Int. J. Advanced Networking and Applications
Volume: 12 Issue: 01 Pages: 4528-4531(2020) ISSN: 0975-0290

Research on Privacy Protection Strategies of Mobile Social Network Users

Pshwang Wang
School of Management Science and Engineering, Anhui University of Finance & Economics, China
Email: pshwang@163.com
Zecheng Wang
School of Management Science and Engineering, Anhui University of Finance & Economics, China
Email: zcwang@ah.edu.cn)

ABSTRACT

In order to protect mobile social network users' privacy information, and promote the healthy development of the mobile social industry, This paper studies the types and ways of user privacy disclosure in mobile social networks, and proposes the privacy protection strategies for users in mobile social networks from the aspects of formulating national laws and regulations, building and managing mobile platforms, improving privacy protection technologies and enhancing personal protection awareness. It also briefly introduces the development trend and future research of access control policies in mobile social network.

Keywords - **Mobile social network, User privacy, Privacy policy, Access control model.**

Date of Submission: Aug 24, 2020 Date of Acceptance: Sep 07, 2020

1. Introduction

In recent years, with the rapid development of mobile Internet and the continuous popularization of intelligent terminals, mobile social applications have achieved rapid development and various terminal applications have been emerging. In China, users' use of mobile Internet mainly focuses on instant messaging, mobile search, mobile shopping and other fields [1]. However, these mobile applications often require user information, such as mobile phone number, ID number, address book, location information and address information, etc. when they log in, register or provide services. The obvious problem is that users' personal privacy will be more easily disclosed. With the accelerated development of cloud computing, artificial intelligence, big data and other technologies, privacy leakage will become more and more serious [2]. Therefore, ensuring the security of mobile social networks and enabling users to fully enjoy the advantages and convenience brought by mobile social networks in the era of big data while better protecting user privacy is an important issue that needs to be urgently solved in the current big data environment, and is also the key to the orderly and healthy development of mobile social platforms.

2. Classification of User Privacy In Mobile Social Networks

In the era of big data, professional data collection, information tracking technology and location-based service technology (LBS) make users' basic information available, which not only creates value and facilitates our life, but also threatens users' privacy security. User privacy in mobile social networks is a manifestation of personal privacy information on mobile devices, which involves a wider range and more complex and diversified data [3]. At present, the privacy of mobile social networks mainly includes the following categories:

Basic information. It refers to the personal information such as name, age, identity information, contact information, occupation and address used by users when using mobile social network, and even includes the address book, photos, memos and other information in users' mobile devices. This information not only promotes the communication between users, but also increases the risk of user privacy disclosure to some extent.

Location information. It mainly refers to the real-time and historical location information including the user's specific geographic coordinates and specific time. Such information is often combined with practical applications, such as "location", "check-in", "search for nearby food/bus" and other location-based services, and the exact time and geographic coordinates of such information may expose the user's location privacy.

Trajectory information. Trajectory information refers to the position information [3,4] which is serial in chronological order and can reflect the specific behavior rules of users. This includes information saved by users when they access the network, such as frequent places, habits, interests, etc., which can be directly or indirectly inferred.

Information on social relations. Refers to the intimate information generated in the process of using mobile social networks, such as friend recommendation, interaction, information sharing and other related text, picture, audio and video information.

3. Disclosure of user privacy in mobile social network

3.1 Users' self-disclosure on mobile social platforms

On the one hand, in the process of using mobile social platforms, many users are keen to publish their current location, status and other information on the Internet when sharing text, photos, links, etc. Compared with traditional social network, mobile social network can deliver more and more accurate information [4]. On the other hand, in order to obtain location-based personalized services, such as trip check-in and query of relevant information near the immediate location, users will submit their own location information in the application. However, in this process, users do not attach great importance to the disclosure of their own information, and the limited privacy protection settings provided by the service providers are often only used by a few people [5], which will inadvertently make personal privacy disclosure and the use of malicious theft.

