An Analysis of the Cause of Privacy Paradox among SNS Users: take Chinese College Students as an Example

Han Menghong
Shanghai University of International Business and Economics
naweidai@163.com

Shen Siqi
Shanghai University of International Business and Economics
sersishen@gmail.com

Zhou Yuexin
Shanghai University of International Business and Economics
anna97061@126.com

Xu Zebing
Shanghai University of International Business and Economics
xuzebing777@163.com

Miao Tianyue
Shanghai University of International Business and Economics
TYLucretia@163.com

Qi Jiayin
Shanghai University of International Business and Economics
qijiayin@139.com

Abstract

It has been proved that the privacy paradox does exist, yet the cause of the phenomenon remains vague. This article tries to analyze the cause of privacy paradox phenomenon on SNS (WeChat) among Chinese college students based on Privacy Calculus Theory and the TPB model and introduces two new factors: the credibility of SNS and the cost of protecting privacy. Through a questionnaire and interview survey, our result shows that there is no significant correlation between users' privacy concerns and the intention of privacy disclosure. While the more users trust the SNS platform, the more possibility they tend to disclose their private information, and the cost of privacy protection can somehow weaken the relationship between the intention and the actual behavior. Therefore, by increasing SNS's credibility, users tend to disclose more personal information to SNS providers, which may improve the competitiveness of SNSs and contribute to their sustainable development.

1. Introduction

In the era of Web 2.0, personal information has already become one of the most vital business resources. However, if SNS providers collect or use personal information arbitrarily and ignore the privacy protection law and regulations, not only users will suffer from the risk of privacy leakage but also SNS providers will bear the loss. Besides, the development path of big data is very likely to be hindered to some extent.

It is universal acknowledge that people now are paying concern on personal information and privacy increasingly, and Europe is at the forefront of privacy protection by enacting The EU General Data Protection Regulation (GDPR), the most strict privacy protection law. Enterprises shall pay more attention when dealing with users' privacy because those who infringe provisions will face the fine maximum up to € 20 million or up to 4% of the annual worldwide turnover of the preceding financial year. Moreover, the huge devastating blow Facebook has suffered for leaking the privacy information to Cambridge Analytica -- a data analysis company served the Trump campaign once again alarm SNS providers the consequence of losing the trust of its users. According to Bloomberg, Facebook's share price fell 6.8% to $172.56 after the crisis, resulting in Zuckerberg's net assets falling to $70.4 billion.

However, high privacy concern does not result in a comparatively high level of protection behavior. According to TechPinions, after the Facebook privacy crisis, only 9% deleted their accounts from their phones and other devices altogether. That is to say, most of the users although perceived the risk chose to use Facebook continuously, and that mainly because the cost of deleting Facebook accounts is too high and results in much inconvenience. This contradiction between the privacy concerns expressed by people and their actual disclosure behavior is called privacy paradox, which is proved to exist by numerous scholars around the world. Various theories have been used to explain this phenomenon, and the most used ones are the Theory of Planned Behavior (TPB) model and the privacy calculus theory. In privacy calculus theory, privacy concern is influenced by perceived risk and perceived benefit, when users see more benefits over risks they tend to disclose their privacy.

While whether this phenomenon exists in China and to what extent it does exist are still under discussion, since some scholars argue that long Chinese history of collectivist culture and tradition may result in a relatively low privacy concern level and a comparatively high privacy disclosure possibility. Besides, what Li Yanhong, the CEO of Baidu (The world's largest Chinese search engine, the largest Chinese website) has said recently may somehow explain the argument. He said, "Chinese are more open to privacy issues and relatively less sensitive, and in many

URI: https://hdl.handle.net/10125/60046
ISBN: 978-0-9981331-2-6

cases, they are willing to disclose privacy for convenience, security or efficiency. Thus we can make use of their information they provided to us and gave them benefits in return." Meanwhile, those scholars who proved the existence of privacy paradox in China conduct their studies focusing on how to protecting users' privacy, however, studies on explaining the cause of the paradox have not yet been fully realized. Moreover, those who tried to analyze the cause of the paradox mainly introduce TPB model or privacy calculus theory, but few of them combine these two theories to address a more comprehensive model to present the dynamic thinking process of users better. Also, concerning the strong antagonism of Facebook's users after Facebook illegally disclosed users' personal information and how they behave, it is necessary to test how the credibility of SNS and the cost of protecting privacy affect users' privacy disclosing the decision.

The remainder of this paper is organized as follows. First, we present the definitions and literature review. Followed by a description of the research theories and hypothesizes, research methodology, and findings. The paper concludes with the implications of the results and directions for future researches.

2. Definitions and Literature Review

2.1 Definition of Privacy

Different areas have different definitions of privacy. In the Web 2.0 era, the definition of privacy needs to be re-examined and defined from various perspectives.

