it stimulates illegal merchants and personnel, illegally acquires and USES personal information to gain profit for business opportunities. In addition, some governments have demanded access to personal privacy in order to safeguard national...
cyber security and security, thus making national security and personal privacy at odds.

PERSONAL INFORMATION SECURITY ISSUES AND PRIVACY LEAKS

With the emergence of new Internet technologies, due to the users in the use of the registered account in the process of personal information is recorded, so the user experience and enjoy the convenient way at the same time, also feel system all the time in the "monitoring" of his own actions. According to China Internet network information center, the number of Internet users in China reached 731 million by the end of 2016, up by 0.43 billion from 688 million in 2015. Along with the further promotion and application of the Internet, personal information will be recorded and stored by the various systems and platforms, which to a certain extent, improve the chances of the personal information was leaked, personal information security has become an important social problem. Further analysis of factors threatening personal information security will be discussed below.

Inadequate protection of Internet data due to technical backwardness

In the big data environment, people will have multiple accounts in order to experience various tools and platforms.

The application will be required to bind to the mailbox or phone number. In this way, a mailbox or phone number will be associated with multiple accounts of the user. Sometimes various tools or platforms can be used to facilitate user operation, and they can also enhance cooperation and access multiple applications or platforms through an account. However, some websites cannot effectively protect users' data because of their poor technical ability. Some hackers take advantage of an Internet company's database to get information about companies or individuals. For example, 12306 user data breaches are due to poor data protection.

The commercialization of personal information and the loss of control of personal information by users

Data in the context of big data is highly correlated, and the in-depth analysis of data can expose certain privacy information of individuals. For example, personal data in e-commerce not only have value but also become a commodity. Some lawless merchants may be able to sort through the collected personal information, and then search the Internet for customers who specialize in personal information, and sell the information at a high price. Although users can protect their data through cryptography, that is to say, users' personal information security is guaranteed. However, in the context of big data, some businesses are both producers of data and managers and users of data. Therefore, it is very difficult to make the user's personal information absolutely safe.
Personal protection

Many Internet users in order to obtain some merchant's interests, when registered membership will give their name, phone number, occupation, family address and even personal information such as credit CARDS information to fill in, there is no ego to protect consciousness. The results are likely to be exploited by criminals, and the cases of fraud are common. In addition, more and more people are using social software nowadays, in the process of social software release mood, interactive communication, will inadvertently reveal personal information, such as geographical location as well as the schedule, if you do not set access permissions, so this information will be an open secret.

The means by which criminals steal privacy are diversified

In March 2017, the ministry of public security under the unified command, Beijing, anhui and other 14 provinces, municipalities directly under the central government to the public security organ abort a use of stealing all personal registration information from the Internet, copy, bank CARDS, implementation for unauthorized card of illegal and criminal gangs. The public security organs seized more than 5 billion personal information from the computer of a major criminal, involving all kinds of personal information such as banking, transportation, logistics, medical care, social and other citizens. The illegal activities such as stealing citizens' personal identity and other information are mainly illegal.

THE TROJAN VIRUS IS USED TO STEAL INFORMATION IN THE QR CODE

The qr code is widely used in various applications because of its simple and unique characteristics of identifying objects. Especially in today's mobile phone payments, in most cases, users will be able to use a mobile scan to pay for a paypal or WeChat qr code. But many people use mobile phones to scan the unknown qr code images for the sake of illegal benefits. When a user literally scan to identify a qr code, could open a Trojan program, or a phishing site, mobile phone will be invaded by virus, access to personal information will be virus, then uploaded even sent directly to the criminals of the server. Because of the simplicity of the way of making and publishing the qr code, no organization or individual will check it, and the qr code can easily be disguised, making it easy for users to be cheated.

USE THE "COLLISION LIBRARY" TO STEAL PERSONAL IDENTITY INFORMATION

Criminals use personal data such as usernames, passwords, email addresses and mobile phone Numbers that are stolen online to build huge databases. Because many users in different sites use the same account and password, criminals use at a particular site to steal user account and password to "bump library" attack user account in another web site, for illegal activities.
USE THE SOFTWARE'S "CHECK-IN" FUNCTION LOCATION

Many of the intelligent mobile phone software has "check-in" function, users can share their status anytime and anywhere through the function, and with his location at that time, of course, the realization of the function of this must rely on the mobile phone GPS to open. Once the mobile positioning function is enabled, the user's location information will be obtained. In social software like WeChat, this feature becomes an essential part of the user. However, the risks that exist behind such functions are often ignored by users, and some users are not even aware of such risks. It is not known that the seemingly unimportant location information may be exploited by lawbreakers and engaged in illegal activities.

