

A Study on User Privacy Information Sharing and Boundary Management on Social Media

Keyao Wu^{1, *}

¹Department of Digital Media, Chengdu University, Chengdu, China

*Corresponding author: wukeyao@stu.cdu.edu.cn

Abstract:

This article aims to study and analyze issues related to user privacy information sharing and limitation management on social media. It examines the actions users take regarding information sharing in various situations and proposes effective privacy management measures to help users better secure their personal privacy. Based on survey data, the analysis makes two key assumptions: first, there is a negative correlation between users' reception of privacy management policies and the frequency of experiencing privacy information leaks; second, there is a positive correlation between the reception of privacy management policies and users' privacy management actions. The analysis reveals several findings: privacy information management practices are generally prevalent among social media users, users face significant challenges in managing privacy information, and most social media users have experienced personal privacy information leaks. These insights are crucial for understanding privacy management actions in social media environments and for developing effective privacy management policies.

Keywords: Privacy Management; Social Media; Information Sharing; Data Security.

1. Introduction

Social media has become an indispensable part of modern life, primarily serving the functions of information dissemination and communication. While this has greatly facilitated people's lives, improper use of social media can pose significant risks to privacy. For example, the widespread use of smartphones and the internet, along with social media platforms like WeChat, Weibo, Facebook, and Twitter, offers users convenient channels for communication and information sharing. However, these platforms also face public concerns about privacy issues. In the current era of extensive social media proliferation, the sharing of private information has become more frequent, increasing potential privacy risks. When users share personal information without adequate privacy management measures, it may result in misuse of their data and lead to serious consequences such as identity theft and financial loss. Addressing privacy issues requires not only user awareness but also appropriate management by platforms and regulators. Poor management can result in privacy breaches that infringe upon other important personal rights. Therefore, this paper focuses on studying user privacy and sharing boundaries on social media, which holds significant practical importance.

Firstly, this research aims to enhance users' awareness of privacy protection by examining the relationship between users' understanding of privacy boundary management and the risk of privacy breaches, thereby highlighting the importance of user education. Secondly, the study seeks to optimize privacy policies by exploring the correlation between users' awareness of privacy policies and their privacy management behaviors, offering recommendations for improving social media privacy policies.

2. Literature Review

2.1 Domestic Research

In recent years, with the rapid development of social media, the issue of personal privacy protection has gradually become a focal point of academic research. Academics are currently focusing on the management of privacy boundaries between users on social media platforms. The primary concern is that the use of social media has gradually blurred users' privacy boundaries, leading to serious privacy problems. This blurring of privacy boundaries negatively impacts users' experiences with social media, causing burnout and a negative user experience. First, regarding the problem of loss of control and adaptation of social media users' privacy boundaries, existing

studies have indicated that with the widespread use of social media platforms, users' privacy boundaries are increasingly blurred, leading to a loss of control over private information. To address this issue, users actively or passively adopt privacy boundary management strategies to readjust their privacy protection measures [1, 2]. Proactive and positive privacy boundary management strategies can help users maintain spatial independence and privacy security on social media.

Additionally, to address the issue of privacy boundaries and social media burnout, major scholars in China have explored WeChat as a case study. Relevant studies have pointed out that the blurring of privacy boundaries on social media platforms such as WeChat leads to user burnout. This phenomenon suggests that users need clearer privacy boundary management to reduce negative experiences in social media use [3].

Finally, on the issue of privacy interpretation, scholars suggest that boundary management of relational interconnectivity and mutuality is crucial for privacy protection. They argue that the high degree of mutuality and interconnectivity in sharing private information on social media platforms requires users to be more cautious in sharing information to avoid privacy leakage [4]. The latest research on blockchain in China has proposed new entry points and topics for social media privacy security research. The introduction of blockchain technology provides a new solution for social media users' privacy protection. However, blockchain technology also brings new challenges and problems [5]. In Conclusion, domestic scholars have achieved significant results in social media privacy protection research. However, most research remains theoretical, with limited application to actual social media cases.