From the perspective of rights, Brandeis and Warren (1890) defined privacy as the right to maintain personal independence [1]. Mason (1986) directly defined privacy as "the right to collect, use, and control personal information [2]." From the perspective of products, Klopfer and Rubenstein (1977) believed that privacy could be seen as an economic term to be used to exchange for the greater value of rights [32]. Laudon (1996) believes that the current crisis in personal privacy information is the result of market failure and calls for market adjustments to focus on privacy through information technology [3]. From the perspective of states, Westin (1967) defined four states of privacy: anonymity, loneliness, backup, and intimacy [1]; Laufer and Wolfe (1977) pointed out that privacy, as a concept of a situation, has three dimensions: self-dimension, environmental-dimension, and interpersonal relationship-dimension [5]. From the perspective of the control ability, Margulis (1977) combined Westin's (1967) and Altman's (1975) views, and finally gave the definition: privacy is the control of various things in people's communication, and the ultimate goal is to improve autonomy or reduce vulnerability [6] [1]. Stone (1990) refined the definition of privacy and stated that "privacy is the ability of one person to control the redistribution or lease of personal information and control the state and quantity of social exchange [7]." This research treats sensitive personal information as a form of privacy for the convenience and accuracy of the analysis.

2.2 Privacy Concern

To measure users' privacy concerns in e-commerce, Malhotra et al. (2004) used social contract theory to design an online consumer privacy concern scale [33], abbreviated as IUIPC. It contains three dimensions of perception: collect, control, and awareness/concerns of privacy practice. The control dimension measures the opinion of online users about their ability to control their own information. The collect dimension measures the degree of consumer concern about the collection and use of personal information by network companies. The awareness/concerns of privacy practice measure the extent to which users are concerned about the privacy practices of network companies. Heng Xu, Tamara Dinev, H. Jeff Smith, Paul Hart (2008) explained the composition of privacy concerns [34].

Shen Qi (2013) used the three dimensions of the IUIPC scale to find out the current privacy concern of university students in Shanghai, and the result showed that students are generally worried about the security of privacy online [12]. In the three dimensions, students are most concerned about their ability to "control" personal information, and their online privacy protection is at an average level. The higher the level of privacy concern, the more privacy protection actions college students will take.

2.3 Privacy Paradox

M. C. Oetzel and T. Gonja defined privacy paradox as "the contradiction between the privacy concerns expressed by people and their actual disclosure behavior [36]." Oomen and Leenes (2008) consider the paradox to be a certain degree of risk perception implies a more excellent knowledge of privacy protection strategies but appears an insufficient motivator to apply such approaches [37]. Many studies have already confirmed the privacy paradox. For instance, A. Acquisti and R. Gross (2005) surveyed students and faculty members in U.S. colleges and universities and found that the specific privacy concerns and actual privacy disclosure behaviors have a significant duality. Most users with a high level of privacy concern will still use Facebook as usual [30]; also, Z. Tufekci's (2008) regression analysis confirmed that the relationship between the privacy concern and information disclosure is weak or the correlation is not relevant [35]. Moreover, S. B. Barnes proved that there is no significant connection between college students' use of Facebook and their privacy attitudes [38]. In China, Shen Qi (2015) proved its

existence among college students in Shanghai [10]; Xitong Guo et al. (2016), confirmed its existence in the field of mobile health services and affected by age differences [14]. Yuanhong and Yating Hou (2016) verified the existence and behavior rules of privacy paradox among SNS generation who are using WeChat by applying the decision tree classification algorithm for data mining [13]. In addition, they found that privacy cognition, the credibility of certain network and involvement of platforms have impacts on privacy paradox.

To summarize, most of the researches on privacy paradox mainly focus on theoretical discussion, only emphasizing its existence, and studies on explaining the cause of the paradox have not yet been fully realized. Moreover, those who tried to analyze the cause of the paradox always confuse the difference between the intention of behavior and actual behavior, while the intention of behavior is actually an essential variable. Therefore, we combine the TPB model and privacy calculus theory to address a more comprehensive model to present the dynamic thinking process of users better. Besides, concerning the strong antagonism of Facebook's users after the Facebook scandal and how they actually behave, it is necessary to test how the credibility of SNS and the cost of protecting privacy affect users disclosing the decision.

3. Theories and Hypotheses Development

3.1 Theories

3.1.1 Privacy Calculus. The privacy paradox can be explained by the privacy calculation theory. The theory of privacy calculus believes that the actual disclosure of information is affected by perceived risk and perceived benefit from the view of risk-return (Culnan, 2000) [48]. Perceived risk refers to the estimated risk of privacy disclosure, and the perceived benefit is generally considered to be interpersonal capitals and social needs like monetary returns or better services.

Various scholars mentioned above attempted to explain the privacy paradox by privacy calculus theory. Zhu Hou et al. (2016) found that perceived risk affects privacy concern positively and affects self-disclosure negatively, while perceived benefits affect self-disclosure positively and affect privacy concern negatively [17]. That means if SNS providers improperly collect and use or even disclose users' personal privacy information, it will increase the perceived risk of users and reduce their participation willingness. On the other hand, when SNS providers are developing or promoting new social media products, they should focus on product management and service mode which allow users to have a more convenient operation management and humanization experience to encourage their continuous motivations.