STEAL INFORMATION THROUGH "AUTHORIZATION REQUEST"

When installing some software in mobile phone or using some software for the first time, you will see is similar to "read the mobile phone address book" and other mobile phone authorization request, many users don't understand the deep meaning of this kind of request, generally choose allow option. In fact, when the user confirmed the permission, the information on the phone was captured by the server and uploaded to the cloud computing technology. There are many different user profiles stored in the cloud, and some of the software automatically alerts you to add a friend function based on this principle. In the cloud computing environment, the data acquisition, processing and upload speed quickly, the user's data will quickly complete the match, and quickly find out the user's mutual friends and other information. Although, this kind of friends add to remind may not exist too much risk, we should be aware, however, users of personal data in their unwitting circumstance are uploaded to the cloud, the cloud is easy to be criminals access to information resource, users frequently harassed and even fraud.

In an age of information that is widely used in cloud computing, information seems to be becoming more and more vulnerable to leaks and eavesdropping, and it is difficult to work simply by shielding software or by users themselves.

ANALYSIS OF INFORMATION PROTECTION MEASURES

Considering the characteristics of the big data era and the way of privacy disclosure, we need to consider various factors to find a more reasonable and effective solution.

Strengthen the unified legislation of personal privacy protection

At present, from the point of view of information security related laws and regulations, our country has issued some corresponding rules and regulations, such as in February 2013 on the implementation of the public information security technology and commercial service information system of personal information protection guide, makes the personal information protection in China formally entered the stage of "standard can depend on", its salient features are provisions before sensitive personal information collection and utilization, must first obtain personal information subject
specific authorization. However, in the process of implementation, due to the low level of effectiveness and too small punishment, it can not really protect the personal information security. Therefore, it should be aimed at the personal information security legislation of big data environment, standardize the code of conduct of relevant business opportunities and interest platforms, and improve the crime cost of personal information disclosure. Should fully consider China's national conditions, give full consideration to the inherent law and Internet privacy infringement cases investigation, prosecution and forensics objective of the problem, increase the punishment of violation of privacy act and the crackdown, provide standards and punish the behavior of the invasion of privacy law, perfecting the personal privacy protection laws and regulations of our country.

Encourage the development and innovation of privacy technologies

The state should actively encourage the development and innovation of privacy protection technology, and ensure the privacy security from the technical level. In traditional under the network environment, general technical means such as data encryption, is adopted to realize the security of information, at the same time, through the security vulnerabilities mend, tamper-proof and other means to protect sensitive and important data. However, under the big data environment, these technologies have some limitations, which cannot achieve broader and deeper protection.

In the big data environment, it is necessary to establish security model for cloud, tube and end, and to be aware of personal information security protection. According to the characteristics of huge amounts of data, for example, set up for the verification of the information "symbolic" means, through the symbolic mark user identity information, effectively avoid the big data under the background of cross check the data content, improved the security of the personal information on the technology. In addition, there are other technologies: data publishing, anonymous protection technology, social network anonymity protection technology, data watermarking technology and data traceability technology, etc.

Strengthen the publicity education of personal information protection and improve the awareness of personal information security

Although Internet users pay more and more attention to the protection of privacy, but due to their excessive dependence on the web makes many people believe that the behavior of the website collect personal information will not cause important influence to their privacy, personal privacy protection consciousness waned. Therefore, it is a compulsory course for netizens to learn how to better protect personal information security. Countries should strengthen the network information safety publicity and guidance work, such as through a variety of media to publicize the importance of protecting your personal information in accordance with the law, network and set up to prevent personal information be illegal collection, transmission, such as ideology, enables everybody to understand the scope of the personal information protection, improve the safety of people skills, enhance the consciousness of personal information security protection. For example, you can't upload private pictures of individuals, and you can't log into a bank account at will, and don't start the smart terminal location. In addition, it is important to provide security measures, such as removing Cookies,
enhancing password security Settings, scanning and fixing system vulnerabilities, etc., after using an application.

Establish a sales license mechanism for public data and conduct legal business of open data

In the era of big data, personal information data has become an important resource, providing evidence support for government decision-making, social management, enterprise development strategy formulation and scientific research activities. Some foreign companies have begun experimenting with data deals, such as the launch of data supermarkets in America's Factual company. Fujitsu has set up a data exchange market; Jack ma, a domestic entrepreneur, also made a point of selling data. In the face of the growing demand for data sharing, data disclosure, sharing and privacy protection must be coordinated. That is to sell data in a reasonable and legal way, regulate the personal data trading market and prevent privacy leakage. At the same time, the government restricts data sales enterprises to carry out personal data sales by issuing licenses. While regulating their own behaviors, enterprises supervise their competitors.

CONCLUSION

The advent of the era of big data has greatly promoted the development of the society, but at the same time, the cause of information security problem has been a very anxious, so we urgently need a new mechanism to protect personal privacy. The protection of the personal information security need to be done in many ways, with maximum limit to reduce the risk of personal information leakage, to better protect the security of the Internet information, promote the economic development of our country.

REFERENCES