

# Construction and Empirical Validation of an Influence Model for Social Media Users' Information Disclosure Intention: A Case Study of WeChat Users (Postprint)

**Authors:** Guo Hailing, Ma Hongyu, Xu Zehui

**Date:** 2023-07-26T00:00:00+00:00

## Abstract

[Purpose/Significance] Frequent information privacy leakage incidents on social media have exacerbated users' concerns regarding information privacy, and users' willingness to disclose personal information to platforms during social media usage has become critical for promoting the healthy development of social media platforms. [Method/Process] Using privacy calculus theory and communication privacy management theory as a framework, combined with privacy concerns, this study constructs an influence model of social media users' information disclosure willingness. Taking WeChat as an example, sample data were collected through questionnaire surveys, and Smart PLS software was used to verify the model's rationality. [Results/Conclusion] The study finds that perceived benefits, trust, and perceived information control all positively influence information disclosure willingness, while privacy concerns negatively influence information disclosure willingness; trust negatively influences perceived risk; perceived information control negatively influences privacy concerns; privacy tendency positively influences both privacy concerns and perceived risk.

## Full Text

## Preamble

**ChinaXiv Collaborative Journal**

Volume 63, Issue 15, August 2019

**Construction and Empirical Validation of an Influence Model for Social Media Users' Information Disclosure Intention: A Case Study of WeChat Users**

Guo Hailing, Ma Hongyu, Xu Zehui  
School of Management, Hebei University, Baoding 071002

## Abstract

**[Purpose/Significance]** Frequent information privacy leakage incidents on social media have intensified users' concerns about information privacy. Users' willingness to disclose personal information to platforms during social media usage has become critical to promoting the healthy development of social media platforms. **[Method/Process]** This study constructs an influence model for social media users' information disclosure intention by integrating privacy calculus theory and communication privacy management theory with privacy concerns. Using WeChat as a case study, sample data were collected through questionnaire surveys, and SmartPLS software was employed to validate the model's rationality. **[Result/Conclusion]** The findings reveal that perceived benefits, trust, and perceived information control positively influence disclosure intention, while privacy concerns negatively affect it. Trust negatively influences perceived risk; perceived information control negatively influences privacy concerns; and privacy tendency positively influences both privacy concerns and perceived risk.

**Keywords:** social media, privacy calculus, communication privacy management, information privacy, disclosure intention

**Classification Number:** G203

**DOI:** 10.13266/j.issn.0252-3116.2019.15.013

Social media platforms, as content production and exchange systems built upon user social relationships, have achieved rapid development by relying on data and information disclosed by users. However, in recent years, privacy incidents involving personal information leakage and illegal use have occurred frequently. The 2018 data breach at Facebook, the world's largest online social network, reignited industry and academic discussions about user information privacy. On one hand, social media platforms need to accurately understand users' complex privacy needs; on the other hand, while encouraging users to disclose information, these platforms must also provide adequate protection and respect for user privacy. Therefore, analyzing the process of user information disclosure has become essential. Communication privacy management theory explains this process by achieving a balance between privacy disclosure and concealment through boundary control. The formation of privacy boundaries is influenced not only by users' perceived risks and benefits in privacy calculus but also by factors such as individual privacy control and trust. To comprehensively investigate the specific factors affecting users' information disclosure intention, this study examines the privacy boundary between user information disclosure and concealment, focusing on WeChat—the most active domestic social media platform with distinct strong-tie characteristics. Based on classic privacy calculus theory and communication privacy management theory, combined with privacy

concerns, we construct an influence model for social media users' disclosure intention and validate its effectiveness through empirical research. This research holds significant importance for helping businesses reasonably obtain and utilize user information to provide quality services.

Current domestic and international scholars have primarily studied social media privacy disclosure from the perspectives of platforms or individual user behaviors, employing theoretical frameworks such as the theory of planned behavior, privacy calculus theory, construal level theory, and communication privacy management theory. Among these, privacy calculus theory is the most commonly used theoretical model in information disclosure research. However, recent studies increasingly indicate that social media users' information disclosure intention does not fully conform to privacy calculus outcomes. As a valuable supplement to the privacy calculus model, communication privacy management theory offers an alternative perspective for explaining the user disclosure process.

## 2. Theoretical Foundations

### 2.1 Privacy Calculus Theory

Privacy calculus theory was first proposed by R.S. Laufer and M. Wolfe in 1977 and has gradually developed since then. The theory posits that when disclosing information, users conduct a cost-benefit analysis, only engaging in disclosure when perceived benefits outweigh risks. After more than a decade of development, academic research on privacy calculus theory has matured and been widely applied across various contexts, including e-commerce, social media, and healthcare. Studies show that despite sharing the same theoretical framework, users exhibit different disclosure intentions across different contexts. WeChat is primarily based on strong-tie social networks, where strong-tie groups serve as both important sources of information acquisition and major sources of privacy leakage. This study selects WeChat as the research object to analyze individuals' privacy decision-making processes when weighing perceived benefits against perceived risks on social media platforms.