3.1.2 Theory of Planned Behavior (TPB). Theory of Planned Behavior (TPB) was proposed by Ajzen (1991) which stated that attitude toward the behavior, subjective norms, and perceived behavioral control, together shape an individual's behavioral intentions and behaviors [25]. He introduced a third variable, "behavioral intention" to explain the contradiction between attitude and behavior. Ajzen believes that behavioral intention is the tendency of an individual to take a particular behavior. Therefore, it is a necessary process before any behavior, which is the decision before the act. Dienlin and Trepte (2015) used the concept of behavioral intention to illustrate the process from privacy concern to the actual act of behavior [26]. Xie Gang et al. (2016), proved that the cognition of the importance of network privacy and privacy risk perception positively affect protection consciousness of network privacy, the protection consciousness of network privacy and privacy risk perception positively affect behavior intention [27]. Zhu Hou et al. (2016) based on Privacy Calculus theory and combined with the TPB model established a model about the relationship between privacy concern and privacy disclosure of SNS users proved that users' perceived risk positively influence their privacy concerns, which in return decrease the intention of privacy disclosure, however, when perceiving high level of benefits, users' intention of disclosure would be enhanced significantly, which leads to the final disclosure action [17].

In addition, behavioral intention is the tendency of actual behavior, and it directly determines behavior under conditions where actual control conditions are sufficient. Although the actual behavior is affected by various factors, behavioral intention can predict actual behavior to some extent. This view was proved by Burns S, Roberts L. in 2013 [19], and Xie Gang et al. (2016) found out the stronger the intention of privacy disclosure, the more users likely to actually disclose their privacy.

3.2 Conceptual model and hypotheses

Referred from the model applying for the Theory of Planned Behavior constructed by Dienlin and Trepte (2015) [18] and Feng Xu et al. (2013) [16] as well as the privacy scandal of Facebook, we introduced two factors " the credibility of WeChat" and "the cost of protecting privacy" to see how these two factors will affect the intention of privacy disclosure and the actual behavior. Our conceptual research model is shown in Figure 1.

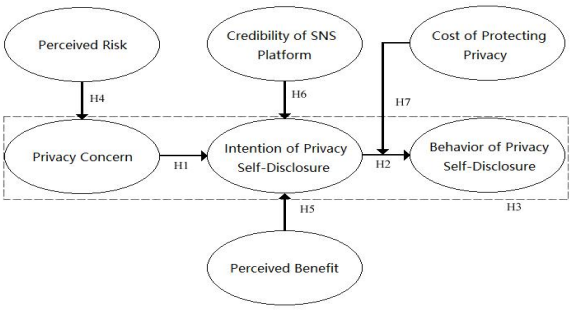

Figure 1. Conceptual Research Model

3.2.1. Privacy Concern and the Intention of Privacy Disclosure. The privacy concern of user is the user's subjective feeling of its privacy state when he or she uses social network applications. It is the concern about the possibility of personal information be stored, stolen or illegally used. The intention bases on the concern, therefore, the higher the level of privacy concern, the lower the intention of privacy disclosure. Moreover, Dienlin and Trepte (2015) hold the view that the intention of privacy disclosure is a process between privacy concern and behaviors of privacy disclosure [26]. Therefore, we get the following hypothesis :

H1: Privacy concern will be negatively related to the intention of privacy disclosure.

3.2.2. The Intention of Privacy Disclosure and Behaviors of Privacy Disclosure. The concept of the behavior of privacy disclosure is cited from Dwyer et al. (2007) [39]. Impressively, the intention of behaviors is the tendency one conducts actual actions. This variable can be defined as the degree of users' willingness to disclose their private information. Theory of Planned Behavior (TPB) proposes a third variable, which is "behavioral intention," to resolve the contradiction between the attitude and behavior. Ajzen (1991) believes that behavioral intention is the tendency of an individual to take a particular behavior [25]. Therefore, the stronger the intention of privacy disclosure, the higher the possibility of privacy disclosure behavior would be. Thus, we have the following hypothesis:

H2: The intention of privacy disclosure will be positively related to the possibility of privacy disclosure behaviors.

H3: The variable of the intention of privacy disclosure can be regarded as the mediator for the other two variables, privacy concerns, and privacy disclosure behaviors.

3.2.3. Perceived Risks and Privacy Concern. The theory of expectation points out that individual behavior is the result of rational calculations, and people will act in the way that maximizes their returns. Perceived risks and perceived benefits are significant parts of the rational calculation of privacy. Xu H. and Dinev T. (2011) explained the concept of perceived risks [34]. On the aspect of perceived risks, some studies showed that most of the network users perceived risks of privacy when they use social network website and e-commerce platforms. The leakage of personal information may result in personal information being stolen, harassed, and other undesirable consequences. And the leakage of information such as bank cards will increase the possibility of property loss. In this research, perceived risks mean the uncertainty that SNS users feel when they use different social software functions which may cause harm or negative impact on their psychological state, property and they themselves. And the higher the perception of risks of privacy disclosure, the higher the level of concern on the personal privacy when they use social network applications. Jochen Wirtz et al. (2007) stated that the risks of privacy would stimulate some worry about privacy and motivation of privacy protection in any network environment [28]. Therefore, we get another hypothesis:

H4: The perceived risks will be positively related to the privacy concern.