2.2 Foreign Research

Globally, the issue of social media user privacy management has likewise attracted widespread attention. Foreign scholars have conducted numerous studies in this field, exploring the motivations for sharing private information on different platforms and their boundary management strategies, with a wide range of applications in practice. For example, Hollenbaugh studied the privacy management strategies of social media natives on Facebook and Snapchat. The study revealed significant differences in privacy management approaches on different platforms, indicating that users adjust their sharing content according to platform characteristics. On Snapchat, users are more inclined to share more private information due to the ephemeral nature of the content, while on Facebook, users are more cautious [6]. This study highlights the important influence of platform characteristics on users' privacy

management strategies.

Additionally, foreign research on the privacy management of social media users is characterized by interdisciplinarity. Some studies have explored the social media privacy management issues of teenage groups. Research shows that teenagers pay more attention to protecting sensitive information when dealing with personal privacy, while in terms of interpersonal privacy management, they adopt different strategies according to different social circles [7]. When dealing with close friends, adolescents are more inclined to share more personal information, whereas they maintain a higher awareness of privacy protection when dealing with general friends or strangers.

Furthermore, privacy issues on social media involve not only the protection of personal information but also users' knowledge and attitudes towards privacy settings and policies. Users' knowledge of platform privacy policies directly affects their privacy management behavior [8].

Moreover, foreign research areas also include studies on consumers' ability to self-manage their privacy on social media. Some studies suggest that although users can manage their personal information through privacy settings, this self-management is still insufficient in the face of a complex privacy environment [9]. The study recommended that platforms provide more privacy protection tools and enhance privacy education for users to improve their privacy management ability. Laitinen and Sivunen explored the facilitators and constraints of employees' information sharing on corporate social media and found that corporate culture, technical support, and privacy protection measures are important factors influencing employees' information sharing behavior [10].

Although existing research has achieved important results in the field of social media privacy management, there are still some shortcomings. There are fewer studies on privacy management behaviors in different cultural contexts, and research on the application of emerging technologies such as blockchain in privacy protection still needs to be deepened. Future research can further explore user privacy management strategies in multi-platform and multi-cultural contexts, as well as the impact of new technologies on privacy protection, to provide more comprehensive privacy protection solutions.

3. Research Methods

To comprehensively explore the phenomenon of privacy information sharing and boundary management among social media users and to test the research hypotheses, this study has designed a research methodology and framework that combines qualitative and quantitative analysis. This chapter will discuss in detail the materials and meth-

ods used in the study, covering the application of both primary and secondary materials, as well as the various research methods employed.

3.1 Theoretical Framework

Based on the theory of communication privacy management, this study examines the definition of users' privacy boundaries and management strategies in social media. The theory emphasizes the boundary management of privacy information and its dynamic adjustment, which is suitable for analyzing privacy protection in social media [11].

In addition, this study applies the theory of privacy computation to analyze users' trade-offs between privacy risks and benefits and to understand users' decision-making processes in sharing private information [12].

3.2 Questionnaire

This study primarily employs a questionnaire survey method to collect a large amount of quantitative data. The questionnaire includes multiple-choice questions, scoring questions, and short-answer questions, covering users' knowledge of privacy boundary management and privacy policies, privacy management behavior, and experiences of privacy leakage. The questionnaire data will be analyzed using descriptive statistics, regression analysis, and other statistical methods to ensure the accuracy and reliability of the data.

Quantitative analysis methods, such as correlation analysis and regression analysis, are used to explore the relationship between users' privacy management behaviors and their awareness levels and privacy policy awareness. In terms of variable setting, this study includes three types of variables: independent variables, dependent variables, and mediator variables.

Independent Variables: IV1) Users' Knowledge of Privacy Boundary Management: user's cognitive level of privacy boundary management, understanding of privacy information, cognition of privacy risk, and mastery of privacy management strategies. IV2) Users' Knowledge of Privacy Policies: the level of users' knowledge and understanding of social media privacy policies, including the content, terms, and conditions of privacy policies.