### 2.2 Communication Privacy Management Theory

Communication Privacy Management Theory (CPM), proposed by S. Petronio in 1991, is a systematic framework for studying users' decisions to disclose or conceal personal information. The theory suggests that a privacy boundary exists between private and public domains, and this boundary is crucial for protecting personal information. Privacy tendency, as a primary factor influencing boundary rule formation, reflects individuals' inherent needs to manage the openness and closure of their privacy boundaries, defined as their general propensity to preserve information privacy space or restrict personal information disclosure. Individuals with higher privacy tendency are more concerned about personal boundaries and require greater control over personal information. Additionally, control and trust—two core elements of CPM—also influ-

ence privacy boundary formation. Control can be understood as users' grasp of privacy boundaries, manifested on social media as users' perceived ability to control disclosed information according to their own wishes. In practice, an increasing number of social media platforms have provided more detailed privacy control permissions, though the true intentions behind these permissions have been questioned. To verify their specific impact on users' information disclosure intention, this study introduces the variable of information control. Given that the research focuses on disclosure intention, and scholars have noted that perceived control is more important than actual control for attitudinal intentions, the model selects perceived information control—a subjective perception of actual information control based on psychological states. Furthermore, trust as a psychological belief helps break down privacy boundaries; higher trust leads to more open privacy boundaries and affects disclosure intention. In social media platforms with strong user interaction, content expression is largely based on trust and privacy, making CPM equally applicable to WeChat.

### 2.3 Privacy Concerns

Privacy concerns, introduced by information systems expert H.J. Smith et al. in 1996, are defined as “concerns arising from potential information loss.” This concept represents users' subjective awareness and feelings about privacy situations involving personal matters, revealing decision-making behavior through privacy value assessment under various influencing factors. As a multidimensional concept, H.J. Smith categorized privacy concerns into four dimensions: collection, errors, unauthorized secondary use, and improper access. N.K. Malhotra et al. argued that Internet privacy concerns include three dimensions: collection, control, and awareness. Due to social media's high user engagement, sociality, and openness, this study investigates the mechanism of privacy concerns in the process of personal information disclosure on social media platforms.

## 3. Research Hypotheses and Model Construction

### 3.1 Perceived Risk

Perceived risk is defined as the potential loss individuals perceive when disclosing information to relevant parties. Due to uncertainties regarding information itself and information recipients, personal information disclosed on social media platforms may be misused by malicious actors, increasing disclosure risks. On social media platforms, perceived risk primarily manifests as internal leakage and trafficking of information, unauthorized access, theft, and use. R. Chen et al. found that higher perceived risk leads to more negative personal information disclosure intention among social network users. P.A. Norberg noted that perceived risk significantly negatively affects privacy disclosure intention when studying the privacy paradox. N. Hajli et al. discovered that perceived risk negatively influences users' information disclosure attitudes on platforms like Facebook, Twitter, and LinkedIn. Therefore, we hypothesize:

**H1:** Perceived risk negatively affects information disclosure intention.

### 3.2 Perceived Benefits

Perceived benefits are defined as the favorable values individuals perceive after information disclosure, including economic benefits, personalized services, and social integration. On social media platforms, perceived benefits mainly derive from the pleasure and sense of integration gained through information sharing with other users. H. Krasnova et al. studied information disclosure behavior across cultures and found that despite cultural differences, perceived benefits positively and significantly affect disclosure intention. Li Gang demonstrated that perceived benefits positively influence users' disclosure attitudes on Sina Weibo. T. Wang et al. found that perceived benefits correlate positively with users' information disclosure intention when studying personal information disclosure through mobile applications. Therefore, we hypothesize:

**H2:** Perceived benefits positively affect information disclosure intention.

### 3.3 Trust

Trust is a crucial factor in social relationships, playing a significant role in the uncertain Internet environment. When users trust service providers, they believe social media platforms care about user interests, leading to dependence and willingness to disclose personal information. Lan Xiaoxia noted that college students' trust in mobile social environments primarily comes from social networking sites and their users. Li Qi et al. found that trust in WeChat platforms positively affects self-disclosure intention, though this effect was not significant in Weibo environments. R. Chen, based on social capital theory, constructed a model of self-disclosure intention among social network users, analyzing Facebook users and finding that trust in other members positively influences disclosure behavior. This study argues that when users trust social media platform operators and other users, they unconsciously lower self-protection awareness, expand privacy boundaries, and increase disclosure intention. Therefore, we hypothesize:

