ChinaRxiv

AI translation · View original & related papers at
chinarxiv.org/items/chinaxiv-202308.00541

Evaluation Indicators and Empirical Study on Mobile APP User Privacy Information Leakage Risk: Postprint

Authors: Tian Bo, Zheng Yusha, Liu Pengyuan, Li Chunhao

Date: 2023-08-27T00:00:00+00:00

Abstract

[Purpose/Significance] In response to the increasingly severe phenomenon of privacy information leakage among mobile APP users, analyzing and evaluating the associated risks contributes to protecting user privacy and fostering the healthy development of information platforms. [Method/Process] This study analyzes the risks of privacy information leakage for mobile APP users, constructs a risk evaluation index system for user privacy information leakage, employs the Analytic Network Process (ANP) and entropy weight method to comprehensively determine the combined weights of indicators, and applies fuzzy comprehensive evaluation to conduct empirical analysis on mobile social APPs. [Results/Conclusion] The constructed risk evaluation index system for mobile APP user privacy information leakage demonstrates scientific validity and practical applicability. Within the index system, risks arising from APP platform factors represent the highest threat to privacy leakage, followed by user-related factors. Overall, PaiPai exhibits the highest privacy leakage risk, while WeChat shows the lowest, though both approach a moderate risk level. To mitigate privacy information leakage risks for mobile social APP users, mobile users, APP platforms, and regulatory authorities should implement targeted measures based on the specific circumstances of each APP.

Full Text

Mobile APP User Privacy Information Leakage Risk Evaluation Index and Empirical Study

Tian Bo, Zheng Yusha, Liu Pengyuan, Li Chunhao
School of Management, Jilin University, Changchun 130022

Abstract

[**Purpose/Significance**] In response to the increasingly serious phenomenon of privacy information leakage among mobile APP users, analyzing and evaluating the risks of privacy information leakage is conducive to protecting user privacy and promoting the healthy development of information platforms. [**Method/Process**] This paper analyzes the risks of privacy information leakage for mobile APP users, constructs a risk evaluation index system for user privacy information leakage, uses the Analytic Network Process (ANP) and entropy method to comprehensively determine the combined weights of indicators, and applies fuzzy comprehensive evaluation to conduct empirical analysis on mobile social APPs. [**Result/Conclusion**] The constructed risk evaluation index system for mobile APP user privacy information leakage demonstrates scientific validity and practical applicability. Within the index system, privacy leakage caused by APP platform reasons poses the highest risk, followed by leakage caused by user reasons. Overall, PaiPai exhibits the highest user privacy leakage risk, while WeChat shows the lowest, but both are close to medium risk. To reduce privacy information leakage risks for mobile social APP users, mobile users, APP platforms, and regulatory authorities should take targeted measures according to the specific circumstances of different APPs.

Keywords: mobile APP users; privacy information; information leakage; risk assessment; analytic network process; entropy method; fuzzy comprehensive evaluation method
Classification Number: G203; TP393

---

1. Introduction

In recent years, the number of mobile APPs has grown dramatically, and the amount of personal privacy information disclosed by mobile APP users has increased substantially. As the scope of personal information utilization continues to expand and the value of personal information is continuously mined, Chinese mobile internet users face threats of personal information leakage and abuse while experiencing personalized services [**?**]. Taking mobile phone APPs as an example, according to data released by the DCCI Internet Data Center in 2017, 96.6% of Android system mobile applications require access to user privacy permissions, with 25.3% exhibiting excessive permission acquisition. This indicates that many potential information leakage risks are hidden in the process of using mobile APPs. Once user privacy information is leaked, it may cause significant distress or loss to users and affect the use and efficiency of information platforms. To protect mobile APP user privacy and promote the healthy development of information platforms, research on user privacy information leakage has become a focus of attention in both industry and academia in recent years.

Mobile APPs refer to mobile application services developed for smart mobile

terminals connected to the Internet or wireless network card services. Privacy refers to "personal information or behaviors that are not disclosed to others." Mobile APP user privacy refers to information that users are unwilling to let others know and disclose during the process of downloading or using mobile APPs, specifically including: (1) personal information such as name, address, phone number, email address, and living status; (2) digital behaviors such as browsed information and dwell time, visited web pages, and ordered products; and (3) communication content including call records, emails, and text messages [**?**].