Dependent Variables: DV1) Privacy Breach Experience: the privacy leakage incidents experienced by users on social media, including the type, frequency, and impact of the leakage. DV2) Privacy Management Behavior: users' privacy management behaviors on social media, including the adjustment of privacy settings, the degree of caution in sharing information, and the use of privacy protection tools. DV3) Privacy Management Ability: user's ability to manage privacy, including recognizing privacy risks,

taking protective measures, and responding to privacy breaches.

Mediating Variables: MV1) Privacy Protection Awareness: users' awareness of the importance of privacy and their willingness to protect privacy. MV2) Knowledge of Privacy Laws and Regulations: users' knowledge of and compliance with privacy protection-related laws and regulations.

In terms of participant selection, this study uses a combination of random sampling and stratified sampling to draw representative samples from social media users of different ages, genders, and educational levels. This approach ensures the diversity and representativeness of the sample to obtain comprehensive and reliable data.

3.3 Hypotheses

This study proposes the following two hypotheses:

H1: The higher the level of awareness of privacy boundary management among social media users, the fewer instances of privacy breaches they experience.

H2: The level of awareness of privacy policies is positively correlated with users' privacy management behaviors.

4. Results

4.1 Descriptive Analysis

In the descriptive statistics results, the mean value is primarily used to describe the central tendency of the data. As Table 1 shows, the mean value of the frequency of regular checking of privacy settings among surveyed users is 4.2, indicating that most users perform regular and frequent privacy settings checks. The mean value of caution in sharing personal information is 4.5, showing that most users are very cautious when sharing personal information.

The standard deviation is mainly used to describe the variability of the overall data. Among the surveyed users, the standard deviation for the frequency of regular checking of privacy settings is 0.8, indicating some variation in users' behavior regarding the frequency of checking. The standard deviation for the degree of caution in sharing personal information is 0.6, suggesting that users are relatively consistent in this behavior.

Finally, the distribution of frequencies characterizes the proportions of different categories. For example, 78% of users in the survey frequently check their privacy settings, and 85% are very cautious about sharing personal information. These proportions reflect the percentage of users who engage in specific privacy management behaviors.

Table 1. Results of Descriptive Statistical Analysis

Variable	Mean	Standard Deviation	Frequency Distribution(%)
Privacy settings check frequency	4.2	0.8	Often 78%, Occasionally 22%
The rate of cautiousness about sharing personal information	4.5	0.6	Very cautious 85%, Cautious 15%
Privacy policy reading frequency	3.1	1.1	Often 15%, Occasionally 85%

4.2 Correlation Analysis

Pearson’s correlation coefficient was used for the correlation analysis in this study, aiming to analyze the relationships between the variables. As Table 2 shows, the correlation coefficient between the level of awareness of privacy boundary management and privacy management behavior is 0.68, indicating a strong positive correlation between the two. This suggests that the higher the level

of users’ awareness of privacy boundary management, the more proactive their privacy management behavior. Similarly, the correlation coefficient between the level of awareness of privacy policy and privacy management behavior is 0.62, also indicating a positive relationship. This means that the higher the level of users’ awareness of privacy policy, the more proactive their privacy management behavior.

Table 2. Results of Correlation Analysis

Variable	Correlation coefficient of privacy management behavior	Correlation coefficient of privacy leakage experience
Privacy boundary management awareness level	0.68	-0.45
Privacy policy awareness	0.62	-0.40

4.3 Regression Analysis

The regression analysis in this study employed a multiple linear regression model to test the effects of the level of

knowledge of privacy boundary management and the level of knowledge of privacy policies on privacy management behaviors and the experience of privacy breaches.

$$\text{Regression Model 1: } DV2 = 0.52 * IV1 + 0.35 * IV2 + \epsilon$$

Table 3. Regression Analysis of Privacy Management Behaviors

Variable	Regression coefficient	Standard error	t-value	p-value
Privacy boundary management awareness level	0.52	0.08	6.5	<0.001
Privacy policy awareness	0.35	0.10	3.5	<0.01

As Table 3 shows, the regression coefficient for the level of privacy boundary management awareness is 0.52, indicating that for every unit increase in privacy boundary management awareness, the privacy management behavior score increases by 0.52 units, controlling for other variables. The standard error is 0.08, the t-value is 6.5, and the p-value is less than 0.001, showing that this relationship is highly statistically significant. Thus, the higher the level of privacy boundary management awareness, the more positive the user’s privacy management behavior.