**H3:** Trust positively affects information disclosure intention.

Trust refers to users' belief that the other party will not engage in opportunistic behavior. Perceived risk is a primary obstacle to information disclosure, while trust can reduce this perceived risk. C. Moorman et al. argued that trust reduces perceived uncertainty, thereby lowering perceived risk. S.L. Jarvenpaa and N. Tractinsky found that perceived trust negatively affects perceived risk in cross-cultural online retail contexts. Therefore, we hypothesize:

**H4:** Trust negatively affects perceived risk.

### 3.4 Privacy Concerns

Privacy concerns represent awareness and perceptions associated with privacy leakage, reflecting subjective feelings in specific privacy situations. Research shows that personal information disclosure intention decreases as privacy concerns increase. For instance, Zhu Hou et al. found that privacy concerns negatively affect users' disclosure intention in social networks. K. Yang discovered that concerns about personal medical privacy lead users to withhold or provide false medical information when studying online medical service systems. Therefore, we hypothesize:

**H5:** Privacy concerns negatively affect information disclosure intention.

Privacy concerns reflect individuals' inherent worries about potential information loss and influence user trust. For example, N.K. Malhotra noted that Internet privacy concerns negatively affect trust-related beliefs. Zhang Xiaojuan et al. also found that stronger privacy concerns among smartphone users lead to lower trust in smartphones. Therefore, we hypothesize:

**H6:** Privacy concerns negatively affect trust.

### 3.5 Perceived Information Control

Perceived information control represents the ease with which users perceive their ability to control personal information on social media platforms. When individuals have more resources or opportunities to execute information disclosure control behaviors, their perceived information control level increases. Enhancing users' control over personal information can weaken privacy concerns to some extent. Zhang Huiping et al. found that users' perceived information control negatively affects their privacy concerns after empirically analyzing factors influencing WeChat users' privacy concerns. Therefore, we hypothesize:

**H7:** Perceived information control negatively affects privacy concerns.

Once personal information is uploaded to social media platforms, information subjects lose partial control over privacy information and can only passively accept platform operators' control, bearing the risk of privacy violations at any time. Higher perceived information control means users can better determine the type and scope of information disclosure, which can limit or even eliminate risks from privacy leakage. N. Hajli et al. found that stronger perceived information control leads to lower perceived risk among users of Facebook, Twitter, and LinkedIn. Therefore, we hypothesize:

**H8:** Perceived information control negatively affects perceived risk.

Undoubtedly, control over personal information plays a crucial role in information privacy research. When individuals realize they have more control to manage information privacy, they are likely to expand information privacy boundaries and increase disclosure intention. Li Gang et al. found that only when

users' perceived information control ability is stronger will their disclosure intention be stronger when studying Sina Weibo users' personal information privacy disclosure intention. H. Cavusoglu et al. discovered that granting users more privacy control permissions increases their information-sharing behavior when studying how privacy policy changes affect Facebook users' disclosure intention. Therefore, we hypothesize:

**H9:** Perceived information control positively affects information disclosure intention.

### 3.6 Privacy Tendency

Privacy tendency refers to individuals' general propensity to preserve information privacy space or restrict personal information disclosure. Individuals with higher privacy tendency are more sensitive to potential privacy threats and more concerned about their privacy boundaries. H. Xu et al. found that privacy tendency positively affects users' privacy concerns when studying individual perceptions and institutional privacy protection. Zhang Huiping et al. also verified the positive effect of privacy tendency on privacy concerns when studying the formation mechanism of WeChat users' information privacy concerns. Therefore, we hypothesize:

**H10:** Privacy tendency positively affects privacy concerns.

When other factors remain constant, lower privacy tendency results in users' insufficient attention to information leakage risks, with risk perception limited to the immediate term rather than long-term consequences, even believing that no risk exists if personal property isn't harmed. Regarding their relationship, Z. Liu et al. found that individuals with higher privacy tendency perceive greater risks when disclosing information. Li Kai also discovered that privacy sensitivity tendency positively correlates with perceived risk among LBS users when studying factors influencing LBS users' information disclosure intention. Therefore, we hypothesize:

**H11:** Privacy tendency positively affects perceived risk.

Based on the above analysis, the conceptual model framework constructed in this study is shown in Figure 1 [Figure 1: see original paper].

## 4. Research Design

### 4.1 Questionnaire Design

The questionnaire consists of two parts. The first part investigates factors influencing WeChat users' information disclosure intention, including seven latent variables: perceived information control, privacy tendency, privacy concerns, trust, perceived risk, perceived benefits, and disclosure intention. The second part covers demographic variables, including gender, age, education level, and WeChat usage frequency. For scale development, all measurement items were

adapted from previous studies and appropriately modified based on the actual situation of domestic WeChat users. Specific measurement variables and reference sources are shown in Table 1 . All items used a five-point Likert scale. This study collected data from WeChat users, a well-known domestic social platform, through questionnaire surveys and employed SmartPLS software for empirical validation of the research model.