2. Literature Review

Scholars both domestically and internationally have conducted relevant research on privacy information leakage risks for internet and mobile APP users. International scholar K. Zhu et al. [**?**] calculated the risk coefficient of privacy leakage for mobile APP users and recommended safe APPs for users based on their applications to reduce privacy leakage. G. Bansal et al. [**?**], based on rational behavior theory and prospect theory, explored factors affecting trust levels and disclosure willingness during mobile user transactions from two aspects: the sensitivity of the privacy information disclosure environment and user personality. Y. Li [**?**] studied the impact of two contextual factors—website perceived reputation and user familiarity with websites—on the relationship between user privacy attitudes and website privacy concerns, and analyzed the indicators and sources of privacy attitudes. B. Martínez-Pérez et al. [**?**] analyzed the security and privacy of personal health information in mobile health applications, examined current relevant laws in the EU and the US, supplemented some standards and certifications regarding security and privacy, and provided recommendations for mobile health application designers. C. L. Miltgen et al. [**?**] developed a new comprehensive model including an antecedent variable (regulatory knowledge), a moderating structure containing perceived privacy regulatory protection, trust, and privacy risk, two outcome variables (protective behavior and regulatory preference), and incorporated the direct and moderating effects of perceived benefits. After researching and testing the model, they proved its practicality.

Domestic scholars Wang Xiwei et al. [**?**] analyzed and compared the research status, hotspots, and future trends of information privacy in the new media environment both domestically and internationally, and analyzed hotspots and development trends of information privacy in the new media environment through knowledge mapping. Li Zhuozhuo et al. [**?**] studied relevant regulations on personal privacy information protection domestically and internationally from the perspective of the data lifecycle, analyzed related issues in mobile APP service agreements, and proposed corresponding recommendations. Liu Jiao et al. [**?**] conducted a comparative analysis of "user privacy statements" in Chinese and English APPs, finding that Chinese APPs had more problems and lower emphasis on personal privacy protection compared to English APPs. Zhu Guang

et al. [?], based on qualitative analysis of network privacy risks in the big data environment, used the Delphi method to construct a risk evaluation index system, introduced the entropy method to assign weights to indicators, and finally conducted empirical analysis on the privacy risks of a social network service platform. Wang Shan et al. [?] analyzed the research status of privacy protection from three aspects: law, regulation, and technology, and proposed prospects for personal information protection research in the big data era. Meng Xiaoming et al. [?] studied possible causes of personal privacy leakage in various commercial development models of social network big data and proposed corresponding personal information protection strategies. Xu Xiaolu [?] analyzed the status and causes of privacy leakage in mobile social networks, studied mobile social network users' concerns about personal privacy protection from multiple aspects, and proposed a series of strategic recommendations to improve network users' personal information protection levels. Zhang Qiujin [?] constructed a cloud computing privacy security risk assessment index system containing 28 secondary evaluation indicators and evaluated personal privacy security risks during cloud computing service processes. Zhu Yijie [?] constructed an index system containing 26 secondary evaluation indicators from five aspects: direct communication leakage, eavesdropping channel leakage, theft leakage, third-party leakage, and other factors, and evaluated user privacy leakage risks in location-based services.

Based on the above review of domestic and international research, studies on mobile APP users' personal privacy information have mostly focused on the rationality analysis of platform privacy statements, comparisons of privacy information protection between China and other countries, and research on user privacy security, privacy concerns, privacy attitudes, information disclosure behavioral intentions, and users' personal privacy information protection on certain types of network platforms. In contrast, scholars have paid more attention to user privacy information leakage risks in the internet environment, but there has been little research on risk evaluation specifically targeting mobile APP users. However, since mobile APPs rely on mobile devices with characteristics such as mobility, portability, and increasingly high usage frequency, the privacy leakage risks for mobile APP users are significantly different from traditional network user privacy leakage risks. Therefore, this study specifically addresses mobile APP user privacy information leakage risk evaluation, which serves as a beneficial and necessary supplement to existing research.

2. Design of Mobile APP User Privacy Information Leakage Risk Evaluation Index System

2.1 Basis for Evaluation Index System Design After carefully reviewing a large number of relevant documents, this paper organizes and summarizes the content related to mobile APP user privacy information leakage risk evaluation. This study divides mobile APP user privacy leakage risks into four aspects: privacy information leakage caused by user reasons, APP platform (operator)