3.2.4. Perceived Benefits and the Intention of Privacy Disclosure. This variable, the concept of perceived benefits is defined by Forman et al. (2008) [45]. And some research suggests that perceived benefits are money and service returns. Nevertheless, In the process of using the social network platform, on one hand, the information exchange brought by the disclosure of personal information can bring a pleasant feeling of social communication to users, on the other hand, the disclosure of personal data can promote the establishment of new social relations and growth of social capital. Krasnova (2012) proposed that the feeling of involvement and pleasure people get when they use the social network is a kind of benefit [29]. Thus, users tend to disclose personal information to obtain the perceived benefits mentioned above. Therefore, we get a new hypothesis:

H5: Perceived benefits will be positively related to the intention of privacy disclosure.

3.2.5. The Credibility of SNS and the Intention of Privacy Disclosure. The integrative models of trust have been forwarded by Mayer, Davis, and Schoorman (1995) and McKnight, Cummings, and Chervany (1998) divide trust into three dimension: the trust in the SNS itself (which also represents trust beliefs in the company or entity behind the SNS), the trust in an individual's own friends, and the trust in everyone (i.e. all SNS users) [41] [42]. While the credibility of SNS in this paper only refers to users' trust in SNS itself, when using all the services provided by SNS in the field of SNS payment, chat, moments as well as various third-parted small intelligent programs. Users' trust in SNS may be affected by the level of privacy protection, reputation, and regulations of the platform. The credibility of SNS will directly affect whether users will disclose their privacy or not.

Many research proved that trust has an essential impact on users' disclosure behavior on SNS. P. Papadoupoulou et al. (2013) did comparative analysis in the context of e-commerce and mobile commerce, and found trust has strong impacts on users' disclosure behaviors [47]; Bergström A (2015) found trust has different impacts on different groups of people on their privacy concern and then influence their behaviors [43]; Morosanc (2015) found customers' trust in the hotel influences their trust in hotel's app, and then influences their disclosure behaviors [44]; Lo and Riemenschneider (2010) conducted research on Facebook users and found that trust in service provider can prompt users to disclose information, and the higher level of credibility, the more chances users tend to disclose information on this platform [24].

The credibility of SNS refers to the user's trust in the use of SNS, and it will be affected by the platform's rules and regulations, reputation, and the level of SNS privacy protection. The credibility of the social platform will affect user status. On the one hand, the higher users' trust in the social network platform, the more frequent they will use the platform. Thus the more likely for users to disclose personal information on this social network platform; on the other hand, the lower the degree of trust in the social network platform, the fewer frequency users use this social network platform when they need to provide some personal information. Therefore, we have a hypothesis:

H6: The credibility of SNS will be positively related to the intention of disclose privacy on SNS.

3.2.6. The Cost of Protecting Privacy and Behaviors of Privacy Disclosure. From users' point of view, Zhang, L. & McDowell, W. C. (2009) proved that although setting up complex codes or changing codes frequently can increase the level of users' privacy safety, few people actually act in this way because it is hard to remember the complicated codes and it takes times to change codes [40]. Also, when chatting or posting a moment on SNS, it is troublesome to grouping contacts. Furthermore, even when annoyed by the platform on privacy issues, the cost of switching to another platform is high.

The cost of protecting privacy means the protective actions people take when using social network applications. Privacy protection actions, such as grouping contacts, setting up complex passwords, and switching to a more secure social software will weaken the ease of using SNS, and replacing social software will result in the loss of social capital on social applications. And we attribute those impacts of privacy protection behaviors as the cost of protecting privacy. With the low cost of privacy protection, people are more likely to the action to protect privacy. Accordingly, the privacy disclosure behaviors will be reduced. At the same time, if one's privacy concern is high, he or she would be more inclined to adopt these privacy protection actions; therefore their intention to disclose privacy as well as disclosure behavior would be reduced. At last, we have a hypothesis:

H7: The cost of protecting privacy will be positively related to the possibility of privacy disclosure behaviors, while the privacy concern is negatively related to the possibility of privacy disclosure behaviors.

4. Research Setting

We choose Wechat as the representative SNS in our study. Up to the second quarter of 2016, the total number of WeChat public accounts of each brand has exceeded 8 million, the number of mobile application connections exceeds 85,000, advertising revenue has increased to RMB 3.679 billion, and WeChat payment users have reached approximately RMB 400 million. WeChat is no doubt the most potent Chinese multi-purpose messaging, social media and mobile payment app.

We select university students from Songjiang University Town as our survey population. Up to 2017, the proportion of netizens in the 20-29 age group is the highest, reaching 30.0% among the 277 million users, and constitutes for 77.3% of SNS users according to CNNIC [49]. Besides, this age group has higher consumer propensities and more personalized spending habits, which is the primary target SNS providers would like to retain and attract. Most importantly, it is proved that university students care more about personal information and privacy. Songjiang University Town located in one of the most highly developed and open cities -- Shanghai, and has seven tertiary universities in diversified fields, acknowledged as China's biggest tertiary education hub on the mainland.

5. Research methodology

5.1 Questionnaire Design and the Sample

To test the hypotheses mentioned above, we design a questionnaire to measure the different variables in our research model. The questionnaire is divided into two parts. The first part is about the personal information of the participants, including gender, major and their grades in universities. The second part is applied to measure the seven variables. A five-point Likert scale is used to measure different variables that will be described in the following section. All questions for measurement are mixed up and re-categorized into different topics of questions to ensure the accuracy of the results.

