

2020 ASIS&T Asia-Pacific Regional Conference (Virtual Conference),  
December 12-13, 2020, Wuhan, China

Open Access

Anrong Fan, Qiao Wu, Xiaofei Yan, Xiaotong Lu, Yue Ma, Xue Xiao\*

# Research on Influencing Factors of Personal Information Disclosure Intention of Social Media in China

<https://doi.org/10.2478/dim-2020-0038>

received August 15, 2020; accepted September 15, 2020.

**Abstract:** The disclosure of personal information by users is very important for social media, in order to balance privacy protection and personalized service. This article probes into the factors influencing users' disclosure intention. Based on the privacy calculus theory and theory of planned behavior, the study constructs an influencing factor model of social media personal information disclosure intention. Then an extensive survey of social media users is conducted through questionnaire, and the hypothetical model is verified using structural equation model, and finally the relationship between various influencing factors and personal information disclosure intentions is obtained. The results show that the perceived benefits and subjective norm are related to personal information disclosure intentions, and privacy view is associated with perceived risk. Finally, the study provides new ideas for social media services and user privacy protection, such as creating a secure social media environment, increasing valuable social services, reducing users' risk perception and making information processing open and transparent.

**Keywords:** personal information disclosure intention, privacy calculus theory, theory of planned behavior, influencing factor model

## 1 Introduction

Personal information refers to all kinds of information recorded by electronic or otherwise that can be used to independently identify or be combined with other information to identify specific natural persons (National People's Congress, 2020). It is always associated with the identity of a natural person in the sense of physical, physiological, genetic, mental, economic, cultural, or social (European Unit, 2018). From the above, it can be seen that personal information can be identified and closely linked with the information subject, which involves the field of privacy life. Once abused by a third party, it will cause great privacy infringement to the information subject.

Disclosure of personal information widely appears in various situations in human social life. In recent years, with the wide application of the mobile Internet, social media has become one of the important personal information disclosure scenarios. Posey, Lowry, Roberts and Ellis (2010) stated that the self-disclosure behavior of online community users refers to the behavior of users leaking personal information when registering or using mobile social networks. The term "social media" originated from *What is Social Media* written by Antony Mayfield in 2007; the author defines social media as "a new type of online media with the characteristics of participation, openness, conversation, community, connectedness, that gives users great participation space." In the process of the gradual development and growth of the mobile Internet, the application scenarios and types of social media have further increased. The *2016 China Social Application User Behavior Research Report* (CNNIC, 2017) divides social applications into three main types: instant messaging tools represented by WeChat and QQ, comprehensive social applications represented by Sina

\*Corresponding author: Xue Xiao, Department of Information Resources Management, Business School, Nankai University, Tianjin, China, Email: xiaoxue@nankai.edu.cn

Anrong Fan, Qiao Wu, Xiaofei Yan, Xiaotong Lu, Yue Ma, Department of Information Resources Management, Business School, Nankai University, Tianjin, China

Weibo, and vertical social applications represented by Douyin (overseas version: Tik Tok) and Zhihu. Although the boundaries of social media are becoming blurred, this classification still has some value.

In the process of using social media, users often need to actively accept the disclosure of personal information. Research by Nie and Luo (2013) pointed out that the disclosure of personal information on social media by users is an important issue that needs to be weighed. Although more disclosure of personal information on social media helps to make full use of the advantages of the platform to meet their own needs, increasing the disclosure of personal information will correspondingly increase the risk of personal privacy leakage. The deepening of this contradiction has further led to the paradox phenomenon of current social media users (Awad & Krishnan, 2006). “Although there are great concerns about privacy issues, they continue to disclose personal information in social media,” Li, Yu, Xu and Xie noted (2018). On one hand, through the disclosure of user’s personal information, social media can realize personalized service and directional recommendation content, and help users to establish a broader social relationship. But at the same time, the privacy security of users has been repeatedly in crisis, such as the public sale of user accounts, crime of face recognition, and so on. China is a major country of mobile Internet and social media applications, with a huge social media user base. In the 44th *Statistical Report on China’s Internet Development Status* released by China Internet Network Information Center (CNNIC, 2019), the number of instant messaging users reached 825 million, accounting for 96.5% of China’s total Internet users. Due to the large base and high proportion of social media users, the issue of personal information disclosure has become one of the common problems in our society.

Through the above background analysis, it can be seen that reasonable access to and use of user’s personal information in social media can alleviate their concerns in privacy disclosure paradox and improve their use experience. Therefore, it is very important to understand the factors that affect users’ intention to disclose information. Although many scholars have studied the issue of online privacy disclosure, the research perspectives are different, and the interaction between various factors is not clear. This study attempts to investigate various types of social media software, combined with multiple theoretical perspectives to establish an analysis framework. Structural equation modeling (SEM) is used to verify the hypothetical model of influencing factors of personal information disclosure intention to determine the specific relationship and net

impact between each variable, to provide a theoretical basis for providing the relevant countermeasures and suggestion.

