Research on Personal Privacy Protection Strategies in Social Networks

Tan Ying

Department of Information, Yunnan University of Finance and Economics, Kunming 650221, China

Keywords: Social networks, Privacy protection, Anonymous technology, Track privacy

Abstract: With the development of network technology, people's social activities based on network are more and more extensive. While enjoying more convenient, fast and diversified social activities, people's privacy is also facing great security threats. This paper describes and analyzes the technical means of privacy protection in social networks, and puts forward the privacy protection countermeasures from the legal level, industry self-discipline and improving users' self-protection awareness.

1. Introduction

Since the birth of human beings, human beings have never stopped social activities. With the continuous progress and development of human society, the social needs of human beings are also increasing. In recent years, with the rapid development of Internet technology, social networks have gradually become an important carrier of people's social activities. It not only makes communication between people more convenient and faster, but also shortens the distance between people and expands the scope of communication between people. Especially in the new epidemic in early 2020, more and more people began to choose such social ways as online office and online learning. As more and more people use social networks to serve their lives, they also expose their basic information, life trajectory, preferences, health, work conditions and other user privacy. Therefore, the privacy security of users in social networks has become an important issue and a new research hotspot.

2. Privacy in Social Networks

The social network is called Social Network Service (SNS). Its purpose is to provide people with a social network Internet application service and provide users with a platform for online interaction and communication. At present, social networks at home and abroad are very widespread, and there are many social platforms, such as FaceBook and MySpace abroad, QQ, WeChat, Sina Weibo, Renren. The scale of social networks around the world is still expanding and the number of users is still increasing. According to its different functions, it can be divided into three categories: 1. Communication tools, such as QQ and WeChat, are designed to facilitate users to keep in touch with their friends. Of course, its function goes beyond this. Users can share their experiences, photos and videos on the platform. 2. E-commerce platforms, such as Taobao, Jingdong, Pinduo, etc., establish social activities between merchants and customers and between customers and customers. 3. for online learning and online office platforms, such as Tencent Conference, Rain Class, etc. 4. Entertainment platforms, such as games, network video playing, etc. Social relationships are formed between players and video viewers. From this, we can see that the scale of social network users is very large, the social scenes are also varied from traditional social activities, and the social groups are rich.

All kinds of people have established and formed all kinds of social networks on all kinds of platforms, in which people share their lives, geographical locations, hobbies, online transactions, online meetings, online lectures, etc. These information contain user privacy such as home address, travel route, health status, work status, bank card information, etc. Once these privacy information is obtained by lawless persons, it will damage the life and economy of users.

Copyright © (2020) Francis Academic Press, UK DOI: 10.25236/iwass.2020.037

3. Ways to Infringe Privacy

3.1 Unintentional Disclosure by Users

Many users like to publish their experiences, photos of outing, family and friends gathering information and so on through social platforms, which contain a lot of privacy for users, even if users set these publications to be only visible to specific groups. However, these information may still be transmitted to the third party, resulting in the leakage of user privacy, which is mainly due to the user's lack of defense psychology, blind trust in people in social network groups, and lack of awareness of self privacy protection, which may also cause the disclosure of other people's information.

3.2 Disclosure of Social Networking Sites

If users want to use the social network platform, they must register and fill in their relevant information when registering. At this time, users' private information will face two possibilities: one is that their information can be well protected by social networking sites, but they still face the leakage of users' personal information caused by hacker attacks on social networking sites. The second is that social networking sites themselves voluntarily disclose users' private information, thus obtaining certain benefits.

3.3 Leaked by a Commercial Company

At present, many commercial companies set up public numbers for users to pay attention to and register as their members, or users conduct online transactions through e-commerce. Some merchants always try to collect and accumulate a large amount of personal data about consumers in these activities in order to provide personalized services for users. However, many businesses still collect users' personal information, establish user information databases, and transfer and sell users' personal information to other companies for profit or for other commercial purposes.

3.4 Disclosure in Data Mining

A large amount of personal information on social networks is collected, processed, analyzed, shared and published by organizations or individuals, and useful knowledge is mined for commercial use or scientific research. In the process of data mining, a large amount of personal sensitive information will inevitably be leaked. How to ensure high availability of data without disclosing users' private information has attracted increasing attention of researchers at home and abroad.

