Research on Personal Information Security Guarantee Based on Social Network in Big Data Era

Congman Zhang

Department of Sociological Studies, the University of Sheffield, Sheffield, United Kingdom

Keywords: Big Data Age, Social Networks, Information Security

Abstract: In the context of big data, this paper analyzes the new characteristics of social networks in the era of big data and points out that personal information security faces problems such as account theft, privacy intrusion, and loss of personal information control. Moreover, we propose countermeasures in terms of laws and regulations, industry self-regulation, security technology and personal security literacy to ensure personal information security in social networks in the era of big data.

With the development of technology, the amount of data generated and captured by modern society is growing rapidly, and the amount of statistical data is increasing by petabytes (1024TB), indicating that we have entered the era of big data. With the rise of social networks, more and more people are willing to share their experiences in this interactive era, and every action we take online through computers, cell phones and other electronic devices is recorded by servers. In the era of big data, personal information in social networks has become a major focus of the game between businesses. While exploiting the potential value of personal information in social networks, we urgently need to solve new problems in the era of big data, such as how to ensure the security of personal information, how to ensure that personal information is not illegally collected and improperly used, and how to improve the user's control over personal information.

1. Big data-based social networks

1.1 The era of big data.

To put it simply, big data is data of huge size and complexity that can be efficiently processed by standard database technology. To be called big, data needs to have three key attributes, namely, large scale, high efficiency and diversity. Large scale refers to the size of the data. People are generating a lot of data on their cell phones and computers all the time. Today, Facebook has more than 1 billion registered users, uploading more than 1 billion photos per month and generating more than 300 TB of log data every day. High efficiency means that the data is particularly time-sensitive and needs to be stored and processed quickly. The system will change the online advertising strategy in real time according to the current needs of each user, and the user also wants to extract information from the network at a faster rate. Diversity refers to the variety of forms of data expression, including text-based structured data, as well as other forms of unstructured data such as images, audio and video. Most of the data in social networks are unstructured.

1.2 Social networks in the era of big data

The booming of big data brings opportunities and challenges to social networks, and in turn, social networks present new features in the era of big data.

First, unstructured information on social networks is increasing. Tencent's WeChat application, launched in January 2011, has exceeded 300 million registered users as of January 2013, and its features such as voice chat and picture sharing have gained great popularity among users. Papa, a social application that lets photos speak, uses audio to introduce the stories behind the photos, and the appeal of sound has attracted many users. In addition, other social networks have also added the function of voice and video communication. Unstructured information such as audio and video

provides users with a new interactive experience. But on the other hand, it also reveals more personal information on social networks. The ease of reproduction of digital information also makes individuals less able to control their own information.

Secondly, mobile geolocation information applications are becoming popular. Since 2010, social networks in China have entered the era of "CheckIn", and users can add geolocation information when writing microblogs and posting photos. Moreover, mobile applications that rely on instant geolocation information to make friends are becoming a fashion in China. Therefore, geolocation information has become an important part of personal information resources in social networks nowadays. Although geolocation information gives users a more realistic user experience on social networks, a large amount of information is exposed to the public, which poses a threat to the security of users' information.

In addition, the increased interconnectivity of resources is another major feature of the era of big data social networks that is changing. Friends can access information on other social applications that users are bound to, and users can link information from other sites to the social networking applications that they frequently visit. Users on MOMO can access their friends' information bound to their accounts on Sina Weibo, Tencent Weibo and Renren platforms, while users on Papa can link their updated information to their personal Sina Weibo accounts. WeChat Moments supports information linked from other mobile social networks such as Qzone and Tencent Blog. Data interconnection is an inevitable choice for social networks operators to respond to users' higher communication needs in the era of big data. However, it also provides a convenient way for people with ulterior motives to mine users' personal information system, which leads to the worry of personal information security.

2. The problems of personal information security in social networks

At the core of big data is prediction 16. Social networks operators can only be invincible in the competition of big data by mastering massive data, analyzing users and products through scientific software, predicting market trends, and uncovering products and services with great value. However, the double-edged sword of Big Data facilitates the social interaction of users and predictive analysis of businesses, and at the same time, personal information security is facing unprecedented threats and challenges in the new era and new situation.

1) The risk of account theft has increased. User account security is the basic requirement for social networks. Compared with the traditional Internet environment, people have more social networks accounts in the era of big data. People usually use the same email address or cell phone number to apply for authentication services among multiple communities for the sake of memorization. In order to facilitate users' operations, network operators are also cooperating with each other, so that users can use one social networking account to log in to multiple websites to enjoy related membership services. In the era of big data, data is highly correlated, and theft of one user's social account may lead to the security of his or her accounts on other sites. As an important asset for merchants, account information is also a coveted target for criminals. Therefore, account security is even more critical in the era of big data.

2) Privacy security is a concern. Privacy security is the biggest threat to personal information security in the era of big data, and the biggest obstacle to the development of big data. People post their moods, share photos on social networks, and interact with friends on microblogs and chat apps. As a result, our emotions, our geographic locations, and our schedules are to some extent already transformed into data. Despite people’s delight to share their personal information online, I do not think many of them feel it happy when they realize that social networks are silently recording and collecting data on every aspect of their lives. At this stage, companies implementing big data strategies in social networks do not clarify the real purpose of the personal data they collect from users, which is the reason for users' mistrust. Unlike the traditional Internet era, data in the big data environment is more connected. Although operators share and analyze customers' personal data with anonymity, as the number of sources and volume of data increases, seemingly disparate and separate data can be matched by certain correlations, rendering the prior anonymization ineffective.