## 2 Literature Review

As early as 1992, Amidon put forward a discussion on privacy concerns related to electronic information media. With the rise of social media in 2002, a large number of information behavior research on users of different platforms emerged. In 2011, two literature reviews on Internet privacy were published in the *MIS Quarterly*, which made the disclosure of user information privacy a hot topic in this field (Smith, Dinev, & Xu, 2011; Pavlou, 2011). The research on personal information disclosure can be sorted out from the research perspective, research context, and influencing factors. In the early research, it focused on explaining the mechanism of personal information disclosure behavior by establishing interdisciplinary theory, and gradually expanded to different application contexts and their influencing factors.

### 2.1 Research Perspective of Personal Information Disclosure Intention

#### 2.1.1 Privacy Calculus Theory

When studying the intention of personal information disclosure behavior, scholars generally use the existing behavior theory as a framework for further analysis. Among them, Privacy Calculus Theory is the most commonly used. It believes that users decide whether to disclose their personal privacy information in the balance of risks and benefits (Korzaan & Boswell, 2008). The perceived benefits and perceived risks are key considerations of personal information disclosure. User’s intention will be motivated, and their disclosure behavior will be generated, only when the perceived benefits are greater than the perceived risks (Li, Hong & Zhu, 2016). Metzger (2004) found that the privacy risks in the Internet environment have a negative effect on the disclosure of private information by users. As for privacy benefits, Hann, Hui, Lee and Png (2007) conducted an empirical research. It proved that economic compensation promotes user’s disclosure of privacy information (Hann et al., 2007) and even the vast majority of users are willing to sacrifice personal privacy in exchange for personalized online services (Chellappa & Sin, 2005).

### 2.1.2 Theory of Planned Behavior

Theory of Planned Behavior (TPB) believes that personal behavior intention is the direct factor that affects actual behavior, and personal behavior intention is affected by behavior attitude, subjective norm, and perceived behavioral control (Ajzen, 1991). This means that when a user has a positive attitude, strong outside support, and strong perceived control over his behavior, he would likely disclose his personal information. Based on this theory, Guo, Duan, & Wang (2018) verified the privacy information disclosure behavior of mobile learning users from the above three aspects. In addition, this theory is often used in conjunction with Privacy Calculus Theory. For example, some researchers have combined the two theories to establish models in their research (Li & Chen, 2010; Shi, 2011).

### 2.1.3 Trust Theory

Trust Theory is mainly applied in the fields of psychology, sociology, organizational behavior, and so on. Trust means that one party ignores the ability to monitor the other party and accepts the intention to be at a disadvantage based on the expectation of the other party and that the other party will perform a specific and important behavior for itself (Mayer, Davis, & Schoorman, 1995). In the Internet environment, users are the subject of personal information. Neither their amount of information possession nor their ability to protect information is sufficient to “confront” information service providers. Thus, users can be seen as a relatively disadvantaged party. At this time, trust can resolve the risks and anxiety perceived by users, thereby increasing users’ personal information disclosure intention (Dinev & Hart, 2006). Trust can be disassembled into two concepts: Social Networking Site (SNS) and SNS users, both, can influence personal information disclosure intention through the mediating variable “personal information disclosure attitude” (Li & Wang, 2015).

### 2.1.4 Other Theoretical Perspectives

Scholars have also analyzed personal information disclosure intention from other theoretical perspectives: the Uses and Gratifications Theory believes that users’ disclosure of private information has a certain purpose and motivation (Hollenbaugh & Ferris, 2014); Personality Theory believes that personality factors such as narcissism and social anxiety have an important impact on the

disclosure of personal identity information by young social network users (Liu, Cong, Ang, Rebecca & Lwin, 2013). From the perspective of Justice Theory, Culnan and Armstrong (1999) proved that perceived fairness has a positive impact on users’ privacy information disclosure intention.

## 2.2 Context of Personal Information Disclosure Intention

### 2.2.1 E-commerce Context

Since the rise of e-commerce and other emerging business models in 2006, the privacy information leakage of Internet consumers is facing great risks. Scholars began to pay attention to the privacy leakage channels, privacy concern measurement scale, privacy protection, and other issues in personalized e-commerce services (Yang, Wang & Wang, 2008). Zhao, Lu, and Gupta et (2012) found that business preferences, privacy policies, and legal awareness had indirect effects on users’ intention to disclose location related information. Ouyang and Yuan (2016) constructed a model of consumer privacy concerns influencing behavior intention in the e-commerce environment, in which information importance, website reputation, and trust are the main influencing factors. Zhu, Liu, Chen, and Lu (2014) studied the privacy threat avoidance behavior of mobile commerce smart phone terminal consumers, which is triggered by avoidance motivation and affected by social impact, perceived threat, and perceived avoidance ability.

### 2.2.2 Social Network Context

In addition, with increasing of social network users, personal information disclosure has become very convenient and more prevalent. Bergström (2015) found that trust had different influences on the online privacy concern of different social network user groups, and then affected the users’ online privacy settings and information disclosure degree. Hou and Ren (2013) built a model of individual privacy perceived risk and protection behavior through interview with users in social environment as QQ and Sina Weibo. Wang and Li (2016) discussed that the impact mechanism of fear appeals on the information security of social network users by analyzing questionnaire survey data, and built a behavior model based on the Fear Appeals Theory, revealing how social network users adopt privacy protection measures.