3.2 Illegal collection by a profiteer for the purpose of obtaining profits

In the era of big data, the user's information can create a huge commercial value by mining processing, to get operation service provider to collect more and more comprehensive user information. A lot of software in the login even installation is required to obtain the user's personal address book, memos, photographs, location, health, and other information [6]. The lack of privacy protection professional technical support, it is easy to cause the leakage of personal information and some speculator illegal use. What's more, some people or enterprises may gain profits by directly selling user data or selling the information after processing.

3.3 Malicious attacks by hackers

Economic value brought by the users' privacy, prompting some people with professional technology to illegally collect user privacy information through technical means, attack social networking sites or users' mobile devices, implant malicious software, gain users' privacy or listen to users' behaviors, and even threaten users' property security, thus bringing great losses and harms to users.

4. Privacy protection strategies for mobile social network users

4.1 Formulation of relevant laws and regulations

National policies and regulations are important safeguards to protect social network privacy. At present, there is no special law concerning the protection of personal privacy on the Internet in China, which has a direct impact on the development of China's big data market and data security. And on the establishment of relevant laws and regulations, also there are many difficulties and limitations, such as the establishment of policy and update speed lag behind the development of technology, legal protection of binding may be a negative impact on industry development, such as privacy infringement case is difficult, it needs to be from the actual situation of our country, the comprehensive factors can adapt to different types and situation of policy, standardize services, to crack down on to steal the privacy of users' personal behavior, promote positive and healthy development of the social network and mobile Internet industry.

4.2 Construction and management of mobile social platforms

Operators of mobile social networking platforms need to strengthen their own platform construction, standardize their behaviors, change their profit-oriented operation mode, and take the protection of users' interests as their responsibility to create a safe mobile social networking environment for users. In terms of construction and management, they should restrain their own behaviors and not collect personal privacy information irrelevant to the application; Standardize relevant "default options" to inform users of the scope and manner of use of personal information to increase the transparency of data use; Pay attention to the security of user data, strengthen the function of information confidentiality, avoid the phenomenon of data sales and disclosure. Other aspects include enhancing the security awareness of platform data managers, reminding users to improve the security level of personal privacy information settings, etc.

4.3 Improvement of privacy protection technology

Due to the overheated mobile social networking market, many service providers, driven by interests, are often eager to launch imperfect software while ignoring the construction of data security, which is extremely detrimental to the protection of users' personal information [7]. On the other hand, the development of privacy protection technology also needs to seek the balance between privacy protection and service quality, which can not only ensure the data mining and storage of user information in a secure and effective environment, but also not hinder the development of mobile social network platform due to excessive data protection. Both of these two aspects require the related researchers and service providers to conduct in-depth research and discussion on privacy protection technology from multiple aspects such as data processing and storage.

4.4 Enhanced awareness of personal privacy protection

As the subject of using mobile social applications, users should be fully aware of the importance of protecting personal privacy information and reduce the risk of personal information disclosure due to their weak awareness of privacy and security. Users should be aware of the possible consequences of their information sharing behaviors in the application, and share important information cautiously. For example, when the service provider requests to obtain address book, photo, location and other information during application installation, it should confirm whether the application really needs such information when providing relevant services, and improve the setting of privacy rights. Minimize location information when sharing links or personal status; Try to use false names to protect personal information when registering websites that do not require real user information, and do not provide real ID number or mobile phone number; Other

operations, such as using links to regular websites to download apps and turning off Cookies, are also included. In addition, in the event of information infringement, users should take the initiative to protect their legitimate rights and interests.

5. Development trend and future work

Mobile social network has a huge social relation map, and the access control model based on the relationship is more conducive to expressing the complex relationships among them, so as to construct the access control strategy combination with rich and natural social significance [8]. Therefore, the development trend of mobile social network access control model may be based on relationship, integrate trust value calculation and ontology technology, and strive to cover the mobile social network relationship map and behaviors based on it in detail and naturally.

Personalization of access control policy is an inherent requirement of mobile social network, which requires a policy language with strong expressive ability, authorization policy needs to be flexible, and has certain conflict detection and resolution ability. Existing policy language, such as: OWL, SWRL, modal logic language, mixed logical, regular expressions, PBel language based on the logic of four values, etc. Its expression ability is poorer, or rule derivation efficiency is low, or the lack of policy conflict detection and solving ability. Mobile social network access control model is an important research direction in the study may be express ability, high efficiency, conflict detection and resolution ability of access control policy language.

