Privacy Management and Privacy Concerns in Social Media

Runting Li(✉)

Journalism Department, Guangzhou Huashang College, Guangdong 511300, China
runtingli1022@gmail.com

Abstract. This study focuses on the privacy issues in social media, analyzes the current privacy issues in terms of privacy management and privacy concerns, hoping to explore the relationship between the public's perceptions and behavioral levels in terms of privacy. The study proposes five hypotheses through literature analysis, and later collects relevant data by means of questionnaire collection and uses a form of structural equations to verify the hypotheses. The study concludes with platform and individual specific responses from the data studied.

Keywords: Social media · Privacy concerns · Privacy management

1 Introduction

As social media continues to integrate into people's daily lives, privacy-related issues are emerging and becoming the focus of discussion. At present, there is no unified view on the definition of social media, but some characteristics of social media are undeniable, such as strong sense of participation, real-time communication, strong community, strong connectivity and so on. As a platform for users to produce and exchange information content on the Internet, social media has gradually become an inseparable part of people's daily life. The emergence of social media has gradually dispersed the communication mode. The nodes of information dissemination spread all over the entire circulation network, and are easy to connect. This highly participatory, communicative, community-focused, and interconnected platform provides users with a virtual platform for self-presentation, information sharing, and interaction. At the same time, all users' behaviors in the Internet space are also recorded, forming an "unforgeable" online record, and all users' Internet behaviors can be traced back. With the constant infiltration of social media into people's daily life, privacy-related issues are gradually exposed and become the focus of discussion.

By deeply analyzing the privacy concerns of social media users, this paper enriches the research content of privacy issues, enhances the understanding of social media privacy issues, and improves the social media platforms and user privacy management methods, so as to reduce the occurrence of social media privacy issues.

G. Ali et al. (Eds.): ISEMSS 2022, ASSEHR 687, pp. 2956–2964, 2022.
https://doi.org/10.2991/978-2-494069-31-2_348

2 Social Media and Privacy

China's first "2018 Netizens' Internet Security Satisfaction Survey Report" shows that the protection of online personal information has become one of the most urgent problems for Chinese netizens. Among them, it is worth noting that the chat content in social software is the most concerned issue of netizens, in addition to online shopping. Netizens generally believe that the risk of personal information being leaked when chatting in the software is greater. It can be found that in the current social media environment, users' concerns about social media privacy mainly stem from the following four privacy issues in social media.

2.1 Privacy Concerns of Low Platform Transparency and Low User Control

In the process of using social media, users often provide some personal information to obtain services, such as personalized push by providing personal interest and hobby information. This will lead to the low transparency of the current platform in the use of user information, and bring a great sense of insecurity to users. On the other hand, it is also difficult for users to control the personal information they have provided. In other words, users cannot control how personal information is used and whether it is used for a second time. This situation has aroused the high attention of netizens to the social media environment.

2.2 The Conflict Between User Creation and Privacy Concerns in Social Platforms

The platform encourages users to create user privacy anxiety is ignored, and privacy concerns are further stimulated. Even if the survey shows that users are highly concerned about information security issues in the network, social media platforms will not solve this concern and strengthen privacy management. The reason can be attributed to the fact that social media platforms are encouraging users to create, publish and even disclose their personal information. The motivation is that when users maintain a high level of content creation, they will bring more content to the platform. And increase the user traffic of the platform, not only from publishers, but also from viewers. This situation has created a conflict between user creation and privacy concerns. Specifically, on the one hand, users' social activities require social interaction and relationship maintenance, which requires users to publish, share or disclose some personal information through social media platforms. But on the other hand, the disclosure of personal information on social media to maintain relationships, leading to privacy disclosure is becoming more and more common [1].

2.3 The User Cannot Effectively Control the Recipient of the Sent Information

First of all, at the individual level, users cannot control the behavior of the information receiver after receiving the information, especially when the two sides have inconsistent definitions of the privacy of the same information, it is more difficult to grasp the problem

of privacy disclosure. Secondly, at the technical level, with the support of technology, the cost of information exchange between platforms is almost zero. After the private information is sent, the recipient of the information may spread the private information for various reasons or through different platforms, resulting in more extensive privacy violations. In addition, at the content level, the boundary between private information and public information is currently shifting, and it is becoming more and more difficult to control the boundary between private information and public information. Therefore, it's even harder for users to grasp the information transmission. After that, how does the other party understand where the boundary of the privacy is?