## 2.3 Influencing Factors of Personal Information Disclosure Intention

Personal information disclosure intention is affected by many factors, including the external social environment and user's internal reasons. The external factors mainly show as social norms, peer effects, social culture environment, and policy environment. The research of Livingstone (2008) showed that peer effects had great influence on the privacy disclosure intention of teenagers. Zlatolas, Welzer, Heričko and Hölbl (2015) stated that user information disclosure intention was affected by privacy policy, privacy concerns, and privacy social norms.

In addition, the incentive measures and privacy policies of online platforms often affect the extent to which users disclose personal information. Research by Wu, Huang, Yen, and Popova (2012) showed that privacy policy has a negative impact on privacy concerns, thereby enhancing disclosure. However, the empirical study conducted by Stutzman, Capra, and Thompson (2011) on Facebook users showed that people who read more privacy policies tended to disclose less information. User's internal factors include demographic characteristics, user habits, privacy view, and personality traits. For example, Zhang, Chen, and Lee (2013) found in research that female and male employees paid different attention to information privacy. In addition, although factors such as education level and nationality cannot directly establish a connection with user's intention to disclose personal information, they can also be used as control variables to influence the research results (Valk, 2015).

In sum, relevant researches on personal information disclosure intention are still in the exploratory stage, empirical studies are mostly based on a single application (App) context, and the verification of influencing factors is relatively one-sided. Therefore, it is necessary to investigate the applicability of existing theories in different types of social media, and to explore the internal relationship between the factors influencing the personal information disclosure intention.

## 3 Research Model and Hypotheses

### 3.1 Theoretical Grounding

#### 3.1.1 Theory of Planned Behavior

Proposed by Icek Ajzen (1988, 1991), TPB is the successor of the Theory of Reasoned Action (TRA) proposed by

Fishbein and Ajzen (1975, 1980). Holding the view that a well-thought out plan is on account of human behavior, and all factors that may affect behavior indirectly affect the behavior performance through behavior intentions, TPB is generally used to understand how people change their behavior patterns. The behavior intention is affected by three related factors: attitude (internal factor, which means that individual's attitude toward a particular behavior); subjective norm (which affects individuals to take a certain behavior); and perceived behavioral control (external factor, including secondhand information that comes from acquaintance, friends, and so on) (Ajzen & Driver, 1991).

TPB is widely used and has applications in various research fields of behavioral intention. It is not only the basis of the prototype willingness model (Wang & Zheng, 2016), but is also related to TRA and social cognition theory, which makes it a unique advantage in the comprehensive application of related theories.

#### 3.1.2 Privacy Calculus Theory

As early as 1973, Laufer and Wolfe began to pay attention to the difficulties faced by personal information management – the balance between interpersonal interaction and privacy. They introduced Social Exchange Theory of economic field into user research, and refer to the cost-benefit evaluation as “Privacy Calculus”; subsequent research further deepened the theoretical conception, pointing out that calculus behavior is affected by both technology use experience and information management capabilities (Laufer, Proshansky, & Wolfe, 1973). Privacy Calculus Theory is a typical extension of behavior model, which discusses people's attitude and behavior when facing privacy issues. The theory not only considers the positive factors that affect behavioral intentions (perceived benefit), but also takes account of some negative factors called perceived risk (Laufer & Wolfe, 1977). Based on Privacy Calculus Theory, users will weigh the benefits and risks when making personal information disclosure decisions. If the perceived benefit exceeds the cost, people will choose to disclose personal information.

### 3.2 Conceptual Model

The study selects two of the main factors that affect the behavior intention from TPB, and combine them with the basic frame of Privacy Calculus Theory. Finally, it chooses four measurement dimensions: perceived benefit,

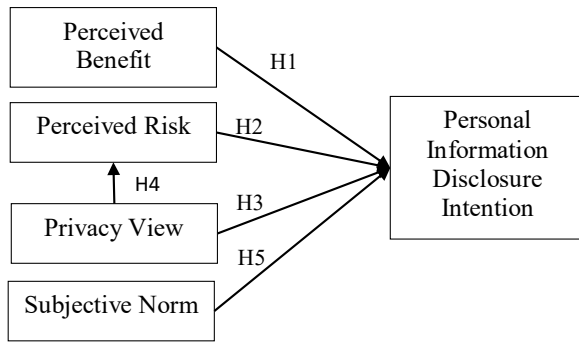


Figure 1. Hypothesis model of personal information disclosure intention.

perceived risk, privacy view, and subjective norm. These variables are assumed to have a direct relationship with personal information disclosure intention. Besides, based on previous studies, the relationship between privacy view and perceived risk is tested. Figure 1 shows the proposed hypotheses.