4. Privacy Protection Strategies for Social Networks

4.1 Technical Proposal

For privacy protection in social networks, the most direct and effective solution is to use technical means. At present, experts at home and abroad have proposed various technical solutions, including encryption technology, anonymity technology, trajectory protection technology, etc.

(1) Encryption technology

Using cryptography tools is one of the most commonly used technical means. The data encryption process is implemented by various encryption algorithms. According to whether the keys of the sender and receiver are the same, the cryptosystem includes symmetric key cryptosystem and asymmetric key cryptosystem. In practical application, these two technologies are usually combined, i.e. asymmetric key cryptography is used to transmit secret keys between two communicating parties, and symmetric key cryptography is used to encrypt and decrypt the data actually transmitted. However, people are using mobile intelligent terminals more and more nowadays. The resources of mobile terminals are very limited, and the resources needed by cryptographic tools for encryption processing are too large.

(2) Anonymity technology

Since Samarati and others first proposed the concept of anonymity in 1998, the research on

anonymity has become a hot topic in recent years. Various new anonymity models and methods have been proposed. Among them, k-anonymity model, (α, k) -anonymity model and t-closeness model are the most typical models. In the k-anonymity model, the larger the value of k, the more attribute values need to be generalized, and the better the privacy protection effect, but the more data loss, the worse the data availability. The smaller the value of k, the less the attribute value to be generalized, the less the data loss, the better the data availability, but the privacy protection effect is not good. Sweeney et al. think that the value of k is generally not more than 5 or 6 William points out that the value of k should be in the range of 3 to 10. whether the value of k is reasonable will be the key to solve the balance between privacy disclosure and data quality. On the basis of k-anonymity model, Wong et al proposed (α, K) - anonymity model to resist network attacks by controlling the frequency of sensitive information in each equivalence class to be no more than α. In 2007, Li Ning-hui et al. proposed a t-closeness model, which requires that the difference between the distribution of sensitive attribute values in each equivalent class e and its global distribution in the anonymization table is less than t, which can effectively solve similarity attacks. However, no matter which model can effectively resist network attacks to a certain extent, each has its own shortcomings: the value of k in the k- anonymous model is not easy to determine. (α, k) -- Anonymous model has dual constraints of k and α, and the loss of information is greater. The t-closeness model requires too much for each sensitive attribute value, and trades for information at the expense of data availability.

(3) Track protection technology

People are increasingly using location-based services in social networks, such as publishing their location when publishing information in WeChat circle of friends, or sharing a certain location with friends in the group. These services can help us quickly find the destination, understand the surrounding environment, traffic conditions, etc. But if people need to enjoy these information services, they must provide their location to lbs server (location based service). If the attacker intercepts these locations and connects them, the user's trajectory will be formed. These locations and tracks imply user privacy, such as home address, travel route, life preferences, health status, work conditions, etc. for this kind of privacy, the commonly used technologies include false track interference method and inhibition release method.

① Some scholars have proposed to generate false tracks by rotation generation or random production, and then add these false tracks or replace the true tracks to realize the fuzzy processing of the original data, so as to achieve the purpose of confusing the real data and protecting the privacy of users' tracks. How to choose the number of false tracks is the key. Too many will reduce the risk of real users being exposed, but the greater the impact on real information, and if too few, the greater the risk real users will face.

② Suppression technology, also known as hiding technology, is to suppress/hide certain data and selectively publish original data. Attackers cannot see the suppressed data. The suppressed data is either deleted or replaced by certain characters. Therefore, the suppression technology is simple to implement and has a high degree of protection for private data. But in the process of practical implementation, when there are too many suppressed data, the data distortion is serious, and the availability of data will be greatly reduced. Therefore, how to suppress information and what information is the key to the effectiveness of this technology.