## 4.2 Data Collection

The questionnaire was distributed through the online platform Wenjuanxing from October 9 to October 25, 2018. A total of 477 questionnaires were collected, with 415 valid questionnaires retained after eliminating invalid responses, yielding an effective rate of 87%. The demographic characteristics of the sample are shown in Table 2 , where frequency refers to the number of respondents and percentage represents the proportion of each category in the total sample. The characteristics of respondents presented in Table 2 are generally consistent with the mobile social user sample characteristics in the *2017 China Mobile Social User Insight Report* [47].

## 4.3 Data Analysis

**4.3.1 Reliability and Validity Analysis** Reliability reflects the questionnaire's reliability, stability, and consistency. This study used Cronbach's alpha and Composite Reliability (CR) to test reliability. Generally, Cronbach's alpha and CR values exceeding 0.7 indicate good internal consistency. In this study, the Cronbach's alpha coefficients and CR values for all latent variables exceeded 0.7, demonstrating high reliability. Validity reflects the effectiveness of measurement results. This study used convergent validity and discriminant validity to test data validity. Generally, factor loadings greater than 0.7 and Average Variance Extracted (AVE) greater than 0.5 indicate adequate convergent validity. The results show that the scale has good convergent validity (see Table 3 ). The criterion for discriminant validity is that the square root of each latent variable's AVE (diagonal elements in Table 4 ) should be greater than its correlation coefficients with other latent variables (off-diagonal coefficients). The results indicate significant differences between latent variables and good discriminant validity.

**4.3.2 Path Analysis and Hypothesis Testing** This study used SmartPLS for path parameter estimation and employed Bootstrapping resampling (500 iterations) to test the significance of path coefficients. Table 5 and Figure 2 [Figure 2: see original paper] present the path coefficients and hypothesis testing results. The path analysis results show that:

- The effect of perceived risk on disclosure intention was not supported (H1 rejected)
- Perceived benefits positively affected disclosure intention ( $\beta = 0.393$ ,  $P < 0.001$ ), supporting H2

- Trust positively affected disclosure intention ( $\beta = 0.217$ ,  $P < 0.001$ ) and negatively affected perceived risk ( $\beta = -0.162$ ,  $P < 0.01$ ), supporting H3 and H4
- Privacy concerns negatively affected disclosure intention ( $\beta = -0.087$ ,  $P < 0.05$ ) but did not significantly affect trust, supporting H5 but rejecting H6
- Perceived information control negatively affected privacy concerns ( $\beta = -0.083$ ,  $P < 0.05$ ) and positively affected disclosure intention ( $\beta = 0.090$ ,  $P < 0.05$ ), supporting H7 and H9 but rejecting H8
- Privacy tendency positively affected both privacy concerns ( $\beta = 0.752$ ,  $P < 0.001$ ) and perceived risk ( $\beta = 0.497$ ,  $P < 0.001$ ), supporting H10 and H11

## 5. Research Conclusions

Based on the hypothesis validation of the social media users' information disclosure intention model, the relationships between latent variables and their path coefficients were analyzed, yielding the following conclusions:

### 5.1 Perceived Benefits Significantly Positively Affect Disclosure Intention

This indicates that services, social integration, and pleasure obtained from using social media promote users' information disclosure intention, consistent with H. Krasnova et al.'s findings [22]. However, the negative effect of perceived risk on disclosure intention was not supported in this study. The main reasons include: (1) As China's mainstream social media tool, WeChat is primarily an emotion-based social network, differing from contract-based platforms. In such environments, users are willing to disclose information despite knowing certain risks exist. (2) Users generally disclose non-sensitive information (e.g., demographic characteristics) rather than sensitive information involving vital interests (e.g., financial or medical records). Moreover, most information disclosed on WeChat has likely been shared on other platforms, so re-disclosure poses no additional risk. (3) Risk perception typically exhibits lag; most users have not experienced serious privacy violations on WeChat, limiting their risk perception to the immediate term rather than long-term consequences, ultimately leading them to disclose information for more value-added services.

### 5.2 Trust Negatively Affects Perceived Risk

Trust as a psychological cognition weakens risks triggered by disclosure, shrinking information closure boundaries and expanding information sharing boundaries. When users have greater trust in social media platforms, they believe the platform is honest, reliable, and capable of protecting user privacy information, which weakens their risk beliefs about information disclosure. This conclusion aligns with C. Moorman et al.'s research [29]. Additionally, trust as a positive

emotional tendency in social relationships enhances users' willingness to disclose personal information.