To cater to the research subjects, who have habits of surfing online, we invite university students to do the online questionnaire on www.wjx.com, which is a popular website among university students for the survey. The duration is

about one month in January 2018. We collected 154 valid data results altogether from the questionnaire.

5.2 Introductions of Variables and measurement

5.2.1 Perceived Risks. According to Xu H. and Dinev T. (2008)'s definition for perceived risks [34], we designed questions on how worried university students feel about the potential threats of privacy self-disclosure, containing three questions.

5.2.2. Privacy Concern. According to Lo J. and Riemenschneider C (2010)'s definition of privacy concern [24], we used eight questions to measure this variable.

5.2.3. Perceived Benefits. This variable is defined by Forman et al. (2008) [45]. We asked the participants four questions about how they feel while using SNSs such as WeChat.

5.2.4. The intention of Privacy Self-disclosure. This variable can be defined as the degree of users' willingness to disclose their private information. Based on this definition, we get our measurement.

5.2.5. The behavior of privacy Self-disclosure. The concept of the behavior of privacy Self-disclosure is collected from Dwyer et al. (2007) [39]. To measure university students' privacy self-disclosure behavior, we use eight questions to measure this variable.

5.2.6. The cost of protecting privacy. This variable can be defined as how much effort a participant would like to make to protect his or her privacy.

5.2.7. The credibility of SNS platform (WeChat). This variable is defined as the degree of the participants' trust in SNS platforms, in this case, WeChat.

6. Construct Reliability and Validity of the Variable Data

6.1 Construct Reliability of the Variable Data

Before applying the data directly, we need to test the reliability of these measurements. If possible, we need to implement a dimension reduction method for the data of the seven variables.

The result shows that all the Cronbach's Alpha coefficient for the seven variables is over 0.7, which implies that the measurement is reliable.

6.2 Construct Validity and Apply Dimension Reduction Method for the Data

We carried out explanatory factors analysis to test the validity of the measurement. We measured the different factors loading of the measurements, the degree of total variance explained of the variables to test whether the variable is suitable for the factor analysis and can represent the majority to construct validity for the data.

From the test, the degree of total variance explained of the variables relatively is over 60%, which implies that the explanatory factor analysis is acceptable to reduce the dimensions of the measures of variables. In addition, all the KMO value for these variables are beyond 0.7, implying that it is suitable to perform factor analysis here.

7. Data Analysis and Results

7.1 Data Analysis and Results

We use AMOS to test all the hypotheses. The results can be shown in Figure 2. We rejected H1 (Privacy concern will be negatively related to the intention of privacy disclosure) and H5 (Perceived benefits will be positively related to the intention of privacy disclosure) since their P values are higher than 0.05, and other hypotheses are acceptable and statistically significant. The intention of privacy self-disclosure (IoPSD) positively influences (0.741) the possibility of privacy self-disclosure behaviors (BoPSD) (H2). Perceived risk (PR) positively influences (0.603) privacy concern (PC) (H4). The credibility of the SNS platform (CoP) positively influences (0.441) the intention of privacy self-disclosure (IoPSD) (H6). Table 1. provides detailed results.

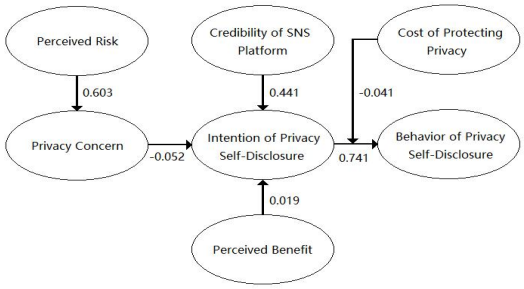

Figure 2. Analysis Results of Formative Measures

Table 1. Structural Model and Relation Paths

Hypothesis	Relation Path			Coefficient Estimated	P value
H1	PC	--->	IoPSD	-0.052	0.073
H2	IoPSD	--->	BoPSD	0.741	0.032
H4	PR	--->	PC	0.603	0.000
H5	PB	--->	IoPSD	0.019	0.056
H6	CoP	--->	IoPSD	0.441	0.002

7.2 Confirmatory Mediation Analysis

To test the hypothesis 3, based on the theory of planned behavior (1991) [25], we've already proved that there is no significant correlation between privacy concern and the intention of privacy self-disclosure, therefore, we conclude that the variable of the intention of privacy cannot be regarded as the mediator for the other two variables, privacy concerns, and behaviors of privacy self-disclosure.

To test the hypothesis 7, we carried out an additional two-step process. In the first step, we introduced the moderating variable the cost of protecting privacy. We have already tested that the intention of privacy self-disclosure positively influences the possibility of privacy self-disclosure behavior. Here we would like to explore if the cost of protecting privacy can be the moderating variable of the relation from H2. Then we determined the extent of the interaction effect, which equals to the intention of privacy self-disclosure multiply the cost of protecting privacy. The result showed that the moderating effect is significant (0.067). Here the path coefficient of the moderating effect reaches 0.18 which shows a medium-sized moderating effect according to Baron R. & Kenny D. (1986) [46]. In addition, the R Square change after adding this interaction raised by 0.021, which implies that 2.1% more related objected can be explained by the relations of behaviors and intention with the cost of protecting privacy. The following table provides detailed results.