From the discussion of the above three issues, we can see that the focus of the privacy protection issues in current social media is still about the users themselves. It can even be considered the most solid and last wall of privacy security issues.

3 Analysis of the Relationship Between Privacy Management and Privacy Concerns

S. Petronio proposed the theory of communication boundary management (CPM) in 1991, which was renamed as "communication privacy management theory" in his book "The Boundaries of Privacy" in 2002 [2]. This theory is based on Altman's (2012) theory of privacy, which regards the boundary between the self and others or the public as the boundary, and regards the management of privacy as the control of the individual's "boundary" to achieve the best state of satisfaction through the control of boundary management [3]. Liu (2007), in explaining this theory, argues that this theory of communication privacy management is internally consistent and can be tested, and that we need a theory of communication privacy management to explain the invasion of privacy in everyday life due to technological advances, and to explain the rule-based management system that is part of this trend [4].

Communication privacy management theory achieves its goals through five basic assumptions, which are: private information, privacy boundaries, control and all, rule-based management system, and management dialectic.

3.1 Research Hypothesis

Based on the hypotheses proposed in the literature analysis, this study develops a model of the relationship between privacy concerns and privacy rules management in the social media environment. The "gender criterion," "environmental criterion," "risk-benefit criterion," "motivation criterion," and "cultural criterion" were used to measure privacy rule making in social media. "motivation criterion" and "culture criterion" to measure privacy rule establishment in social media. The IUIPC scale was used as the basis for privacy rule building, and "secondary use," "control," "collection," "perception," and "secondary use" were used as the basis. "and "secondary use" as variables, and privacy boundary management as the dependent variable.

H1 Gender of social media users significantly affects privacy concerns; H2 Social media environment standards significantly affect privacy concerns; H3 Risk-benefit significantly affects privacy concerns of social media users; H4 Cultural criteria significantly

Table 1: Results of Pearson correlation analysis of privacy rule building and privacy concerns

		collection	control	perception	secondary use
Environmental standard	Correlation coefficient	0.471**	0.525**	0.536**	0.464**
	sig	0.000	0.000	0.000	0.000
Risk-to-benefit ratio criteria	Correlation coefficient	0.498**	0.488**	0.491**	0.550**
	sig	0.000	0.000	0.000	0.000
Cultural Criteria	Correlation coefficient	0.536**	0.533**	0.553**	0.572**
	sig	0.000	0.000	0.000	0.000
Motivation Criteria	Correlation coefficient	0.541**	0.606**	0.608**	0.543**
	sig	0.000	0.000	0.000	0.000

**. Significant correlation at the 0.01 level (two-tailed)
Table Credit: Original

affect privacy concerns; H5 Motivation criteria significantly affect social media users' privacy concerns.

3.2 Privacy Rules and Privacy Concerns Relationship Test

In terms of relationship testing, this study used Pearson correlation analysis to examine the relationship between each element in privacy rule establishment and privacy concerns, and the test results are shown in.

Table 1 shows the results of Pearson correlation analysis for each dimension show that environmental criteria have a significant impact on collection, control, perception, and secondary use in privacy concerns. That is, the element of environment affects users' privacy concerns, and similarly, the risk-benefit ratio criterion, cultural criterion, and motivation criterion all have an impact on privacy concerns.

Although the test of hypothesis using correlation analysis found statistical significance between privacy rule establishment and each dimension of privacy concern, considering that in order to be able to verify the previously proposed hypothesis in further detail, this study conducted a structural equation analysis of the relationship model between the two using Amos 7.0v software based on the above results.