### **5.3 Privacy Concerns Negatively Affect Disclosure Intention**

This conclusion is consistent with N.K. Malhotra et al.'s research [17]. Users' privacy concerns about social media primarily stem from potential threats such as improper collection, illegal use, and unauthorized sale of personal information to third parties. For the same privacy situation, users with higher privacy concerns significantly reduce active information disclosure behaviors. However, privacy concerns did not significantly affect trust, likely because regardless of privacy concerns, as China's mainstream social tool, WeChat demonstrates strong user privacy protection responsibility and employs privacy protection technologies like data desensitization, leading users to generally maintain high trust in the platform.

### **5.4 Perceived Information Control Positively Affects Disclosure Intention**

This conclusion indicates that granting users more information control capabilities increases their disclosure intention. Higher perceived information control means users have more autonomy to control privacy boundaries, unconsciously lowering self-protection awareness, opening privacy boundaries, and sharing more private information. This aligns with Li Gang's research [23]. The results also show that perceived information control negatively affects privacy concerns, suggesting that enhanced control means other entities cannot arbitrarily access and use personal information, weakening privacy worries caused by improper collection and unauthorized use. This aligns with Zhang Huiping et al.'s research [38]. The effect of perceived information control on perceived risk was not empirically supported, primarily because social media platforms increasingly emphasize detailed privacy controls (e.g., Moments permission settings, dynamic display settings, authorized login management), enabling users to better manage disclosed information and thus somewhat ignore risk perception.

### **5.5 Privacy Tendency Positively Affects Both Privacy Concerns and Perceived Risk**

This aligns with H. Xu et al.'s conclusions [12]. The results indicate that users with higher privacy tendency have deeper privacy understanding, express more support for privacy rights, and exhibit greater caution and higher privacy concerns about adverse consequences of providing privacy. Additionally, users with higher privacy tendency are more likely to experience anxiety, suspicion, and other negative emotions, making them more sensitive to potential privacy threats from information disclosure and thus perceiving higher risks.

## 6. Management Implications

The above conclusions provide the following insights and references for public managers and social media platforms when formulating user information privacy protection policies and implementing relevant measures:

### 6.1 Enhance Users' Perceived Information Control

- (1) Move beyond current formalistic privacy policies, as users rarely invest time in reading privacy terms. Platform operators should adopt new measures to enhance users' information control capabilities, such as refining privacy settings and strengthening privacy information reminder services.
- (2) Platforms should increase users' power to dispose of personal information, granting rights to query, delete, block, and correct personal information, and allowing users to set information storage duration independently, thereby increasing personal information controllability.
- (3) Strengthen users' information literacy at the technical level, such as helping users understand platform privacy policy statements and familiarize themselves with privacy setting functions to reduce the gap between perceived and actual control caused by information asymmetry.

### 6.2 Reduce Users' Information Privacy Concerns

- (1) Platforms should continuously improve core privacy protection technologies and encourage users to adopt defensive protection measures, such as data desensitization, anonymous identity protection, and refined information display timing, to reduce anxiety during personal information disclosure.
- (2) Social media platforms should improve encryption systems to effectively prevent user concerns about privacy leakage caused by illegal intrusion into user data; they should fully respect users' right to know, maintain transparent information interaction with users, promptly inform them about information usage methods, purposes, scope, and consequences of refusing to provide information, and adhere to professional ethics by promising not to leak personal information to third parties without user consent.
- (3) China currently shows a trend toward fragmented legislation on personal information protection; accelerating the introduction of a unified national *Personal Information Protection Law* can reduce implicit risks from personal information leakage, eliminate user concerns, and alleviate privacy concerns.

### 6.3 Enhance User Trust

- (1) Social media platforms should establish good images in daily operations, ensure the security of collected user personal information, and significantly enhance user trust through effective preventive and remedial measures.
- (2) Platforms should formulate clear and reasonable privacy policies, listing "personal information protection" and related clauses separately in

user agreements or service agreements, or develop standalone personal information privacy protection rules detailing policies and measures for obtaining, managing, and protecting user personal information. (3) Use user interface design appropriately to strengthen communication among users, change passive privacy protection concepts, pay attention to user feedback on privacy protection needs during platform use, and further improve relevant privacy settings.

#### 6.4 Enhance Users' Perceived Benefits

- (1) Social media operators should develop distinctive friend-making functions, such as building user-friendly community sections and organizing online and offline activities to help users expand their friend circles. (2) Provide users with higher-quality and more convenient products and services. Under the premise of properly addressing user information security and privacy protection, fully utilize big data technology for user profiling to achieve personalized recommendations and enhance perceived benefits. During data analysis, special attention should be paid to data desensitization, with mainstream technologies including watermarking, distortion, merging, generalization, and encryption. (3) Enrich interaction forms among users and help users obtain good experiential value by planning more interactive activities that strengthen emotional communication, such as inviting experts, celebrities, and opinion leaders as VIP users to participate in platform exchange meetings, thereby improving perceived benefits through interaction, communication, knowledge creation, and application.