reasons, management reasons, and other reasons. Since many APPs require network connection during use, mobile APP user privacy leakage risks intersect with network privacy leakage risks, and there have been many studies on network privacy leakage risks in academia. Therefore, the selection of some indicators can refer to relatively mature literature. Kuang Qingqing [**?**] designed a scientific and reasonable evaluation system to study personal privacy leakage risks in the internet environment. This study directly extracted or slightly modified (mostly modified) suitable indicators from it, including multiple mobile APP associations, erroneous operations, and poor network usage habits under user reasons; internal personnel maliciously leaking information, information abuse, and operational errors under APP platform reasons; forced disclosure based on legal or institutional requirements and direct information sharing by supervision institutions under management reasons; and backup materials and purchasing privacy information from third-party platforms under other reasons. This study also extracted two factors from Zhu Guang's [**?**] social network privacy risk evaluation system constructed through the Delphi method: simple mobile APP password settings under user reasons and hacker attacks under other factors. Additionally, by reviewing relevant literature and based on the unique mobility, convenience, stronger immediacy, and higher usage frequency of mobile APPs, this study proposed indicators specifically targeted at mobile APPs: mobile device loss, not turning off mobile positioning function [**?**], uploading excessive privacy data to cloud storage [**?**], not using mobile privacy control functions under user reasons; excessive permission requests by mobile APPs [**?**] under APP platform reasons; and insecurity of unfamiliar wireless networks [**?**] under other reasons.

To further improve the evaluation index system, the research team organized a focus group discussion, which initially yielded a system containing 4 primary indicators and 29 secondary indicators. The detailed content of each indicator will be introduced below.

2.2 Preliminary Establishment of Risk Evaluation Index System

2.2.1 User-Caused Privacy Information Leakage

User-caused privacy information leakage (C1) refers to information leakage resulting from improper operations or behaviors of mobile APP users themselves. This indicator system includes 10 secondary indicators:

- **C11: Mobile APP Association Usage** refers to users associating multiple APPs for use, or using different accounts on the same APP and receiving messages from other accounts, leading to information leakage.
- **C12: User Error Operations** refers to certain erroneous operations by users that lead to information leakage.
- **C13: Overly Simple Mobile APP Password Settings** refers to users setting passwords too simple for easy memorization, making them easily cracked and causing information leakage.
- **C14: Untimely Account Unbinding or Replacement** refers to users not unbinding or replacing old accounts when they are no longer in use. The most

common manifestation is when a mobile phone number is used as an account, the number is no longer used but not unbound from the APP that bound the number. If the account is reused by others, it causes the original account owner's information to leak.
- **C15: Poor Network Usage Habits** refers to bad habits users develop when surfing the internet, such as randomly clicking on unknown links, which may infect the phone with viruses and lead to information leakage.
- **C16: Mobile Device Loss** means that compared to fixed-location devices (such as computers), mobile devices have a greater risk of loss. Once lost, all privacy information is exposed to danger.
- **C17: Overly Optimistic Attitude Toward Privacy Information** refers to being too optimistic about mobile APPs' protection of personal privacy information, willingly or casually disclosing various types of information.
- **C18: Long-Term Non-Closure of Mobile Positioning Function** means that due to the mobility and convenience of mobile devices, many APPs require mobile phones to enable positioning functions, such as Didi Dache and Amap. People usually enable mobile positioning when needed but forget to turn it off afterward, which may lead to leakage of user location or trajectory information.
- **C19: Uploading Excessive Privacy Data to Cloud Storage** means that due to the relatively small storage capacity of mobile devices, people are accustomed to uploading various personal information or files to cloud storage for preservation. If the security of the cloud storage is threatened, personal privacy or important file information may be leaked.
- **C110: Not Using Mobile Privacy Control Functions** means that mobile devices or mobile APPs have designed some functions to prevent privacy leakage risks, such as keyboard locks and remote login verification, but many people disable these functions for convenient and quick use of mobile APPs, burying hidden dangers for the security of personal privacy information.

2.2.2 Mobile APP Platform-Caused Privacy Information Leakage

Mobile APP platform-caused privacy information leakage (C2) refers to leakage of APP users' personal privacy information caused by the platform operator during construction and operation. This reason includes 10 secondary indicators:
- **C21: Unreasonable Mobile APP Function Settings** means the APP itself has functional setting defects that are unfavorable for user privacy protection. For example, QQ software's default setting for QQ space updates is visible to both friends and non-friends. Sent information can be seen by everyone and may be "secondarily disseminated," eventually leading to uncontrollable situations for users.
- **C22: Excessive Openness of Mobile APP Platform** means the APP is too open to "third-party platforms." For example, some APPs recommend other network platforms on their interface to improve cooperation levels. When users browse these recommended platforms, they may leak their own information.
- **C23: Excessive Permission Requests by Mobile APP** means each mobile APP requests authorization during download, such as reading call records,

text messages, etc. Some software even obtains 20-30 authorizations, many of which are unnecessary. Compared with traditional devices like computers, mobile devices' unique telephone communication functions determine that they contain large amounts of call records, text messages, and contact information. Once leaked, the consequences can be severe.