The risk that such personal information can be re-identified puts the issue of user privacy and security increasingly on the agenda of regulators, legislators and other relevant agencies.

3) The control of user personal information has diminished. Compared to the traditional environment, people now have significantly less control over their personal information. In the traditional environment, information dissemination mode is costly and users still have a weak control over their personal information. However, in the era of big data, information about individuals on social networking sites can be easily accessed, collected and disseminated. By integrating and analyzing personal information from different social networks, it is likely to build a system of information including the target's biography, preferences, networks and beliefs. The easy reproducibility and long-term preservation of digital information makes it easy for people with ulterior motives to access the tainted information that is detrimental to us, thus weakening our control over personal information.

3. Ways to protect the security of personal information in social networks in the era of big data

Keeping users' personal information secure is a prerequisite for social networks to continue to develop in the era of big data. The problems of account theft, data loss, and extortion due to privacy make us aware that the problems of social networks in the era of big data must be tackled at all levels, including the state, industry, and users, in order to take advantage of the advantages of big data in enterprise innovation and user service.

1) The laws and regulations related to personal information security should be followed up simultaneously. Big data technology is still a new thing in China, and the industry is constantly trying to figure out and move forward, facing problems such as the lack of relevant laws and regulations and failure to effectively maintain the security of users' personal information. Information Security Technology - Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems, the highest national standard for the protection of personal information, was implemented on March 1, 2013. It defines how to reasonably use personal information in the era of big data to guide and regulate the activities of using information systems to handle personal information. However, the legal effect of national standards and industry standards is far from being able to protect people's personal information security, and the provisions for information security protection scattered in other laws and regulations cannot meet the current needs of people for information dignity and information control. Therefore, in the era of big data, in order to protect personal information security, the top priority should be given to establishing the basic legal system for personal information protection, and it is urgent to introduce the Personal Information Protection Law as soon as possible.

2) The self-regulatory convention of social network service industry should be improved. Good industry regulations and industry self-regulatory conventions are important conditions for the prosperous development of an industry. If social network companies want to go longer in the era of big data, they should make efforts to build common regulations for the industry, maintain the security of user information, build customer trust, and gain lasting benefits from big data.

First, the status quo of users' information secretly collected should be changed. Social network companies should respect users' right to know, inform them of the personal information they collect, and give them the right to authorize operators to collect and use their own information and data. In addition, the terms of service should clarify how personal information data is to be used and how long it is to be used.

Second, efforts should be made to seek a self-regulatory convention recognized by the owners of personal information, data service providers and data consumers in social networks. In this way, the legality of data sharing can be guaranteed, and the privacy and security of users' personal information can be guaranteed by third parties when using users' data on social networks, so as to create a secure environment for data use.

3) The security protection technology of big data should be improved. In the big data environment, in order to protect the security of personal information in social networks, safe and

powerful protection technology is also crucial, in addition to laws and regulations and industry self-regulation constraints, since it can guarantee the security of personal information from the source to some extent.

First, the integration of big data technology and information security technology should be strengthened. In the face of the ever-expanding volume of data and a wide variety of client applications, a higher and broader perspective of big data should be used within the social network service industry to judge and monitor network security. Moreover, the organic integration of big data technology and security technology should be used to discover the security risks of the system in advance as much as possible, and constantly update the characteristics of viruses and phishing software, so that users have a good space for personal information protection when using social networks.

Second, efforts should be made to update and improve anonymization techniques. It has become an unstoppable trend for social network operators to offer precise marketing services by using big data analysis and prediction technologies. The social network service industry should strive to find more professional algorithms to improve the anonymity technology, in order to solve the contradiction between data analysis applications and users' privacy.

4) Information security literacy of users should be improved.

First, users should have a sense of digital abstinence. Users should use social networking sites and mobile social applications rationally, weighing the trade-offs and taking a long-term view when using social networks. Users should be conscious of moderation when sharing real photos, personal whereabouts, and instant geolocation information on the Internet, and effectively set access rights for strangers to keep personal information within their control as much as possible.

Second, users should reduce the comprehensibility of their account information. Users of social networks websites should be prevented from using their names or initials plus birthdays to apply for and set up passwords for social networks websites, and from using the same email address and password to apply for multiple web applications. Also, users should avoid transmitting their network passwords through social networks websites or cell phones.

Third, users should take the initiative to receive information security education. Relevant surveys show that users who have attended information security training courses have stronger information security awareness and more outstanding security ability to protect personal information. In the era of big data, users should carefully read the security and privacy protocols of social networks operators, be familiar with the corresponding privacy settings, and proactively protect their own information security.

4. Conclusion

In the context of big data, users should also update the security software of their computers and smart mobile devices to avoid logging into web applications and using mobile payment under public WIFI conditions to avoid threats to personal information security and property safety. The personal information in social networks is a big gold mine in the era of big data, and it is the focus of many people's attention. In the new era, we are required to improve information security literacy, strengthen big data security protection technology, and protect the security of personal information by legislation and industry self-regulation.

References

[1] Chang Yaping, Zhu Donghong. Measurement of participation motivation of social network users [J]. Library and information work, 2011 (14): 34-37

[2] Shi Yaguang, Yuan Yi. Research on information dissemination mode based on social network [J]. Library forum, 2009, 29 (006): 220-223

[3] Yi Chengqi, Bao Yuanyuan, and Xue Yibo. "Social network big data analysis framework and its key technologies." ZTE technology 01 (2014): 5-10

[4] Wen Xin, Chen Nengcheng, Xiao Changjiang. User influence analysis based on spark graphx and social network big data [J]. Computer application research, 2018, 35 (3): 830-834