#### References

- [1] Sun Xiaoling, Cheng Yang, Zhu Qinghua. Research on influencing factors of user privacy disclosure behavior intention in social search [J]. *Journal of Intelligence*, 2017, 36(10): 172-179, 201.
- [2] Li H, Sarathy R, Xu H. Understanding situational online information disclosure as a privacy calculus [J]. *Journal of Computer Information Systems*, 2010, 51(1): 62-71.
- [3] Hallam C, Zanella G. Online self-disclosure: The privacy paradox linking individual perceptions with institutional privacy assurances [J]. *Journal of the Association for Information Systems*, 2011, 12(12): 798-824.
- [4] Wang Bowei, Li Qihua. Privacy boundaries and management mechanisms of WeChat Moments in the big data era—Based on the theoretical perspective of communication privacy management [J]. *Information Studies: Theory & Application*, 2016, 11(39): 37-42.
- [5] Choi BCF, Land L. The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage [J]. *Information & Management*, 2016, 53(7): 868-877.
- [6] Eastin MS, Brinson NH, Doorey A, et al. Living in a big data world: Predicting mobile commerce activity through privacy concerns [J]. *Computers*

- in *Human Behavior*, 2016, 58(C): 214-220.
- [7] Laufer RS, Wolfe M. Privacy as a concept and a social issue: A multidimensional developmental theory [J]. *Journal of Social Issues*, 1977, 33(3): 23-42.
- [8] Zhu H, Ou CXJ, Vanden Heuvel WJM, et al. Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making [J]. *Information & Management*, 2017, 54(4): 427-437.
- [9] Dienlin T, Metzger MJ. An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample [J]. *Journal of Computer-Mediated Communication*, 2016, 21(5): 368-383.
- [10] Wang Yuchao. Research on influencing factors of health privacy information disclosure intention in online medical communities [J]. *Journal of Information Resources Management*, 2018, 8(1): 93-103, 113.
- [11] Wang Xiwei, Xiang Mengmeng, Zhang Changliang, et al. Research trends and development directions of information privacy at home and abroad in the new media environment [J]. *Library and Information Service*, 2017, 61(15): 6-14.
- [12] Xu H, Dinev T, Smith J, et al. Information privacy concerns: Linking individual perceptions with institutional privacy assurances [J]. *Journal of the Association for Information Systems*, 2008, 9(6): 332-363.
- [13] Dinev T, Xu H, Smith JH, et al. Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts [J]. *European Journal of Information Systems*, 2013, 22(3): 295-316.
- [14] Ajzen I. *Attitudes, personality, and behavior* [M]. Chicago: Dorsey Press, 1988.
- [15] Smith HJ, Milberg SJ, Burke SJ. Information privacy: Measuring individuals' concerns about organizational practices [J]. *MIS Quarterly*, 1996, 20(2): 167-196.
- [16] Hu Changping, Qiu Rongrong. Review of virtual community users' privacy concerns [J]. *Information Studies: Theory & Application*, 2018, 41(12): 149-154.
- [17] Malhotra NK, Kim SS, Agarwal J. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model [J]. *Information Systems Research*, 2004, 15(4): 336-355.
- [18] Chen R. Living a private life in public social networks: An exploration of member self-disclosure [J]. *Decision Support Systems*, 2013, 55(3): 661-668.
- [19] Norberg PA, Horne DR, Horne DA. The privacy paradox: Personal information disclosure intentions versus behaviors [J]. *Journal of Consumer Affairs*, 2007, 41(1): 100-126.
- [20] Hajli N, Lin X. Exploring the security of information sharing on social networking sites: The role of perceived control of information [J]. *Journal of Business Ethics*, 2016, 133(1): 111-123.
- [21] Stone EF, Stone DL. Privacy in organizations: Theoretical issues, research findings, and protection mechanisms [J]. *Research in Personnel and Human Resources Management*, 1990, 8(3): 349-411.
- [22] Krasnova H, Veltri NF, Günther O. Self-disclosure and privacy calculus on social networking sites: The role of culture [J]. *Business & Information Systems*

Engineering, 2012, 4(3): 127-135.

[23] Li Gang, Wang Dandan. Research on influencing factors of social networking site users' personal information disclosure intention: A case study of Sina Weibo [J]. Information and Documentation Services, 2015, 36(1): 35-40.

[24] Wang T, Duong TD, Chen CC. Intention to disclose personal information via mobile applications: A privacy calculus perspective [J]. International Journal of Information Management, 2016, 36(4): 531-542.

[25] Bansal G, Zahedi FM, Gefen D. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online [J]. Decision Support Systems, 2010, 49(2): 138-150.