- **C24: Mobile APP Sharing Information Without User Consent** means the APP platform shares users' personal information without user consent, causing privacy leakage.
- **C25: Mobile APP Modifying User Privacy Information Without Permission** means that after users upload their personal information, the mobile APP platform arbitrarily changes the information for its own purposes.
- **C26: Malicious Information Leakage by Mobile APP Platform Internal Personnel** refers to poor management of the APP platform, where internal personnel privately leak user information.
- **C27: Abuse of Information by Mobile APP Platform Internal Personnel** means APP platform internal personnel use users' personal information for their own purposes, such as privately using a user's name, phone number, ID number, and other information to conduct other business transactions, which may cause losses to users.
- **C28: Operational Errors by Mobile APP Platform Staff** means that APP operator staff cause user privacy leakage due to errors resulting from unfamiliarity with business processes.
- **C29: Inadequate Risk Prevention Technology of Mobile APP** means that the technology of the mobile APP platform has defects, causing certain information uploaded by users on the APP platform to be monitored, eavesdropped on, stolen, or destroyed.
- **C210: Poor Industry Self-Discipline** means that the entire industry has not paid attention to user privacy protection, and user personal privacy information trading has even become "normalized."

2.2.3 Management-Caused Privacy Information Leakage

Management-caused privacy information leakage (C3) refers to possible leakage of mobile APP user privacy information due to certain reasons from relevant management institutions or departments, including 5 secondary indicators:

- **C31: Forced Disclosure Based on Legal or Institutional Requirements** means that to better manage various mobile APPs, some laws or systems require APP platforms to disclose certain necessary registered user personal information, which may also cause user information leakage.
- **C32: Imperfect Network Privacy Information Disclosure Standards** means that China currently does not have a complete set of network user privacy information disclosure standards, resulting in chaotic disclosure of user personal information within the industry, which is detrimental to user personal privacy security.
- **C33: Lack of Supervision and Punishment System** means there is no perfect supervision and punishment system to constrain industry behavior, leading to increasingly serious privacy information leakage problems.

- **C34: Direct Information Sharing by Management Institutions** means that management institutions directly share certain user personal information stored in management departments due to some policy or regulatory requirements, causing user privacy leakage.
- **C35: Leakage by Management Institution Personnel** means that poor management or staff errors in management institutions lead to user information leakage.

2.2.4 Other Causes of Privacy Information Leakage

Other causes of privacy information leakage (C4) refer to causes other than the above three reasons (user, APP platform, and management reasons), including 5 secondary indicators:

- **C41: Backup Materials** means each APP platform backs up important user information to prevent information loss due to server crashes or paralysis. These backup materials that are not deleted at any known time also become a threat to user privacy information security.
- **C42: Insecurity of Unfamiliar Wireless Networks** means that due to the mobile nature of devices, people may use mobile APPs requiring networks in unfamiliar locations. If the mobile device itself does not have sufficient mobile network, it needs to temporarily connect to unfamiliar wireless networks. Connecting to unsafe WiFi may cause personal privacy leakage.
- **C43: Hacker Attacks** means network hackers use technical advantages to steal user privacy information through methods like stealing network servers.
- **C44: Purchasing Privacy Information from Third-Party Platforms** means certain individuals or institutions purchase user information from third-party platforms that retain or manage user privacy information for their own needs.
- **C45: Cracking or Guessing Account Passwords** means certain individuals guess others' passwords based on background information or crack others' passwords using technology to steal personal information.

2.3 Evaluation Index System Optimized by Delphi Method To ensure the scientific validity and rationality of the risk evaluation system, this study used the Delphi method to solicit opinions from relevant experts. Based on expert feedback, the preliminary index system was modified and improved by removing indicators with relatively low importance or those contained by other factors: C14, C22, C25, C27, C28, C35, and C45, making the evaluation system more streamlined. The final evaluation system is shown in Table 1 .

3. Evaluation Index Weight Calculation

3.1 Subjective Weight Calculation Based on ANP Method ANP, also known as the Analytic Network Process, is an extension of the Analytic Hierarchy Process (AHP). ANP is suitable for systems where elements are interdependent, influential, and have feedback relationships, making it more realistic. Therefore, using the ANP method to calculate the weights of various risk indi-

cators is more reasonable.

In the ANP model, indicator factors are divided into two parts: the control layer and the network layer. In this paper, the control layer is the risk of mobile APP user privacy leakage, and the network layer includes four element groups: user-caused information leakage, APP platform operator-caused information leakage, management-caused information leakage, and other causes of information leakage.

Since this calculation process is relatively complex, this paper uses SuperDecisions software to calculate indicator weights. The steps are: first determine the mutual influence relationships among element groups, then construct judgment matrices, and finally calculate the weights of each indicator.