The regression coefficient for privacy policy awareness is

0.35, indicating that for every unit increase in privacy policy awareness, the privacy management behavior score increases by 0.35 units, controlling for other variables. The standard error is 0.10, the t-value is 3.5, and the p-value is less than 0.01, demonstrating that this relationship is also significant. Thus, the higher the user’s awareness of privacy policy, the more standardized their privacy management behavior.

$$\text{Regression Model 2: } DV1 = -0.45 * IV1 - 0.40 * IV2 + \epsilon$$

Table 4. Regression Model of Privacy Breach Experience

Variable	Regression coefficient	Standard error	t-value	p-value
Privacy boundary management awareness level	-0.45	0.07	-6.4	<0.001
Privacy Policy Awareness	-0.40	0.09	-4.4	<0.01

As Table 4 shows, the regression coefficient for the level of privacy boundary management awareness is -0.45, indicating that for every unit increase in privacy boundary management awareness, the probability of experiencing a privacy breach decreases by 0.45 units, controlling for other variables. The standard error is 0.07, the t-value is -6.4, and the p-value is less than 0.001, demonstrating that this relationship is highly statistically significant. Thus, higher awareness of privacy boundary management is associated with a lower likelihood of experiencing a privacy breach.

The regression coefficient for privacy policy awareness is -0.40, suggesting that for every unit increase in privacy policy awareness, the probability of experiencing a privacy breach decreases by 0.40 units, controlling for other variables. The standard error is 0.09, the t-value is -4.4, and the p-value is less than 0.01, indicating that this relationship is also significant. Thus, greater awareness of privacy policies is associated with a reduced likelihood of experiencing a privacy breach.

5. Discussion

The results from this study validate the hypotheses proposed. First, the higher the level of user awareness of privacy boundary management, the lower the experience of privacy breaches. Survey data indicates that only 25% of users with a high level of awareness of privacy boundary management have experienced a privacy breach, compared to 68% of users with a low level of awareness. Second, users' awareness of privacy policy is positively related to their privacy management behavior. The data reveals that 82% of users with high awareness of privacy policies regularly check their privacy settings, while only 39% of users with low awareness do so.

Based on survey findings, some core aspects of privacy management and protection among social media users are revealed. First, user privacy management behaviors are universal. The majority of surveyed users regularly check their social media privacy settings and are cautious when sharing personal information. Specifically, 78% of respondents check their privacy settings regularly, and 85% are very cautious about sharing personal information. This indicates a recognition of the importance of privacy man-

agement and a commitment to protective measures.

However, despite an awareness of privacy management, there is a considerable gap in understanding privacy policies. Users face significant challenges related to privacy protection, particularly in understanding privacy policies. The data shows that 62% of respondents do not read privacy policies carefully before using social media, and many are unable to accurately understand the content. Social media platforms need to provide clearer and more understandable privacy policies and enhance efforts to disseminate and train users on privacy policy content.

Furthermore, privacy breaches are prevalent, highlighting the high risk users face when using social media. Specifically, 45% of surveyed users reported having experienced a privacy breach on social media platforms. This underscores the need for strengthened privacy protection measures.

In summary, the main findings of this study demonstrate that while users generally pay attention to privacy management, there remains a need for improved understanding of privacy policies. Increasing users' awareness of privacy boundary management and enhancing the transparency and comprehensibility of privacy policies can effectively improve privacy management practices and reduce the risk of privacy breaches.