[26] Lan Xiaoxia. Empirical research on information disclosure intention in mobile social networks—From the perspective of privacy calculus and trust [J]. Modern Information, 2017, 37(4): 82-86.

[27] Li Qi, Wang Luyao, Qiao Zhilin. The influence of privacy calculus and social capital on mobile social users' self-disclosure intention—A comparative analysis based on WeChat and Weibo [J]. 2018, 37(5): 169-175.

[28] Gefen D. It is not enough to be responsive: The role of cooperative intentions in MRP II adoption [J]. Database for Advances in Information Systems, 2000, 31(2): 65-79.

[29] Moorman C, Zaltman G, Deshpande R. Relationships between providers and users of market research: The dynamics of trust within and between organizations [J]. Journal of Marketing Research, 1992, 29(3): 314-328.

[30] Jarvenpaa SL, Tractinsky N. Consumer trust in an internet store: A cross-cultural validation [J]. Journal of Computer-Mediated Communication, 1999, 5(2): 1-33.

[31] Rifon NJ, LaRose R, Choi SM. Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures [J]. Communications of the ACM, 1999, 42(4): 80-87.

[32] Hoffman DL, Novak TP, Peralta M. Building consumer trust online [J]. Communications of the ACM, 1999, 42(4): 80-87.

[33] Zhang Yue, Sun Xiaoling, Lu Jiaying, et al. Empirical research on mobile social users' information disclosure intention based on privacy calculus theory—A case study of WeChat [J]. Library & Information, 2018(3): 90-97.

[34] Zhu Hou, Wang Ke, Yan Zhijun, et al. Research on SNS users' privacy paradox based on privacy calculus theory [J]. Journal of Intelligence, 2017, 36(2): 134-139, 121.

[35] Yang K. Consumer technology traits in determining mobile shopping adoption: An application of the extended theory of planned behavior [J]. Journal of Retailing & Consumer Services, 2012, 19(5): 484-491.

[36] Zhang Xiaojuan, Li Zhenzhen. Information privacy concerns, trust, and personal information security behavior intention of smartphone users [J]. Modern Information, 2018, 38(3): 45-50.

[37] Cavusoglu H, Phan TQ, Cavusoglu H, et al. Assessing the impact of granular privacy controls on content sharing and disclosure on Facebook [J]. Information Systems Research, 2016, 27(4): 848-879.

[38] Zhang Huiping, Yang Jingdian, Tang Zhiwei. Research on the formation

- mechanism of social media users' information privacy concerns [J]. *Information Studies: Theory & Application*, 2017, 40(6): 40-43.
- [39] Liu Z, Wang X. How to regulate individuals' privacy boundaries on social networking sites: A cross-cultural comparison [J]. *Information & Management*, 2018, 55(8): 1005-1023.
- [40] Li Kai, Huang Jingyao, Wang Xiaowen. Analysis of influencing factors of LBS users' information disclosure intention—An empirical study based on exchange theory [J]. *Journal of the China Society for Scientific and Technical Information*, 2016, 35(1): 84-97.
- [41] Xu H, Dinev T, Smith JH, et al. Examining the formation of individual's information privacy concerns: Toward an integrative view [C]//*Proceedings of the 29th International Conference on Information Systems*. Paris: AIS Electronic Library, 2008: 14-17.
- [42] Fogel J, Nehmad E. Internet social network communities: Risk taking, trust, and privacy concerns [J]. *Computers in Human Behavior*, 2009, 25(1): 153-160.
- [43] Krasnova H, Spiekermann S, Koroleva K, et al. Online social networks: Why we disclose [J]. *Journal of Information Technology*, 2010, 25(2): 109-125.
- [44] Pavlou PA, Chellappa RK. The role of perceived privacy and perceived security in the development of trust in electronic commerce transactions [D]. Los Angeles: Marshall School of Business, USC, 2001.
- [45] Kehr F. Feeling and thinking: On the role of intuitive processes in shaping decisions about privacy [D]. St. Gallen: University of St. Gallen, 2015.
- [46] Schierz PG, Schilke O, Wirtz BW. Understanding consumer acceptance of mobile payment services: An empirical analysis [J]. *Electronic Commerce Research and Applications*, 2010, 9(3): 209-216.
- [47] 199IT Chinese Internet Data Consulting Center. 2017 China Mobile Social User Insight Report [EB/OL]. [2018-11-01]. <http://www.199it.com/archives/609904.html>.

## Author Contributions

Guo Hailing: Proposed the research topic, determined the research framework, wrote and revised the manuscript.

Ma Hongyu: Conducted literature review, data collection and analysis, and manuscript writing.

Xu Zehui: Conducted data collection and analysis.