3.2 Objective Weight Calculation Based on Entropy Method Entropy can be used to measure the uncertainty of things occurring [**?**]. Information entropy theory holds that information is a measure of a system's ordered state, while entropy is a measure of a system's disordered state. Generally, if the information entropy of an indicator is smaller, it means the indicator provides more information, plays a greater role in comprehensive evaluation, and thus has greater weight; conversely, it is smaller.

Since weights calculated by ANP have certain subjective elements, the entropy method can objectively calculate the weight of each indicator to a certain extent, modifying the subjective weights calculated by ANP to make the final results more reasonable. The steps for calculating weights using the entropy method are as follows:

First Step: Construct judgment matrix R = (r_{ij}){m×n} *based on expert scoring tables, and standardize the data in the matrix to obtain* Y{ij}:

Y_{ij} = (r_{ij} - min(r_i)) / (max(r_i) - min(r_i)) (Formula 1)

Normalize the standardized matrix. Assuming the normalized matrix is X_{ij}:

X_{ij} = Y_{ij} / Σ(Y_{ij}) (Formula 2)

Second Step: Calculate the information entropy of each indicator. Assuming the information entropy of the j-th indicator is e_j:

e_j = -k Σ(x_{ij} ln x_{ij}) (Formula 3)

where k = 1/ln(n). When x_{ij} = 0, x_{ij} ln x_{ij} = 0.

Third Step: Determine the weight v_j of each indicator:

v_j = (1 - e_j) / Σ(1 - e_j) (Formula 4)

3.3 Combined Weight Calculation Combining relevant literature [**?**] and considering the specific methods applied in this paper, the combined weight w_j

can be calculated using the principle of minimum information entropy and the Lagrange multiplier method:

w_j = (u_j v_j)^0.5 / Σ(u_j v_j)^0.5 (Formula 5)

4. Empirical Analysis

4.1 Sample Selection This study takes mobile social APP users as the research object to evaluate mobile APP user privacy information leakage risk. Social APPs were chosen because they are currently the most widely used type of APP. Users can access them via mobile phones or tablets, and they can be downloaded on both Android and iOS systems with basically the same usage methods and functions. Mobile social APPs can be roughly divided into three categories: (1) traditional SNS, such as Sina Weibo, Tencent Weibo, and Renren; (2) stranger social networking, such as Momo and Tantan; and (3) instant messaging, such as WeChat and QQ [**?**].

To ensure representative and universal sample selection, this paper comprehensively considered the 2018 Apple iTunes (China region) and Android app store mobile social APP rankings, selecting the top-ranked APP from each category and the bottom-ranked APP, totaling six typical mobile social APPs: Sina Weibo, Interest Tribe, Momo, PaiPai, WeChat, and MiLiao. Expert scoring was used to judge the risk level of mobile APP user privacy leakage, with a score range of 1-10, where higher scores indicate higher risk levels corresponding to the indicator. To conduct the empirical study more objectively and scientifically, this study selected eight experts for questionnaire surveys and interviews, including four experienced internet development professionals and four mobile APP research scholars with associate professor titles or above. Table 2 shows the scoring results of the eight experts for each indicator.

4.2 Evaluation Process 4.2.1 Entropy Method for Determining Objective Weights

Through Formula (1) and Formula (2), the original matrix was standardized and normalized to obtain the matrix. Using Formula (3) to determine the information entropy of each indicator, the weight v_j can be calculated through Formula (4):

v_j = (0.0462, 0.0303, 0.0360, 0.0493, 0.0509, 0.0621, 0.0544, 0.0360, 0.0465, 0.0469, 0.0303, 0.0290, 0.0408, 0.0476, 0.0303, 0.0388, 0.0494, 0.0461, 0.0331, 0.0307, 0.0367, 0.0575, 0.0714)

4.2.2 ANP for Determining Subjective Weights

When using SuperDecisions software for calculation, the mutual influence relationships among element groups were first determined, as shown in Figure 1 [Figure 1: see original paper], where arrows indicate influence relationships. Taking element group C1 as an example, this group influences itself (for instance, a user's erroneous operation may lead to every subsequent operation being wrong) and also influences element group C4 (for example, users' poor network usage

habits make illegal attacks by hackers easier, causing more privacy information theft by illegal elements).

Then, judgment matrices were constructed in the software, as shown in Figure 2 [Figure 2: see original paper]. Taking element group C2 as the main criterion and element C23 as the secondary criterion, elements in element group C2 were compared pairwise and scored to judge importance levels. For example, in this case, element C21 is more important than element C24, with a relative importance of 5.