4.2 Legal Measures

Foreign countries have studied the right to privacy for more than a hundred years, while China is still in its infancy. There is no systematic legislation on the right to privacy. Provisions concerning the protection of the right to privacy are scattered in some laws, regulations and rules, with scattered contents and lack of unity. Some regulations are repetitive and lack cohesion and unity. When citizens' right to privacy on the Internet is violated, they cannot get legal relief. In addition, due to the virtual and technical reasons in social networks, it is very difficult for users to have sufficient technology as support once their privacy rights are violated. It is very difficult to investigate the infringement liability and it is almost impossible to identify the identity of the infringer. Therefore,

it is very necessary and urgent to legislate to construct the legal protection system of network privacy in our country.

4.3 Strengthen Users' Self-Protection Awareness

Users should strengthen their awareness of personal privacy protection and pay attention to carefully reading their privacy policies when downloading software or registering a social networking platform. When using these social tools, care should be taken to set up the privacy tools they provide. When sharing their personal life information, care should be taken to protect the sensitive information consciously. Don't trust strangers on the Internet. When conducting online transactions, care should be taken to prevent the disclosure of important information such as bank cards, ID numbers and so on. When conducting online meetings, care should be taken to properly keep the password for entering the meeting. Once users pay attention to their privacy in social networks, the possibility of their privacy being violated will be greatly reduced.

4.4 Industry Self Discipline

Since the legal system always lags behind the practice of the network, we cannot rely solely on the legal system to control the network behavior, and the strict legal system will also inhibit the development of the network. However, industry self-discipline can adopt more flexible policies, which can be adjusted with the development of information technology. Self-discipline protection measures can also be improved with the improvement of infringement methods, which can better adapt to the development of the network, and can make up for the relative lag and lack of flexibility of laws and regulations. Therefore, the establishment of an effective industry self-discipline mechanism coordinated with legislative protection can better adapt to the changes and development of the network.

All social networking sites must take the initiative to protect the privacy of users. In 2010, Canadian scholars conducted a survey on the privacy policies of six major social networking sites in the United States, namely Facebook, LinkedIn, MySpace, YouTube, Twitter and Orkut. It was found that most of the six major SNS sites protected the privacy of users from the purpose and visibility of information, but lacked the protection of granularity and server cache information. Even in the past decade, this situation has not improved significantly. Therefore, social networking sites must strengthen their own security, take reasonable and effective protection measures to protect the privacy security of their platform users, and also explain to users the purpose and purpose of the information collected when they register, and actively guide users how to set their privacy security in the application.

5. Conclusion

Social networks will become more popular with the development of information technology, and people will increasingly rely on social networks to engage in social activities. Therefore, it is very important to improve the information security and privacy security of users in social networks. In addition to the continuous updating and improvement of technology, the government is also required to formulate relevant laws. The industry has shouldered its responsibilities, and users have strengthened their awareness of protection to provide a better environment for the healthy development of social networks in the future.

References

[1] Samarati P, Sweeney L. Generalizing data to provide anonymity when disclosing information[C]. Proceedings of the Seventeenth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems, Seattle, WA, USA, 1998: 188.

[2] Sweeney L. Achieving K-anonymity privacy protection using generalization and suppression [J]. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 2002, 10(5):571-588

[3] William E Winkler. Using simulated annealing for k-anonymity [R]. Research Report 2002-07, US Census Bureau Statistical Research, Division, 2002

[4] RC Wong, J Li, AW Fu. K Wang. (α, k)-Anonymity: An Enhanced K-anonymity Model for Privacy-preserving Data Publishing [C]. Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data mining. New York: ACM press, 2006

[5] Li Ning-hui, Li Tian-cheng, Venkatasubramanian S. T-Closeness-privacy beyond K-anonymity and L-diversity[C].Proceedings of IEEE 23RD International Conference on Data Engineering. Istanbul, Turkey: IEEE Press, 2007:44-56

[6] YOU T H, PENG W C, LEE WC. Protecting moving trajectories with dummies[C]//Proceedings of the 2007 International Conference on Mobile Data Management. IEEE, 2007: 278-282.

[7] Leanne Wu, Maryam Majedi, Kambiz Ghazinour, et al. Analysis of social networking privacy polices[C]. Proceeding of the 2010 EDBT/ICDT Workshops, Lausanne, Switzerland 2010.