Table 2. Regression Analysis before and after adding the interaction factor

	Change Statistics				
Regression Analysis	R Square Change	F Change	df1	df2	Sig. F Change
Before	.551	92.557	2	151	.000
After	.021	.181	1	150	.067

8. Discussion and conclusion

8.1 Theoretical implications

This study strives to extend prior research on the privacy paradox in China further. Through conducting questionnaires, analyze the collected questionnaire data statistically and using the structural equation analysis method to verify the hypothesis, the verification results show as follows.

First, this study provided the existence of privacy paradox, since there is no significant correlation between the privacy concern and the intention of privacy disclosure (Coefficient Estimated = -0.052, p> 0.05=0.073).

Second, this study empirically unpacked and validated the privacy paradox by privacy concern, the intention of privacy disclosure, and the behavior of self-disclosure based on the Theory of Planned Behavior. The results show that the behavior of self-disclosure is mainly affected by the intention of self-disclosure (Coefficient Estimated = 0.741, p< 0.05=0.032). That is to say, SNS users' privacy disclosure intentions have a substantial and significant positive impact on their actual disclosure behaviors.

Third, this study combined the privacy calculus theory with the TPB model. We found that perceived risks are significantly positively related to the privacy concern (Coefficient Estimated = 0.603, p< 0.05=0.000), while perceived benefits are positively related to the intention of privacy disclosure. In other words, when perceiving privacy risks, SNS users will draw in stronger privacy concern. However, it is worthwhile to note that perceived benefits may not significantly affect the intention of privacy disclosure (Coefficient Estimated = 0.019, p> 0.05=0.056). This result differs from that of previous studies, partly because WeChat is a more closed platform that only opens to whom users have confirmed, and partly because there may be other factors that can affect the intention of privacy disclosure significantly. In our model, the credibility of SNS could be one of the factors.

Fourth, this study found out the factor the credibility of SNS that affects the intention of privacy disclosure significantly (Coefficient Estimated = 0.441, p< 0.05=0.002). And since the intention of privacy disclosure significantly affects the privacy self-disclosure behavior (Coefficient Estimated = 0.741, p< 0.05=0.032), it can be concluded that the more SNS users trust in the SNS platform, the more possibility they tend to disclose their privacy. Therefore, it is notable for SNSs like WeChat to make efforts to further enhance rules and regulations concerning privacy, and improve the level of privacy protection to raise reputation and reliability of users. This finding is consistent with the previous conclusion drew by Iacob Cătoiu et al. (2014) [50] on Facebook and Twitter based on the trust model. Furthermore, the consequence of Facebook scandal once again emphasizes how the credibility of SNS matters to the industry. According to a YouGov and The Economist study that eMarketer cites, the number of those who agreed that Facebook was protecting their privacy dropped from 79% in 2017 to just 27% after the Cambridge Analytica news broke, and trust is lowest where Facebook has the most trouble attracting users: the young. "Ultimately the problem here is one of trust," said Julian Sanchez, privacy and technology fellow at the Cato Institute, "If users no longer believe the company is responsibly handling their information or feel they cannot understand the company's policies for sharing their data, and even if they really are making genuine improvements, as it appears they are, once that trust is gone, it's hard to get back."

Moreover, we found the high cost of privacy protection contributes to the more significant gap between the

intention of privacy disclosure and the actual behavior, and the result is the same as that of the research by Shen Qi in 2017. When users find it was troublesome to set up complex passwords, to change codes more frequently, to group contacts or to switch to another platform, they tend to disclose privacy even if they intended not to disclose. Under this circumstance, government and related SNS providers should protect the users by reducing the cost of protecting, therefore, formulating personal information classification protection measures to simplify the process of protecting the privacy of netizens according to individual security needs is needed.

In conclusion, it is vital for SNS providers to notice that the more SNS users trust in the SNS platform, the more possibility they tend to disclose their privacy, in other words, by improving the platform's rules and regulations, reputation, and the level of privacy protection, SNS users tend to disclose more personal information to SNS providers, and it may cost much for users to switch to other SNS. All these will improve SNS providers' competitiveness and contribute to their sustainable development.

In addition, since the data protection regulations in other regions and countries up to now are less strict compared to GDPR, that is to say, not only these regions and countries should accelerate the pace on perfecting the act of personal information protection, but also SNS supports like WeChat should enhance self-regulation in the big data era.

8.2 Field interviewing implications

We also conducted a field interview with 20 college students to go further to find out other reasons that may cause the privacy paradox and try to learn more about how they make decisions. The findings would contribute to the field of privacy protection.

First of all, undergraduates do not have sufficient knowledge of the privacy disclosure environment, in other words, they cannot manage to perceive privacy risks since nowadays many of services Internet companies provided which ask for privacy in return are well-decorated and hard to recognize. Therefore, even they have a high level of privacy concern, this worry may not be converted into the intention or act to protect their privacy. The user's lack of awareness of the social networking environment can be divided into two dimensions: space and time. The insufficiency of any level will cause users to upload personal information while claiming they understand the privacy issues of the social networking sites like Wechat. S. B. Barnes (2016) also pointed out in the relevant research that the registration process of social networking sites, to some extent, confused the users between public and private space, which makes users mistakenly believe that it is safe to disclose personal information on the platform [38]. To solve this issue, college students need more related education giving them the knowledge of how to recognize certain risks and improve their media literacy.