---

## Construction and Demonstration of the Influence Model of Social Media Users' Information Disclosure Intention: A Case Study of WeChat Users

Guo Hailing, Ma Hongyu, Xu Zehui  
School of Management, Hebei University, Baoding 071002

**Abstract:** [Purpose/significance] Frequent information privacy leakage incidents on social media have intensified users' concerns about information privacy.

Whether users are willing to disclose personal information to platforms during social media usage has become key to promoting the healthy development of social media platforms. [Method/process] Based on privacy calculus theory and communication privacy management theory as the framework, combined with privacy concerns, this paper constructs a model of factors influencing social media users' information disclosure intention. Taking the WeChat platform as an example, sample data were collected through questionnaire surveys, and Smart-PLS software was used to verify the rationality of the model. [Result/conclusion] The study finds that perceived benefits, trust, and perceived information control all positively affect disclosure intention, while privacy concerns negatively affect disclosure intention; trust negatively affects perceived risk; perceived information control negatively affects privacy concerns; and privacy tendency positively affects both privacy concerns and perceived risk.

**Keywords:** social media, privacy calculus, communication privacy management, information privacy, disclosure intention

---

### Call for Papers: Forum on the Development of Information Science and Information Work (2019)

Since its establishment, the Forum on the Development of Information Science and Information Work has been successfully held for two sessions, effectively promoting the scientific development of information science and information work and receiving positive responses and widespread recognition. Big data and artificial intelligence are reshaping the core and application scenarios of information science and information work. To continue the spirit of the “Nanjing Consensus,” grasp transformation and change opportunities, gather and highlight the latest progress in the information field, promote exchanges among Chinese information science scholars and information workers, innovate theories and practices of information science and information work, and establish an annual national academic conference platform for information science to form an academic tradition, the “New Era, New Mission, New Actions—Forum on the Development of Information Science and Information Work (2019)” will be held at Central China Normal University in Wuhan from November 8-10, 2019. This forum will uphold the fine tradition of the Forum on the Development of Information Science and Information Work, inviting experts, scholars, student representatives, and practitioners from local, military, and public security universities and research institutes to participate in in-depth exchanges and collisions around the innovation and development of information science and information work in the new era. Through discussions and interactions among scholars and experts from different fields, the forum will promote the in-depth development of information science and information work. We warmly welcome teachers, students, scholars, experts, and practitioners in the field of information science and information work to submit papers and attend the conference!

#### 1. Organizers

China Society for Scientific and Technical Information  
China Society for Social Sciences Information  
China Society for Defense Science and Technology Information  
School of Information Management, Central China Normal University

## 2. Conference Dates

November 8-10, 2019

## 3. Conference Venue

Wuhan, Central China Normal University

## 4. 征稿主题: Innovation and Development of Information Science and Information Work in the New Era

The 征稿主题 includes but is not limited to the following topics for authors' reference:

- (1) Development and innovation of information science theory
- (2) Innovation and application of information science methods
- (3) Innovation and practice of information technology
- (4) Information behavior and information services
- (5) Security intelligence
- (6) Discipline construction of information science
- (7) Information work and information career development

## 5. 征稿要求

### (1) 征稿对象

The forum invites submissions from teachers, students, scholars, experts, and practitioners in the field of information science and information work.

### (2) Important Dates

Submission deadline: August 31, 2019

Notification of review results: September 30, 2019

### (3) Manuscript Requirements

Submitted papers must be original, unpublished research, with a length of approximately 8,000 words. Please refer to the "Submission Guidelines and Format Specifications" of *Library and Information Service* for formatting requirements.

### (4) Acceptance, Awards, and Publication

The forum organizers will invite experts to conduct strict reviews of submitted papers. Accepted papers will receive remuneration, and authors invited to present will be provided with accommodation during the conference (limited to one author per accepted paper). Based on the quantity and quality of submissions, outstanding papers will be selected for first, second, and third prizes and awarded certificates and prizes. Outstanding papers will be recommended for publication in journals such as *Library and Information Service*, *Library and Information Knowledge*, *Journal of Intelligence*, *Information Science*, *Information Studies: Theory & Application*, *Journal of Information Resources Management*, *Intelligence Engineering*, *Journal of Intelligence*, *Modern Information*, *Knowledge Management Forum*, and *Agricultural Library and Information Science* (in

no particular order).

**6. Contact Information**

Li Yuhai, School of Information Management, Central China Normal University  
Email: yhli@mail.ccnu.edu.cn  
Phone: 027-67868865

Yi Ming, School of Information Management, Central China Normal University  
Email: yiming0415@mail.ccnu.edu.cn  
Phone: 13387599231

**Organizing Committee of the Forum on the Development of Information Science and Information Work (2019)**

School of Information Management, Central China Normal University  
April 2, 2019

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

*Source: ChinaXiv — Machine translation. Verify with original.*