### 3.2.1 Perceived Benefit

Perceived benefit is defined as the benefit that is brought to users when they use a product, and users are aware of that (Lu, Tan, & Hui, 2004; Culnan & Bies, 2003). The main purpose that users disclose personal information on social media is to maintain or establish more interpersonal relationships, in order to gain a sense of belonging to the organization, and to obtain more services (Shi, 2011). The usefulness of social media includes four dimensions: relationship value, communicational value, informational value, and instrumental value. Some researchers have pointed out that, as an Internet application that helps people build and maintain social networks, the function of social media first performs in the establishment and maintenance of interpersonal relationships, then manifests as communicating with like-minded people, which means that social media have communicational value (Ellison, Steinfield, & Lampe, 2007). For informational value, it means that users obtain or share information through social media to understand popular opinions in the society. Instrumental value means that users can find solutions to problems and obtain others' help through continuous online interaction and communication in order to complete certain tasks (Nie & Luo, 2013).

In previous studies, the significant impact of the perceived benefits to social network privacy disclosure has

been proved (Li & Chen, 2010; Li et al., 2016). Sharma and Crossler (2014) found that perceived benefits will increase personal information disclosure for social commerce customers. It is also proved to be negatively related to the active protection of privacy (Anic et al., 2019). The opposite influence of perceived benefit and privacy concern on privacy disclosure has also been mentioned (Al-Jabri, Eid, & Abed, 2019). Therefore, we establish the first hypothesis:

H1: Perceived benefit will positively affect personal information disclosure intention.

### 3.2.2 Perceived Risk

Perceived risk refers to the loss that may be caused by the users' personal information disclosure behavior due to social media's illegal or improper use of information, and it is the user's prediction of the worst outcome (Xu, Dinev, Smith, & Hart, 2008). The risks perceived by users mainly come from inappropriate access and inappropriate use of information (Dinev, Xu, Smith, & Hart, 2013). Previous studies have confirmed that there is a negative correlation between perceived privacy risk and disclose intention online (Dinev & Hart, 2006). That is to say, the more risks a user perceives, the less intention there is, to disclose personal information.

The negative influence of perceived risk to personal information disclosure has been proved by many studies. Sharma and Crossler (2014) found the impact of perceived risk in the social commerce environment. It also has a significant effect on social network (Xu, Michael, & Chen, 2013; Li, Hong & Zhu, 2016), and mobile learning users (Guo, Ma, & Xu, 2019). But the influence of perceived risk has also been proved insignificant. Lan (2017) and Guo et al. (2019) have found that perceived risk does not have an apparent impact on mobile social network users. As a result of the contrary conclusions, the effect of perceived risk needs testing. Therefore, the second hypothesis is established:

H2: Perceived risk will negatively affect personal information disclosure intention.

### 3.2.3 Privacy View

Privacy view reflects the importance of an individual's treatment of personal privacy, and is related to the individual's personal characteristics, cultural background, and experience (Li & Wang, 2015). Information sensitivity is defined as the level of privacy concerns that users



perceive for certain types of information in a specific context (Li, Hong & Zhu, 2016). Privacy view affects disclosure intention through information sensitivity. The stronger the privacy view is, the more sensitive users are to perceive risks, and users may show more cautiousness when they are asked to disclose their personal information. Therefore, the following hypotheses are made:

H3: Privacy view will negatively affect personal information disclosure intention.

H4: Privacy view will positively affect perceived risk.

### 3.2.4 Subjective Norm

Subjective norm refers to the social pressure that users perceive when deciding whether to perform a certain behavior (Ajzen, 1991). Social pressure mainly comes from the social and cultural environment, and people (family members, friends, etc.) who have a certain influence on the user. Subjective norm affects the risk users perceive and their intention to disclose their personal information.

Subjective norm has been widely used in researches about personal information disclosure intention, but the relationship between subjective norm and personal information disclosure intention depends on how others tend to behave. Some researchers hold the opinion that subjective norm shows a negative impact on personal information disclosure intention through perceived risk (Li, Hong & Zhu, 2016). Meanwhile, other researchers explain subjective norm as others' willingness to show personal information and have discovered a positive relationship between subjective norm and personal information disclosure intention (Heirman, Walrave, & Ponnet, 2013; Varnali & Toker, 2015; Jiao, 2019). Therefore, Hypothesis 5 is established:

H5: Subjective norm will negatively affect personal information disclosure intention.

## 4 Methodology

### 4.1 Questionnaire Design

The following five constructs were measured using multiple-item scales: perceived benefit, perceived risk, subject norm, privacy view, and personal information disclosure intention. All items use five-point Likert-type scales (*strongly disagree* = 1 to *strongly agree* = 5). Prevalidated items were used following a pretest to ensure content validity.

Prior to data collection, a pilot test was conducted with 33 social media users who have different demographic backgrounds. They were requested to review the items to evaluate the constructs, semantics, suitability, and format of the questionnaire. According to their feedback, the questionnaire was revised. Moreover, we conducted a pilot study to ensure reliability and validity of the scales. The result of data analysis shows that Cronbach's alpha of all constructs were above 0.7, which implies a strong internal consistency of theory. An online version of survey was designed and its hyperlink was posted on Wenjuanxing, a famous online survey platform, and distributed via WeChat. The subjects who had experience of using social media were invited to fill out the questionnaire. The items are listed in Appendix.