Repeating this step until all judgment matrices were provided, the weight u_j was obtained:

u_j = (0.0215, 0.0153, 0.0214, 0.0261, 0.0387, 0.0450, 0.0127, 0.0202, 0.0095, 0.0798, 0.1049, 0.0508, 0.0794, 0.1238, 0.0677, 0.0199, 0.0495, 0.0877, 0.0102, 0.0200, 0.0225, 0.0264, 0.0475)

4.2.3 Determining Combined Weights

Combined weights w_j were calculated according to Formula (5), with results shown in Table 3 .

4.2.4 Fuzzy Comprehensive Evaluation Method for Judging APP Risk Levels

Taking WeChat as an example, the evaluation process of the fuzzy comprehensive evaluation method is demonstrated. Table 4 shows the indicator weights and expert survey results for the WeChat APP.

Based on the data in Table 4, the fuzzy evaluation matrix can be calculated. According to the weights of each indicator, fuzzy comprehensive transformation of matrix R yields the fuzzy comprehensive evaluation index.

Establishing an alternative set for assignment of evaluation results:
V = {High risk, Higher risk, Medium risk, Lower risk, Low risk} = (9, 7, 5, 3, 1)

The final comprehensive membership degree is 4.7070. Overall, the survey indicates that the risk level of privacy leakage for this APP user is between lower risk and medium risk, closer to medium risk.

Using the same method, the comprehensive membership degrees of other APPs can be calculated. The comprehensive membership degrees of Sina Weibo, Interest Tribe, Momo, PaiPai, and MiLiao are 4.9110, 4.8903, 5.4230, 5.5156, and 4.8534, respectively. According to membership degree size, the risk levels of each APP from high to low are: PaiPai > Momo > Sina Weibo > Interest Tribe > MiLiao > WeChat.

4.3 Discussion and Analysis 4.3.1 Primary Indicator Discussion and Analysis

Results show that among primary indicator weights, the most important is "privacy information leakage risk caused by mobile APP platform reasons

(C2)," followed by "privacy information leakage risk caused by user reasons (C1)," "privacy leakage risk caused by management reasons (C3)," and "privacy information leakage risk caused by other reasons (C4)." This data indicates that in mobile user privacy information leakage risks, platform developers should strengthen platform function settings, request authorizations within normal business scope, and simultaneously establish corresponding user information confidentiality management systems and information leakage accountability mechanisms internally. They should also adopt appropriate security key technologies to avoid external hacker or virus intrusions due to technical reasons, thereby preventing consumer privacy information leakage caused by platform reasons. Users should strengthen privacy protection awareness and carefully disclose personal information. Industry regulatory departments should also issue corresponding industry regulatory systems or legislation on consumer personal privacy leakage to strengthen supervision of platform developers at the national institutional level.

4.3.2 Secondary Indicator Weight Analysis

To better understand the risk levels of secondary indicators with different weights and enable managers to focus on relatively important risks, secondary risk indicators are classified into risk levels based on their weight sizes. Combining relevant literature [**?**] and the specific situation of mobile social APP user privacy leakage risk, according to the combined weight results of each indicator, secondary risk indicators are divided into four levels: weights above 0.65 are extreme risk, weights between 0.5-0.65 are high risk, weights between 0.3-0.5 are medium risk, and weights below 0.3 are low risk.

Based on evaluation results, there are 3 extreme risks: "inadequate mobile APP risk prevention technology," "lack of supervision and punishment system," and "unreasonable mobile APP function settings." There are 5 high risks: "purchasing privacy information from third-party platforms," "malicious leakage of information by mobile APP internal personnel," "excessive permission requests by mobile APP," "users' overly optimistic attitude toward privacy information," and "imperfect mobile APP user privacy information disclosure standards."

Secondary indicator data analysis results show that in addition to APP platforms' strict self-discipline, functional improvement, and technological enhancement, relevant departments should issue relevant policies and regulations, such as APP user privacy disclosure standards and authorization request standards, to prevent user privacy leakage. The government should also increase punishment for malicious privacy leakage behaviors and regulate personal privacy information usage behaviors. Users should also improve their own privacy protection awareness and vigilance.

4.3.3 Mobile Social APP User Privacy Information Leakage Risk Analysis

Among the six selected APPs, WeChat has the lowest user privacy leakage risk level, while PaiPai has the highest. From a categorical perspective, instant messaging social APPs have the lowest risk level, stranger social networking

APPs have the highest risk level, and traditional SNS social APPs are in the middle. Moreover, generally among the same type of APPs, APPs with higher usage have slightly lower user privacy leakage risk than those with lower usage, because more popular APPs have longer development times, richer construction and operation experience, more adequate risk prevention measures, and stronger awareness of protecting user privacy information, so their risk levels are relatively lower.