3.3 Structural Model Testing

Based on the theoretical model, this paper used the environmental dimension, risk-benefit dimension, cultural dimension, and motivation dimension established by privacy rules as dependent variables and privacy concerns as independent variables to build a structural equation model. The data from 517 questionnaires obtained in the large sample collection

Table2: Preliminary measurement model fit analysis results

d.f.	X2	RMSEA	SRMR	GFI	AGFI
367	1292.055	0.070	0.0351	0.848	0.819
NFI	NNFI	CFI	IFI	PGFI	PNFI
0.915	0.931	0.938	0.938	0.715	0.827

Table Credit: Original

Table 3. Fit analysis results of the modified measurement model

d.f.	X2	RMSEA	SRMR	GFI	AGFI
361	827.476	0.050	0.0367	0.902	0.882
NFI	NNFI	CFI	IFI	PGFI	PNFI
0.946	0.965	0.969	0.969	0.748	0.842

Table Credit: Original

were analyzed by AMOS software using maximum likelihood estimation method and the data were fitted.

The results of fitting the data using the maximum likelihood estimation method are shown in Table 2.

According to Wheaton (1977), when this value is less than 5, it is acceptable and therefore meets the statistical requirements. The RMSEA value is The RMSEA value is 0.070, according to Steiger (1990) this value is less than 0.01 which means that the model fits well, but in real empirical studies this indicator is difficult to achieve, and he points out that when this indicator is less than 0.1 it indicates that the model is a good fit. The SRMR value is 0.0351 which meets the requirement of less than 0.08. In addition, the NFI, NNFI, and IFI of the model are higher than 0.9, but the AFGI and GFI of the absolute fit indicators do not meet the statistical requirements and are less than 0.9, so the model needs to be corrected before analysis.

The fitted indices after the correction are shown in Table 3, and all values are optimized after the correction. The cardinality to degrees of freedom ratio is 2.29; the GFI is 0.969, which is greater than 0.9; the CFI is 0.969, which is greater than 0.9; and the NFI is 0.946, which is greater than 0.9. All are within the standard range. The parsimonious fit indices PGFI and PNFI were 0.748 and 0.842, respectively, which exceeded the requirement of needing to be greater than 0.5, thus implying that the overall fit of the model was good and the model could be analyzed.

3.4 Structural Model Hypothesis Testing

In this study, after revising and optimizing the model, the path coefficients between the variables were collated and analyzed to test the hypotheses presented in the previous section. The standardized coefficient between “environmental dimension” and “privacy

concern" is 0.198; the standardized coefficient between "risk-benefit ratio dimension" and "privacy concern" is 0.292. The standardized coefficient between the "risk-benefit ratio dimension" and "privacy concern" is 0.292; the standardized coefficient between the "culture dimension" and "privacy concern" is The standardized coefficient between "motivation dimension" and "privacy concern" is 0.246. The regression coefficient can be considered significantly non-zero when the t-test value is greater than 1.96 in the structural equation model hypothesis.

The analysis results showed that: the environmental criteria of privacy rule establishment in social media positively and significantly affect privacy concerns, H2 holds; the risk-benefit ratio criteria of privacy rule establishment in social media significantly affects privacy concerns, H3 holds; the cultural criteria of privacy rule establishment in social media significantly affects privacy concerns, H4 holds; the motivation of privacy rule establishment in social media significantly affects privacy concerns, H5 holds.

4 Countermeasures and Suggestions for Platforms and Individuals

In terms of social media, "opening and sharing" is the norm and implicit operating rules of social media. The uncertainty, high risk perception, and low transparency of the platform will greatly increase users' privacy concerns, which will greatly reduce users' willingness to disclose themselves on the platform. Social media loses the disclosure and sharing behavior of users, and may become an illusory resource that cannot run for a long time. Therefore, for the platform, to achieve long-term operation, it is necessary to reduce users' privacy concerns and privacy risk perception, and strive to build a secure and stable privacy environment for users to take the initiative to speak in the platform.

4.1 Social Media Should Pay Attention to the Privacy Experience of Users Within the Platform

Through the observation and analysis of the data, it can be found that users' awareness of privacy concerns in social media is relatively significant. "Exchanging privacy for benefits" is a common choice for current users, but people's concerns about privacy will not be reduced. In contrast, today's Internet companies are less concerned about users' privacy and security. At the China High-level Development Forum in 2018, Li Yanhong, Baidu CEO, said that "privacy is exchanged for efficiency and convenience". These comments are enough to reflect the current disregard of social media platform to the user's privacy experience. Therefore, based on the research results, social media operators should realize the importance of improving the privacy experience of users, and no longer restrict users simply by providing benefits, which will only consume users' experience and eventually make them leave the platform. These platforms can try to provide users with more comprehensive and detailed privacy protection measures by strengthening security technology and privacy encryption technology.