### 4.2 Data Collection

We posted a survey hyperlink to the social media users from May 30 to the end of June and September 10 to 28, 2020. Convenience sampling and snowball sampling were used as sampling method for respondents who filled out the survey successfully received small monetary rewards. Finally, a total of 580 questionnaires were collected. Based on the selection of question 25 ("Please select "very disagree" for this question") and the response time of the questionnaire (less than 60 s) and the same answer to all questions, we eliminated invalid data, and a total of 517 responses were left. The description of demographic characteristics of the respondents is shown in Table 1. More than half of the respondents are female, accounting for 69.83%. The ages of the respondents are concentrated in the young and middle-aged (19–59 years old), which is in line with the overall characteristics of the social media user group. The educational background is principally undergraduate. The description of demographic characteristics of the respondents is shown in Table 1.

## 5 Data Analysis and Results

### 5.1 Non-response Bias

This study addressed the issue of non-response bias follow the procedure suggested by Armstrong and Overton (1977) to conduct Chi-Square test for the early and late respondents. A total of 410 respondents who completed the survey during the early stage were considered earlier respondents and 107 respondents completed the survey

Table 1  
Demographic Characteristics of the Respondents (N = 517)

Category	Item	N	Percentage (%)
Gender	Male	135	26.11
	Female	361	69.83
	Unwilling to disclose	21	4.06
Age	19–35 years old	38	7.35
	36–59 years old	360	69.63
	18– years old and below	96	18.57
	Over 60– years old	23	4.45
Education	College degree and below	61	11.80
	Undergraduate	324	62.67
	Master's degree	98	18.96
	PhD and above	34	6.58
Occupation	Student	345	66.73
	Teacher/researcher	51	9.86
	Institutional staff	36	6.96
	Civil servant	8	1.55
	Corporate Staff	36	6.96
	Self-employed/Freelances	25	4.83
	Others	16	3.09

during the later stage. We compared the means of all variables and demographics for these two stages and found no significant differences. Thus, we excluded the possibility of non-response bias.

## 5.2 Common Method Bias

We conducted three test to address the potential concern for common method bias(CMB). One is Harman's one-factor tests (Podsakoff & Organ, 1986). Evidence of common method bias exists when a general construct accounts for the majority of covariance among all constructs. A principal component factor analysis was performed and the results excluded the potential threat of common methods bias (Shiau & Luo, 2012). The combined five factors accounted for 76.205% of total variance; the first (largest) factor accounted for 17.510% (the variances explained ranges from 13.056% to 17.510%) and no general factor accounted for more than 50% of variance, indicating that common method bias may not be a serious problem in the data set. The second followed Liang's (2007) method. A common method factor was included in the PLS model

and it determines all indicators of the principal constructs. The result is shown in Table 2, indicating that the ratio of average substantively explained variance of the indicator (0.750) to average common method-based variance(0.011) was about 69.6:1. In addition, most method factor loadings were not significant. The third one used VIF as an indicator to test whether common method bias exist or not (Kock, 2015). In this study, all factor-level VIFs were range from 1.419 to 2.032, lower than 3.3, so the model can be considered free of common method bias. Based on the above tests, we concluded that common method bias was not a major concern in this study.

## 5.3 Measurement Model Test

We used partial least squares (PLS) with SmartPLS 3.0 to test the measurement model, which evaluates the measurement and structural model at the same time (Gefen et al.,2000). The result is presented in Table 3. All factor loadings of measurement scales were above 0.7 and the average variance extracted (AVE) values of every construct ranged from 0.661 to 0.856, all exceeding 0.50, showing a satisfactory convergent validity. All Cronbach's alpha values and the composite reliabilities (CR) exceeded 0.70, implying a good reliability of the scale.

The convergent and discriminant validity were assessed by checking whether the AVE (average variance extracted) of each construct is larger than its correlation with the other constructs, and whether each item had a higher loading on its assigned construct than on the other constructs (Fornell & Larcker, 1981; Gefen, Straub, & Boudreau, 2005). The results indicate that the discriminate validity was achieved, as shown in Table 3.

## 5.4 Structural Model Test

A bootstrap analysis with 5,000 resampling method was applied to determine the significance of the structural model paths. The path coefficient and significance of each hypothesis were examined and the explained variance ( $R^2$ ) of each dependent construct was calculated. Figure 2 shows the results of the tests. Overall, the model explained 18.4% of the variance for personal information disclosure intention and 33.0% of the variances was explained in privacy view and perceived risk. Specifically, perceived benefit was significantly related to personal information disclosure intention ( $b = 0.151, t = 3.443$ ), which supported H1. Privacy view was significantly related to perceived risk ( $b = 0.575, t = 12.603$ ) and subjective norm was significantly

Table 2  
Common Method Bias Analysis

Construct	Indicator	Substantive factor loading( $R_1$ )	$R_1^2$	Method factor loading( $R_2$ )	$R_2^2$
Perceived Benefit(PB)	PB1	0.81***	0.6561	-0.058	0.003364
	PB2	0.882***	0.777924	-0.061	0.003721*
	PB3	0.805***	0.648025	0.125	0.015625**
Perceived Risk(PR)	PR1	0.925***	0.855625	-0.03	0.0009
	PR2	0.926***	0.857476	0.03	0.0009
Subjective Norm(SN)	SN1	0.906***	0.820836	0.062	0.003844
	SN2	0.907***	0.822649	-0.062	0.003844
Privacy View(PV)	PV1	0.792***	0.627264	0.294	0.086436
	PV2	0.866***	0.749956	-0.075	0.005625
	PV3	0.786***	0.617796		0**
Personal Information Disclosure Intention(PIDI)	PIDI1	0.887***	0.786769	0.05	0.0025*
	PIDI2	0.885***	0.783225	-0.051	0.002601*
Average		0.86475	0.750304	-0.00025	0.01078