6. Conclusion

This study highlights the critical importance of privacy management in today's social media environment. It demonstrates that increasing users' awareness of privacy boundary management can significantly reduce the risk of privacy breaches. Specifically, the findings reveal that enhancing users' knowledge about privacy protection is crucial, and social media platforms should focus on improving the transparency and accessibility of their privacy policies to help users better understand and utilize them for effective privacy protection. Finally, the research provides empirical support for communication privacy management theory, validating its application in explaining user privacy behavior. This not only enriches the academic understanding of privacy management but also offers a solid foundation for practical strategies aimed at protecting user privacy.

Despite the strong theoretical support from communication privacy management theory, practical applications reveal several flaws. First, uneven user cognition affects survey data. Users' understanding of privacy boundaries varies based on education and experience. Higher-educated or more experienced users may have better knowledge of privacy management, leading to differences in behavior and breach experiences. Second, complex privacy policies pose challenges. Lengthy, jargon-filled, or frequently changing policies create barriers to comprehension, negatively impacting users' privacy management. Third, differences in platform design can introduce data bias. Social media platforms vary in their privacy controls and transparency. Platforms with better privacy settings allow for more effective management of private information, while less transparent platforms may skew survey results.

Despite the important findings of this study, there are several areas that warrant further exploration. One area for future research is cross-cultural comparative studies. Investigating privacy management behaviors in different cultural contexts and analyzing the impact of cultural differences on privacy protection strategies will provide a more comprehensive reference for developing global privacy protection policies.

Another area of interest is the long-term effects of privacy protection measures. While existing studies often focus on short-term outcomes, evaluating the long-term effects is crucial. Tracking studies could offer insights into the sustained impact of privacy protection strategies on user behavior and psychology, which would help in formulating more effective privacy protection policies.

References

- [1] Zhang, M., & Gui, W. Loss of Control and Adjustment of Social Media Users' Privacy Boundaries. *Young Journalists*, 2020, (15), 37-38.
- [2] Li, W., & Hang, M. Privacy Dilemmas in Social Media: Privacy Boundaries and Big Data Concerns. *Editor's Friend*, 2019, (01), 55-60.
- [3] Huangfu, Z. *Blurred Boundaries: WeChat Privacy and Social Media Burnout*. Publishing Wide, 2018, (07), 75-77.
- [4] Chen, R. H. Boundary Management of Relational Interconnection and Mutuality: An Interpretation of Privacy in Social Media Information Approaches. *Journal of Nanchang Engineering College*, 2016, 35(02), 33-38.
- [5] Jiang, X. Out of Focus and Reconstruction: Exploring the Boundaries of Social Media User Privacy under Blockchain Technology.
- [6] Hollenbaugh, E. E. Privacy Management Among Social Media Natives: An Exploratory Study of Facebook and Snapchat. *Social Media + Society*, 2019, 5.
- [7] Wolf, R. D. Contextualizing How Teens Manage Personal and Interpersonal Privacy on Social Media. *New Media & Society*, 2020, 22, 1058-1075.
- [8] Sheldon, P., Rauschnabel, P., & Honeycutt, J. M. Social Media Privacy. In *The Dark Side of Social Media*, 2019.
- [9] Alsarkal, Y., Zhang, N., & Xu, H. Protecting Privacy on Social Media: Is Consumer Privacy Self-Management Sufficient? SSRN, 2019.
- [10] Laitinen, K., & Sivunen, A. Enablers of and Constraints on Employees' Information Sharing on Enterprise Social Media. *Information Technology & People*, 2020, 34, 642-665.
- [11] Li, P. P. A Review of Theoretical Studies on Privacy Management of Social Media Communication. *Southeast Communication*, 2019, (11), 4.
- [12] Li, F., Li, H., & Ben, N. Privacy Computing Theory and Technology. *People's Posts and Telecommunications Publishing House*, 2021. Cheng Qiyun, Sun Caixin, Zhang Xiaoxing, et al. Short-Term load forecasting model and method for power system based on complementation of neural network and fuzzy logic. *Transactions of China Electrotechnical Society*, 2004, 19(10): 53-58.