In terms of specific measures and suggestions, the application advantages of big data can be fully combined by using blockchain and new encryption technology to strengthen data security management. Blockchain technology has the characteristics of decentralization, point-to-point transmission, transparency, traceability, non-tampering,

and data security. However, account identity information can be highly encrypted through technology, so the introduction of blockchain technology can greatly improve the security of social media.

4.2 Social Media Platforms Should Refrain from Secondary Use of User Information

Social media users' daily social behavior will produce a lot of information, such as personal information, social relations, geographical location and so on. The gradual accumulation of information has formed a huge information database of the platform. There is no doubt that the mining of these data by social media platforms can create new value and better serve users, but this behavior also gave birth to the emergence of data transactions. For example, in March 2018, the information of more than 50 million users of Facebook, an American social networking site, was leaked, which was one of the largest user data leakage incidents since the establishment of social media. It is also reported that Twitter sold user data to Cambridge scholars. Recently, Victor Goff, a security researcher at the network security agency GDI Foundation, found that 364 million private chat records of Chinese users were leaked to the Internet, including WeChat payment records that are closely related to most people. These cases have stimulated users' privacy concerns. In addition, social media and their companies need to strictly abide by the regulations, respect users' right to know, and collect users' personal information only under the premise of users' authorization. Therefore, social media platforms should always exercise restraint and prudence when using user information. Under the premise of respecting users' right to know, information can only be reused after obtaining users' authorization.

4.3 Social Media Platforms Should Improve Functions and Provide Diversified Choices

The continuous use of users on the social media platforms is the result of the superposition and reinforcement of multiple behavioral motivations. However, previous analysis also points out that privacy issues still haunt users [5]. Therefore, the platform' functions should be as complete as possible, providing different users with options to alleviate users' privacy concerns through various optional and feasible functions.

In this regard, this study observed that "digital moderation" is gradually becoming the focus of attention, and many social media sites are already on the way to enrich the functions of digital moderation in the platform. In China, WeChat's three-day visible function, private visible function, QQ flash photos, and snoring bubble letters all reflect this situation. In addition, Alipay's "life circle" chat has recently added the "burn after reading" function. In foreign countries, Snaocha, as the representative of "burn after reading", has attracted a large number of young users since its launch in 2011. This platform 178 million users worldwide, where users share more than 2.5 billion personal pictures and videos every day. "Burn after reading" in this platform means that users can automatically destroy all chat records with their friends in a free time period (usually within 1–10 s). The content that can be destroyed includes text, pictures, and voice, videos and expressions, so the platform can better ensure the privacy and security of

users. The rise of such websites and the development trend of domestic social platform functions have demonstrated that "digital moderation" is becoming a new breakthrough in preventing privacy leakage, because "excessive performance" will lead to privacy disclosure.

5 Conclusions

Through previous research and empirical observation, this study found that in the current social media environment, the privacy problems in users' social media mainly stem from the following four points: 1) The low transparency of the platform and the low control rights of users have brought privacy concerns, 2) The contradiction between user creation and privacy concerns in social platforms, 3) Users cannot effectively control the recipients of their messages. Guided by privacy rule management theory and privacy concern theory, this paper studies the relationship between social media users' privacy rule management and privacy concern on the basis of analyzing the relevant data, and tries to put forward countermeasures and suggestions for the current privacy problems.

Acknowledgments. Thanks to the instructor, Professor Xuebo Zhang, and the respondents to the survey.

References

1. Ouyang Yang, Yuan Qinjian. A Review of Research on Privacy Concerns in the E-commerce Environment at Home and Abroad [J]. Information Science, 2016, 34 (7): 170-176.
2. PETRONIO S. Boundaries of Privacy [J]. State University of New York Press, Albany, NY, 2002.
3. O' Bien D, Torres A M. Social Networking and Online Privacy: Facebook Users' Perceptions[J]. Irish Journal of Management, 2012, 31(2): 63–97.
4. Liu, H. L., Translation. Beijing: People's University of China Press, 2007.
5. Barnes. S B. A Privacy Paradox: Social Networking in the Unit- ed States [J]. First Monday, 2006, 11(9): 1–14.[2]