Note: \* $p < 0.05$ ; \*\* $p < 0.01$ ; \*\*\* $p < 0.001$

Table 3  
Results of Confirmatory Factor Analysis

Factor	Item	Mean	SD	Factor Loading	Cronbach's $\alpha$	CR	AVE
Perceived benefit	PB1	3.443	1.117	0.828	0.779	0.871	0.693
	PB2	3.364	1.080	0.891			
	PB3	3.807	1.003	0.775			
Perceived risk	PR1	4.325	0.873	0.923	0.832	0.923	0.856
	PR2	4.468	0.773	0.927			
Subjective norm	SN1	3.221	1.059	0.904	0.783	0.902	0.822
	SN2	2.642	1.150	0.909			
Privacy view	PV1	4.321	0.863	0.833	0.747	0.853	0.661
	PV2	4.360	0.920	0.853			
	PV3	4.667	0.686	0.749			
Personal information disclosure intention	PIDI1	2.720	1.206	0.894	0.727	0.880	0.785
	PIDI2	2.190	1.032	0.878			



Table 4  
Correlations and Discriminant Validity of Constructs

	PB	PIDI	PR	PV	SN
Perceived benefit (PB)	<b>0.832</b>				
Personal information disclosure intention (PIDI)	0.203	<b>0.886</b>			
Perceived risk (PR)	0.100	-0.028	<b>0.925</b>		
Privacy view (PV)	0.127	-0.067	0.575	<b>0.813</b>	
Subjective norm (SN)	0.174	0.394	0.034	0.032	<b>0.907</b>

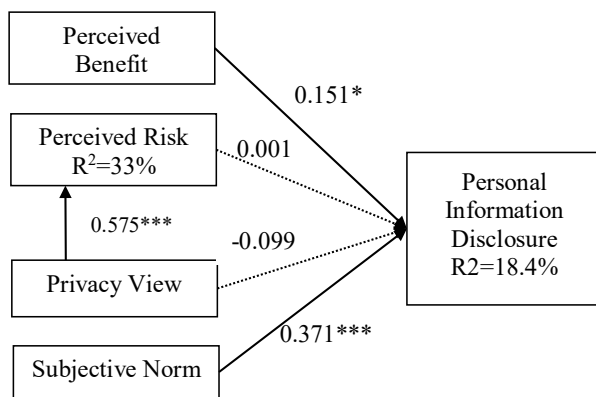


Figure 2. Result of structural model test  
\* $p < 0.05$ ; \*\* $p < 0.01$ ; \*\*\* $p < 0.001$ ; ns: non-significant at the 0.05 level.

associated with personal information disclosure intention ( $b = 0.371$ ,  $t = 8.857$ ), which supported H4 and H5 respectively. H2 and H3 were not supported because they are not significantly related to personal information disclosure intention.

## 6 Discussion and Implications

### 6.1 Discussion of the Preliminary Results

The results verified by previous studies show that perceived risk has a significant negative impact on personal information disclosure intention (Li & Wang, 2015), but the results of this study show that it has no effect. It is mentioned that if users do not provide certain personal information, they cannot use social media functions in the privacy policy to users made by social media. As a result, users have to accept the provision of

personal information even when they perceive risks. It may be one of the possible reasons why the perceived risk does not have a significant impact. It is also possible that users feel that they are lurkers in social media and will not gain too much attention, and whether or not to disclose personal information is not so important. Users' trust in social media brands may also affect users' perceived risks.

With this study, we make two aspects of theoretical contributions to the theory and literature. First, our research uses social media with rich connotations and classifications, which means that our research objects extend to all social media rather than a specific social media, so it can provide some ideas for other specific research. Second, for the Privacy Calculus Theory, our preliminary findings imply that the social media's restrictions on the user's acceptance to use will affect the loss calculation in the user's privacy calculation. The Privacy Calculus Theory needs to consider more adjustment factors.

Drawing on preliminary findings from this study, we also provide some guidelines for social media. First, social media should improve the privacy settings and enhance their privacy protection technology, which should be humanized and easy to use. Second, the more benefits users perceive, the stronger their intention to disclose personal information will be. Therefore, social media should further enhance their use experience and provide users with valuable social services. They can design the corresponding functions to meet users' relationship and instrumental benefit needs, such as self-display, perceived usefulness of life or work, and so on. At the same time, while meeting the basic social needs of users, social media can also provide other personalized functions to ensure users' diverse needs. Third, the proliferation of opportunism has caused various types of information of users' to be stolen or sold. The personal information disclosed by users on social media is varied, which creates various risks. Social media should use content or function as a profitable method and reduce the investment in worthless advertising or unnecessary recommendations. And social media should pay attention to the protection of users' sensitive information and balance the relationship between providing users with personalized services and limiting access to users' personal information.