In interviews, experts were mainly asked which risk indicators they considered more important and the performance issues of each important indicator on different mobile APPs. Interview results basically covered most extreme and important risk indicators in the empirical analysis. Compared with questionnaire survey data, interview results are somewhat more ambiguous but can also provide much information. For example, for "unreasonable mobile APP function settings," Sina Weibo and Tantan may have slightly stronger risk performance, while for "excessive permission requests by mobile APP," the performance of several APPs is roughly similar. Verification shows that these six APPs all obtain about 10 permissions, with little difference. Therefore, the risk level of different indicators may be similar or significantly different across different APPs.

In response to the above situation, users should improve their vigilance, especially when using stranger social networking APPs, and be more cautious about disclosing personal information to enhance privacy protection awareness. From the APP perspective, mobile APP platforms should improve their capabilities, improve functions and basic settings according to their own APP characteristics, focus on improving high-risk indicators based on actual conditions, strengthen internal management, enhance staff quality and moral standards, and regularly update and improve user privacy leakage risk prevention technologies to ensure user privacy information security.

5. Research Conclusions

The theoretical value of this study lies in constructing a mobile APP user privacy leakage risk evaluation index system based on influencing factors of mobile APP user privacy information leakage and conducting risk evaluation on mobile social APP user privacy information leakage. The paper establishes an index system with 4 dimensions and 23 secondary indicators. On this basis, ANP and entropy methods are used to determine subjective and objective weights respectively, and then combined weights of each indicator are calculated, achieving complementary advantages of the two methods and providing methodological support for mobile APP user privacy leakage risk evaluation.

The practical value of this paper lies in selecting mobile social APPs for empirical analysis. Primary indicator data analysis results show that privacy leakage risk caused by APP platform reasons is the highest, followed by user reasons, management reasons, and other reasons. Secondary indicator data analysis results

show 3 extreme risks: “inadequate mobile APP risk prevention technology,” “lack of supervision and punishment system,” and “unreasonable mobile APP function settings.” There are 5 high risks: “purchasing privacy information from third-party platforms,” “malicious leakage of information by mobile APP internal personnel,” “excessive permission requests by mobile APP,” “users’ overly optimistic attitude toward privacy information,” and “imperfect mobile APP user privacy information disclosure standards.”

Empirical analysis results of mobile social APPs show that risk levels vary among several APPs, but all are close to medium risk level, indicating that privacy leakage risks when users use social APPs cannot be ignored. Moreover, overall risk levels differ among different types of social APPs. More popular APPs have relatively lower risk levels. In this situation, mobile APP platforms, users, and regulatory departments should work together to take corresponding measures according to different APPs’ specific circumstances to reduce privacy leakage risks for social APP users during use.

This study only conducted user privacy risk evaluation analysis on six social APPs, which has certain limitations in sample selection. In subsequent research, the authors will conduct comparative analysis of privacy disclosure risks among different types of APPs and detailed comparative analysis of representative APPs in each category.

References

[1] Luo Li. Research on personal information security risks and governance of mobile internet users in China[J]. Library Science Research, 2016(13): 37-41.
[2] Li Lina. On how to strengthen the legal protection system of privacy rights in China[D]. Yanji: Yanbian University, 2006.
[3] Zhang Jun, Xiong Feng. Overview of network privacy protection technology[J]. Computer Application Research, 2005(7): 9-11, 28.
[4] ZHU K, HE X M, XIANG B, et al. How dangerous are your smartphones? app usage recommendation with privacy preserving[J]. Mobile information systems, 2016(4/5): 1-10.
[5] BANSAL G, ZAHEDI F M, GEFEN D. Do context and personality matter? trust and privacy concerns in disclosing private information online[J]. Information & management, 2016, 53(1): 1-21.
[6] LI Y. The impact of disposition to privacy, Website reputation and Website familiarity on information privacy concerns[J]. Decision support systems, 2014, 57(1): 343-354.
[7] MARTÍNEZ-PÉREZ B, DE LA TORRE-DÍEZ I, LÓPEZ-CORONADO M. Privacy and security in mobile health Apps: a review and recommendation[J]. Journal of medical systems, 2015, 39(1): 181-189.
[8] MILTGEN C L, SMITH H J. Exploring information privacy regulation, risks, trust, and behavior[J]. Information & management, 2015, 52(6): 741-759.
[9] Wang Xiwei, Xiang Mengmeng, Zhang Changliang, et al. Research trends and development directions of information privacy in the new media environ-