Another reason is "Third Person Effect," which means the users believe that the violation of personal and property safety caused by disclosure of privacy is always far away from him or her, and always happen upon other people. Therefore, they may perceive the risks and have a high level of privacy concern, but they do not tend to take protective measures.

All in all, we would like to address again that it is true that privacy is more and more challenging to protect nowadays and we citizens are all helpless in front of the invisible all-round threats. However, to protect privacy from the source is the only method we can relive the endless nightmare.

9. Limitations and future research directions

Based on self-reported data collection, the survey may fail to adequately measure people's whole privacy protection behaviors in every process. Moreover, the number of the questionnaire we sent may be limited.

It is suggested later scholars can examine this model on all age groups not only the college students. Besides, other SNS needs to be taken into consideration such as Facebook.

10. Acknowledge

This research was supported by The National Key Basic Research Program (No. 2017YFB0803304), National Natural Science Foundation of China (No. 91546121, No. 71231002), major projects of National Social Science Foundation of China (16ZDA055).

11. References

[1] Westin, A. F. Privacy and Freedom, New York: Warren, S. D., and Brandeis, D. L. "The Right to Privacy" Harvard Law Review (4: 5), 1890, pp. 193–220.
[2] Mason, R. O. "Four Ethical Issues of the Information Age" MIS Quarterly (10: 1), 1986, pp. 4–12.
[3] Laudon, K. C. "Markets and Privacy" Communications of the ACM (39: 9), 1996, pp. 92–104.
[4] Weinstein, W. L. "The Private and the Free: A Conceptual Inquiry, " in Privacy: Nomos XIII, J. R. Pennock and J. W. Chapman (eds.), New York: Atherton Press, 1971, pp. 624–692.
[5] Laufer, R. S., and Wolfe, M. "Privacy as a Concept and a Social Issue: Multidimensional Developmental Theory, " Journal of Social Issues (33: 3), 1977, pp. 22–42.
[6] Margulis, S. T. "Conceptions of Privacy: Current Status and Next Steps, " Journal of Social Issues (33: 3), 1977, pp. 5–21.
[7] Stone, E. F., and Stone, D. L. "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms, " Research in Personnel and Human Resources Management (8: 3), 1990, pp. 349–411.

[8] Shen Qi, "Risk and Cost Trade-offs: "Privacy Paradox" in Social Networks," Journalism & Communication, Vol. 24 No. 8, 2017, pp.55-69+127.
[9] May O. Lwin, Jerome D. Williams. "A Model Integrating the Multidimensional Developmental Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online" [J]. Marketing Letters. 2003 (4).
[10] Shen Qi, "Benefits, Risk and Internet Information Privacy Cognition of College Students in Shanghai," Chinese Journal of Journalism & Communication, Vol. 37 No. 7, 2015, pp.85-100.
[11] Shen Qi, "Self- disclosure and Privacy Protection Behavior in SNS: A Case Study of College Students' WeChat Usage," Journalism & Communication, Vol. 22 No. 4, 2015, pp.5-17+126.
[12] Shen Qi, "Internet Information Privacy Concern and Privacy Protection Behavior of College Students in Shanghai," Journalism & Communication, Vol. 35 No. 2, 2013, pp.120-129.
[13] Yuan Hong, Hou Yating, "On Personal Data Privacy Paradox of Network Generation on the Basis of Wechat Usage," Journal of Intelligence, Vol. 35, No. 3, 2016, pp: 169-173+164.
[14] Xitong Guo, Xiaofei Zhang, Yongqiang Sun. The privacy–personalization paradox in health services acceptance of different age groups [J]. Electronic Commerce Research and Applications, 2016, 16.
[15] Sun Xiaoling, Cheng Yang, Zhu Qinghua, "Exploring the Factors of Social Search User's Privacy Disclosure Intention," Journal of Intelligence, Vol. 36, No. 10, 2017, pp: 172－179, 201.