### 6.2 Limitations and Future Research

There are also some limitations in this study. First, the main sample of this study was middle-aged and young people, while there is still space to optimize research methods and

research objects. Second, this research is only conducted on Chinese social media users, and is insufficient in terms of regional cultural diversity. Therefore, future research will expand the age range and geographical scope of the research objects. Otherwise, some scholars (Awad & Krishnan, 2006) believe that Privacy Calculus Theory is the most useful framework for analyzing user privacy issues; however, our preliminary findings imply that users cannot use some services without accepting personal information, which makes the calculation and balance of users' interests in privacy less obvious. The impact of this factor on the calculation of privacy interests will also be one of the considerations of future research.

**Acknowledgments:** This work was supported by grant from the Social Science Foundation of China (17BTQ079).

## References

- Ajzen, I. (1988). *Attitudes, personality, and behavior*. Homewood, IL, US: Dorsey Press.
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior & Human Decision Processes*, 50(2), 179–211. doi: 10.1016/0749-5978(91)90020-T
- Ajzen, I., & Driver, B. L. (1991). Prediction of leisure participation from behavior, normative, and control beliefs: An application of the theory of planned behavior. *Leisure Sciences*, 13(3), 185–204.
- Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Engle-wood Cliffs NJ: Prentice-Hall.
- Al-Jabri, I. M., Eid, M. I., & Abed, A. (2019). The willingness to disclose personal information: Trade-off between privacy concerns and benefits. *Information and Computer Security*, 28(2), 161–181. doi:10.1108/ICS-01-2018-0012
- Amidon, P. (1992). Widening privacy concerns. *Online (Bergheim)*, 16(4), 64–67.
- Anic, I. D., Budak, J., Rajh, E., Recher, V., Skare, V., & Skrinjaric, B. (2019). Extended model of online privacy concern: What drives consumers' decisions? *Online Information Review*, 43(5), 799–817. doi:10.1108/OIR-10-2017-0281
- Armstrong, J. S., & Overton, T. S. (1977). Estimating nonresponse bias in mail surveys. *Journal of Marketing Research*, 14(3), 396–402.
- Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *Management Information Systems Quarterly*, 30(1), 13–28.
- Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, 53(DEC), 419–426. doi:10.1016/j.chb.2015.07.025.
- Beuker, S. (2016). *Privacy paradox: factors influencing disclosure of personal information among German and Dutch SNS users* (Master thesis, University of Twente). Retrieved from <https://www.semanticscholar.org/paper/Privacy-paradox-%3A-factors-influencing-disclosure-of-Beuker/3b91d3a851ec63d5e0ae8bf5957cb5fe12375edf>
- Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, 6(2-3), 181–202. doi: 10.1007/s10799-005-5879-y.
- CNNIC. (2017). *2016 China social application user behavior research report*. Retrieved from [http://search.cnnic.cn/cnnic\\_search/showResult.js](http://search.cnnic.cn/cnnic_search/showResult.js)
- CNNIC. (2019). *The 44th statistical report on China's Internet development*. Retrieved from <http://www.cnnic.net.cn/hlwfzyj/hlwzbg/hlwjtjbg/201908/P020190830356787490958.pdf>
- Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104–115. doi: 10.1287/orsc.10.1.104
- Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *The Journal of Social Issues*, 59(2), 323–342.
- Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology*, 23(6), 413–422.
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61–80. doi: 10.1287/isre.1060.0080
- Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3), 295–316. doi: 10.1057/ejis.2012.23
- Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook “friends”: Social capital and college students use of online social network sites. *Journal of Computer-Mediated Communication*, 12(4), 1143–1168.
- European Unit. (2018). *General data protection regulation*. Retrieved from <https://gdpr-info.eu/>
- Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50. doi:10.1177/002224378101800104
- Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, 16(1), 91–109. doi: 10.17705/1CAIS.01605
- Guo, H., Ma, H., & Xu, Z. (2019). Construction and demonstration of the influence model of social media users' information disclosure intention: A case study of WeChat users. *Library and Information Service*, 63(15), 111–120. doi: 10.13266/j.issn.0252-3116.2019.15.013
- Guo, Y., Duan, Q. S., & Wang, X.W. (2018). An empirical study on privacy information disclosure behaviour of mobile learning users. *Journal of Modern Information*, 38(4), 98–105+117. doi: 10.3969/j.issn.1008-0821.2018.04.014
- Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. L. (2007). *Analyzing online information privacy concerns: An information processing theory approach*. Paper presented at the Hawaii International Conference on System Sciences. Piscataway, NJ: IEEE. doi: 10.1109/HICSS.2007.81