ment at home and abroad[J]. Library and Information Service, 2017, 61(15): 6-14.
[10] Li Zhuozhuo, Ma Yue, Li Mingzhen. Personal privacy information protection from the perspective of data lifecycle: content analysis of mobile APP service agreements[J]. Information Theory and Practice, 2016, 39(12): 63-68.
[11] Liu Jiao, Bai Jing. Comparative study of Chinese and foreign mobile APP user privacy protection texts[J]. Journal of Shantou University (Humanities & Social Sciences Edition), 2017, 33(3): 82-87.
[12] Zhu Guang, Feng Mining, Chen Ye, et al. Fuzzy evaluation research on social network privacy risks in big data environment[J]. Information Science, 2016, 34(9): 94-98.
[13] Wang Shan, Li Yongxian. Review of personal information protection research in China's big data era[J]. China Collective Economy, 2016(28): 54-55.
[14] Meng Xiaoming, He Minwei. Personal privacy protection in social network big data commercial development and utilization[J]. Library Tribune, 2015, 35(6): 67-75.
[15] Xu Xiaolu. Research on privacy security issues and protection of mobile social network users[D]. Chongqing: Chongqing University, 2014.
[16] Zhang Qiujin. Cloud computing privacy security risk assessment[D]. Kunming: Yunnan University, 2015.
[17] Zhu Yijie. Analysis and evaluation of privacy leakage risk in location-based services[D]. Guiyang: Guizhou University, 2016.
[18] Kuang Qingqing. Risk assessment based on personal privacy leakage[D]. Guiyang: Guizhou University, 2016.
[19] Shen Hongzhou, Tang Xueting, Zhou Ying. Research on usability of privacy protection functions of mobile social media in China[J]. Library and Information Service, 2017, 61(4): 23-30.
[20] Wang Na, Xu Dachen. Investigation and analysis of personal information protection status in mobile social networks: from the perspective of user behavior habits[J]. Journal of Intelligence, 2015, 34(1): 185-189, 194.
[21] Cheng Yao, Ying Lingyun, Jiao Sibeibei, et al. Research on user privacy leakage issues in mobile social applications[J]. Chinese Journal of Computers, 2014, 37(1): 87-100.
[22] Qi Xiaona, Zhang Yujing, Feng Erying. Research on user privacy protection issues in mobile social networks[J]. Industry and Technology Forum, 2017, 16(16): 35-36.
[23] Wang Lianfen. Theory and algorithm of Analytic Network Process (ANP)[J]. Systems Engineering Theory & Practice, 2001(3): 44-50.
[24] Luo Qian, Xia Jingbo, Chen Tianping. Comparison of objective weight determination methods in network performance evaluation[J]. Computer Applications, 2009, 29(10): 2624-2626, 2631.
[25] Zheng Xiaoyun, Wang Yu. Integrity evaluation of real estate development enterprises based on AHP and entropy method[J]. Shanxi Architecture, 2016, 42(2): 213-214.
[26] Wang Shuyi, Zhu Na. Research on privacy protection countermeasures for mobile social media users[J]. Information Theory and Practice, 2013, 36(7):

36-40.
[27] Li Minggao. Application analysis of information security risk assessment in information security system construction[J]. Computer & Telecommunication, 2009(1): 83-85.

Author Contributions

Tian Bo: Proposed research ideas and framework, wrote and revised the paper.
Zheng Yusha: Wrote and revised the paper.
Liu Pengyuan: Responsible for data collection, processing, and calculation.
Li Chunhao: Responsible for index system establishment and analysis.

Note: This journal welcomes innovative academic research results in theory, methods, technology, practice, etc., and research results supported by projects such as the National Social Science Fund, National Natural Science Fund, and Ministry of Education. The topic guidelines of the National Social Science Fund and this journal in recent years still have reference value and guidance.

Library and Information Service Journal 2018 Topic Guidelines

1. Mission and responsibility of libraries in cultural power construction
2. Reconstruction of library and information science knowledge system in the big data era
3. Research on relevant laws, regulations, and systems in library and information field
4. Research on balanced and full development strategy of library and information undertakings
5. Libraries' capabilities and strategies for supporting "Double First-Class" construction
6. Construction of library metadata system in big data environment
7. Research on information user behavior and user profiling
8. Think tank research and think tank services
9. Resource discovery and new models of library resource construction
10. Digital literature and data management and long-term preservation
11. Library personalized and precise services

12. Digital humanities, digital heritage, and related technologies
13. Semantic technology, linked data, and knowledge organization
14. Artificial intelligence technology and its application in libraries
15. Development trends of intelligent everything and library service innovation
16. Library reading promotion theory and practice
17. Open data and information security policies
18. Library space reconstruction theory and practice
19. Libraries and digital publishing (library publishing)
20. Construction of library and information science theoretical system in the new era

Library and Information Service Magazine
December 2017

Note: Figure translations are in progress. See original paper for figures.

Source: ChinaXiv — Machine translation. Verify with original.