[16] Feng Xu, Katina Michael, Xi Chen. "Factors affecting privacy disclosure on social network sites: an integrated model" [J].Electronic Commerce Research, 2013, 13 (2): 151-168.
[17] Zhu Hou. Wang Ke. Yan Zhijun. Wu Jiang. "An Analysis of Privacy Paradox Phenomenon in SNS Users Based on Privacy Calculus," Journal of Intelligence, Vol. 36, No. 2, 2017, pp: 134－139，121。
[18] Tobias Dienlin, Sabine Trepte. "Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors" [J] Eur. J. Soc. Psychol. 2015 (3).
[19] Burns S, Roberts L．" Applying the theory of planned behavior to predicting online safety behavior"［J］. Crime Prevention and Community Safety，2013，15 (1):48－64.
[20] Monika Taddicken. "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self‐Disclosure" [J]. J Comput‐Mediat Comm 2014 (2).
[21] Rui Chen. "Living a private life in public social networks: An exploration of member self-disclosure" [J]. Decision Support Systems. 2013 (3).
[22] L, M, Wang, <Civil Law>, China Renmin University Press, 2015.
[23] Smith, H. J., Dinev, T., & Xu, H. "Information privacy research: an interdisciplinary review." Society for Information Management and The Management Information Systems Research Centre. 2011.
[24] Lo, J., & Riemenschneider, C. "An Examination of Privacy Concerns and Trust Entities in Determining Willingness to Disclose Personal Information on a Social Networking Site. Sustainable It Collaboration Around the Globe." Americas Conference on Information Systems, Amcis 2010, Lima, Peru, August (pp.46). DBLP.
[25] Ajzen, Icek "The theory of planned behavior." Organizational Behavior and Human Decision Processes. Vol. 50. No.2. 1991. pp: 179–211. Doi: 10.1016/0749-5978(91)90020-T.
[26] Dienlin T，Trepte S. "Is the privacy paradox a relic of the past? An in－depth analysis of privacy attitudes and privacy behaviors"［J］.European Journal of Social Psychology，2015，45 (3):285－297.
[27] Xie Gang, Wang K, Yan Zhijun, and Wu Jiang "The Empirical Research on Influencing Factors of Network Privacy Protection Behavior Intention" [J]. East China Economic Management, 2016.
[28] Lwin, May O., Jochen Wirtz, and Jerome D. Williams. "Consumer Online Privacy Concerns and Responses: A Power-Responsibility Equilibrium Perspective"， Journal of the Academy of Marketing Science，vol. 35，no. 4，2007，pp. 572－585.
[29] Krasnova H, Veltri N F, 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.
[30] Gross R, Acquisti A (2005) Information revelation and privacy in online social networks. In: Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 71–80.
[31] Workshop on Privacy in the electronic society. ACM, 71–80.

[32] P. Klopfer and D. Rubenstein. The concept of privacy and its biological basis. Journal of Social Issues, 33(3):52-65, 1977.
[33] Malhotra N K, Kim S. S, Agarwal J. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a casual model [J]. Information System Research, 2004，15(4)：336-355.
[34] Xu H, Dinev T, Smith J, et al. Information privacy concerns_linking individual perception with institutional privacy assurances [J]. Journal of the Association for Information System, 2011，12(12)：798—824.
[35] Turekci Z. Can you see me now? Audience and disclosure regulation in online social network sites [J]. Bulletin of Science, Technology & Society, 2008，28(1)：20．36.
[36] Oetzel Marie, & Tijana Gonja. The Online Privacy Paradox: A Social\nRepresentations Perspective. In CHI. Vancouver. 2011.
[37] Oomen I, Leenes R. Privacy risk perception and privacy protection strategies. In: de Leeuw E, Fischer Hubner S, Tseng J, Borking J (eds) Policies and research in identity. Springer, Boston, 2008, pp 121–138
[38] Barnes S B. A privacy paradox: Social networking in the United States[J]. 2006, 11(9).
[39] Dwyer C, Hiltz S. R, Passerini K. et al. Trust and privacy concern within social networking sites: A comparison of Facebook and myspace[J]. Amcis, 2007:339.
[40] Zhang L, Smith W W, Mcdowell W C. Examining Digital Piracy: Self-Control, Punishment, and Self-Efficacy[M]. IGI Global, 2009.
[41] Mayer, R.C., Davis, J.H., Schoorman, F.D., 1995. An integrative model of trust. Academy of Management Review 20, 709–734.
[42] Mcknight D H, Cummings L. L, Chervany N L. TRUST FORMATION IN NEW ORGANIZATIONAL

RELATIONSHIPS[J]. Dissertation Abstracts International, Volume: 66-08, Section: B, page: 4484. 1998.
[43] Bergström A. Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses[J]. Computers in Human Behavior, 2015, 53(5):419-426.
[44] Morosan C, Defranco A. Disclosing personal information via hotel apps: A privacy calculus perspective ☆ [J]. International Journal of Hospitality Management, 2015, 47:120-130.
[45] Forman, c., Ghose, A., and Goldfarb, A. Examing the relationship between reviews and sales: the role of reviewer identity disclosure in electronic markets. Information System Research, Vol 19, No.3, 2008, pp:291-313.
[46] Baron, R. M., &Kenny, D. A. The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. Journal of Personality and Social Psychology, 51,1986, pp;1173-1182.
[47] Papadopoulou P, Peletje. Trust and privacy in the shift from e-commerce to m-commerce: a comparative approach [C]. Conference on e-Business, e-Services, and e-Society． Berlin，Heidelberg: Springer，2013, pp:: 50 －60．
[48] Culnan, Mary J. "Protecting Privacy Online: Is Self-Regulation Working?", Journal of Public Policy and Marketing, Vol.19, No.1, 2000, pp:20-26.
[49] China Internet Network Information Center, "The 40th China Statistical Report on Internet Development", 2017, pp:18-21.
[50] I Cătoiu， M Orzan， OI Macovei， C Iconaru. Modeling users' trust in online social networks, 《Amfiteatru Economic》, 2014, 16 (35): 289-302