- Shiau, W. L., & Luo, M. M. (2012). Factors affecting online group buying intention and satisfaction: A social exchange theory perspective. *Computers in Human Behavior*, 28(6), 2431–2444.
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *Management Information Systems Quarterly*, 35(4), 989–1016. doi: 10.2307/41409970
- Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior*, 27(1), 590–598. doi: 10.1016/j.chb.2010.10.017
- Sun, W. J. (2019). *A study on the influence of technical features of privacy management on m-commerce users' information disclosure intention from the perspective of CPM theory* (Master thesis, Central China Normal University). Retrieved from: <https://kreader.cnki.net/Kreader/CatalogViewPage.aspx?dbCode=cdmd&filename=1019204398.nh&tablename=CMFD202001&compose=&first=1&uid=>
- Valk, R.V.R. van der. (2015). *Online disclosure and privacy measures: How we protect our personal information online* (Master thesis, Utrecht University). Retrieved from: <http://dspace.library.uu.nl/handle/1874/317778>
- Varnali, K., & Toker, A. (2015). Self-disclosure on social networking sites. *Social Behavior and Personality*, 43(1), 1–13.
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), 186–204.
- Wang, D. (2011). *Research on SNS users' information disclosure and its impact factors* (MBA Dissertation, University of Electronic Science and Technology of China). Retrieved from: <https://kreader.cnki.net/Kreader/CatalogViewPage.aspx?dbCode=cdmd&filename=1012296825.nh&tablename=CMFD2012&compose=&first=1&uid=>
- Wang, L. Y., & Li, Q. (2016). User's protection behavioral intention of privacy information security on social network site based on the fear appeals theory. *Journal of Intelligence*, 35(12), 69–74. doi: 10.3969/j.issn.1002-1965.2016.12.013
- Wang, Y. B., & Zheng, F. (2016). Review of factors and theories in overseas empirical study of SNS users' personal information disclosure. *Journal of Intelligence*, 35(5), 201–206. doi: 10.3969/j.issn.1002-1965.2016.05.033
- Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, 28(3), 889–897. doi: 10.1016/j.chb.2011.12.008
- Xu, F., Michael, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: An integrated model. *Electronic Commerce Research*, 13(2), 151–168. doi: 10.1007/s10660-013-9111-6
- Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). *Examining the formation of individual's information privacy concerns: Toward an integrative view*. Paper presented at the 29th Annual International Conference on Information Systems (ICIS), 1-16.
- Yang, S., Wang, Y., & Wang, K. L. (2008). The measurement of online users' privacy concern in China context. *Journal of Intelligence*, 27(10), 3–7. doi: 10.3969/j.issn.1002-1965.2008.10.001
- Zhang, R., Chen, J. Q., & Lee, C. J. (2013). Mobile commerce and consumer privacy concerns. *Journal of Computer Information Systems*, 53(4), 31–38. doi: 10.1080/08874417.2013.11645648
- Zhao, L., Lu, Y. B., & Gupta, S. (2012). Disclosure intention of location-related information in location-based social network services. *International Journal of Electronic Commerce*, 16(4), 53–90. doi: 10.2753/JEC1086-4415160403
- Zhu, H., Liu, H. W., Chen, L., & Lu, T. (2014). Consumer perceived risk of information privacy in mobile commerce—From the perspective of a threat avoidance. *Science and Technology Management Research*, 34(16), 216–222. doi:10.3969/j.issn.1000-7695.2014.16.040
- Zlatolas, L. N., Welzer, T., Heričko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. *Computers in Human Behavior*, 45(APR), 158–167. doi: 10.1016/j.chb.2014.12.012

# Appendix

## Questionnaire Items

	Variable	Item	References	Item design
Part one	Social Media Usage	1. Frequently used social media names		Multiple choice
		2. Experience of using social media.	Sun (2019)	Single choice
		3. The average amount of time you spend on social media in a week.	Qiu (2019)	Single choice
Part two	Perceived Risk	4. Disclosure of personal information to social media may lead to disclosure of personal information.	Dinev et al. (2013)	Five-point Likert-type response scale
		5. In general, there are risks in disclosing personal information to social media.		Five-point Likert-type response scale
	Perceived Benefit	6. Social media can help me build identity and a sense of belonging in a virtual community.	Nie et al. (2013)	Five-point Likert-type response scale
		7. I use social media to help shape my opinion.		Five-point Likert-type response scale
		8. I use social media to communicate ideas with others.		Five-point Likert-type response scale
	Privacy View	9. Using social media may bring some privacy issues.	Beuker, S. (2016)	Five-point Likert-type response scale
		10. I care about how others handle my personal information.		Five-point Likert-type response scale
		11. It is important for me to keep my privacy from being violated by others.		Five-point Likert-type response scale
	Subjective Norm	12. Most of the people around me share real personal information on social media.	Xu, F., Michael, K., & Chen, X. (2013)	Five-point Likert-type response scale
		13. Most of the people around me think I should pay attention to the protection of personal information.	Xu, F., Michael, K., & Chen, X. (2013) and Venkatesh & Davis, 2000)	Five-point Likert-type response scale
	Personal Information Disclosure Intention	14. I disclosed real, detailed personal information on social media.	Wang (2011)	Five-point Likert-type response scale
		15. I will disclose more personal information on social media in the future.		Five-point Likert-type response scale
		16. (lie detector)		Five-point Likert-type response scale
Part three	Demographic Information	17. Your gender		Single choice
		18. Your age		Single choice
		19. Your education background		Single choice