The algorithms and decision mechanisms involved in the access decision process, such as path searching and trust value calculation, must be accurate and efficient. With the development of pattern recognition technology and the advent of algorithms that can accurately identify and automatically generate tags from content such as photos, privacy-related access control will become more complex in the future and more sophisticated and effective solutions will be needed to address the security and privacy challenges of multiple Shared data in mobile social network. It must involve the research of encryption and decryption algorithm, key distribution scheme and so on. Policy management is another area of research, because the social graph of mobile social network is large and constantly changing, users need a very flexible policy language to express their privacy needs, and effective technologies and tools to assess the risks of unauthorized information flows.

Based on the above analysis, the future mobile social network access control model will still be based on relationship as the mainstream, and the research direction may focus on policy language development, efficient and common path discovery algorithm, multi-party authorization and policy conflict solution, privacy disclosure risk assessment, policy management and other aspects.

6. Conclusion

In the era of big data, the development of mobile Internet technology has greatly changed people's work and lifestyle. While making full use of big data to mine all kinds of information and enjoy the convenience brought by big data, users' privacy is inevitably seriously threatened. Therefore, it has become an important practical issue how to make full use of big data, better protect users' personal information, and enable users to use mobile social network services more securely while fully enjoying the benefits and advantages of mobile social networking. In this paper, the type of user privacy, privacy mode is studied and discussed, and put forward the strategy of the mobile social network users' privacy protection from the aspects of national laws and regulations, the construction of the mobile platform, technology, personal privacy protection consciousness, etc. so as to fully protect the privacy of mobile users at the same time promote the healthy development of mobile social industry.

7. Acknowledgment

We thank the anonymous reviewers and editors for their very constructive comments. This work was supported by the National Social Science Foundation Project of China under Grant 16BTQ085.

References

[1] K. Khan, W. Goodridge, A Survey of Network-Based Security Attacks,*International Journal of Advanced Networking and Applications*, 10(5), 2019, 3981-3989.

[2] P. S. Wang, Z. C. Wang, and T. Chen, Personalized privacy protecting model in mobile social network,*Computers, Materials & Continua*,59(2), 2019, 533-546.

[3] G. Q. Jiang, *Privacy-preserving algorithms and its applications in MSNS*,Master diss, Donghua University, China,2016.

[4] H. Shen, M. Zhang, and H. Wang, A lightweight privacy-preserving fair meeting location determination scheme,*IEEE Internet of Things Journal*,7(4), 2020, 3083-3093.

[5] Z. Q. Feng, *Research on Problems of Network privacy under the age of big data: From protection of the rights to personal choice - A Case Study of mobile social networking users*,Master diss, Jilin University, China, 2016.

[6] Y. J. Ren, Y. Leng, and F. J. Zhu, 'Data storage mechanism based on blockchain with privacy protection in wireless body area network'. *Sensors*,19(10), 2019, 2395-2406.

[7] L. S. Huang, M. M. Tian, and H. Huang, Preserving privacy in big data: a survey from the cryptographic perspective,*Journal of software*,26(4), 2015, 946-952.

[8] Y. Cheng, J. Park and R. Shu, An access control model for mobile social networks using user-to-user relationships,*IEEE Transactions on Dependable and Secure Computing*,13(4), 2016, 424-436.

Author Biography

Pingshui Wang, Doctor of Engineering, professor. Graduated from Nanjing University of Aeronautics and Astronautics in 2013. Worked in Anhui University of Finance and Economics in China. His research interests include information technology and information security.

ZechengWang was born in Anhui, China. He received the B.S. degree in computer science and technology from Anhui Normal University, China, in 1993 andthe M.S.,and Ph.D. degrees in computer science and technology from East China Normal University, China, in 2003, and 2008, respectively.

Since 2008, he hasbeen with the School of Management Science and Engineering, Anhui University of Finance and Economics, China, where he is currently an Associate Professor. His research interests include cryptography and information security.