

Association for Information Systems

AIS Electronic Library (AISeL)

ICEB 2013 Proceedings

International Conference on Electronic Business
(ICEB)

Winter 12-1-2013

User Self-Disclosure On SNSs: A Privacy Risk And Social Capital Perspective

Xi Chen

Yin Pan

Shun Cai

Follow this and additional works at: <https://aisel.aisnet.org/iceb2013>

This material is brought to you by the International Conference on Electronic Business (ICEB) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICEB 2013 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

USER SELF-DISCLOSURE ON SNSs: A PRIVACY RISK AND SOCIAL CAPITAL PERSPECTIVE

Xi Chen, Zhejiang University, China, chen_xi@zju.edu.cn
 Yin Pan, Zhejiang University, China, panyin@zju.edu.cn
 Shun Cai, Xiamen University, China, caishun@xmu.edu.cn

ABSTRACT

The growth and popularity of SNSs such as Facebook and Twitter have created a new world for users to conduct activities such as posting, viewing, sharing, replying and playing. One of the most important user participation behaviors is self-disclosure. This study attempts to investigate the relation between privacy risk and self-disclosure behavior in SNSs and to understand how the users selectively reveal personal information in an environment with high privacy risk. By integrating Communication Privacy Management Theory, Disclosure Decision Model and Social Capital Theory, we propose a SNS user self-disclosure model. In particular, we propose that perceived privacy risk (PPR) and perceived information control ability (PICA) are the two key antecedents of user self-disclosure. We further suggest that the three dimensions of social capital, namely, relational dimension, cognitive dimension, and structural dimension, influence PPR and PICA respectively. A survey was conducted and structural equation modeling (SEM) was employed for data analysis. Our hypotheses are generally supported. Research implications are discussed.

Keywords: Social Networking Sites (SNS), Accuracy of Self-disclosure, Perceived Information Control Ability(PICA), Perceived Privacy Risk(PPR), Social Capital.

INTRODUCTION

Social networking sites (SNS) is a cyber environment that allows the individual to construct his/her profile, sharing text, images, and photos, and to link other members of the site by applications and groups provided on the Internet[4][40]. The growth and popularity of SNSs such as Facebook and Twitter have created a new world for users to conduct activities such as posting, viewing, sharing, replying and playing[53]. Compared with traditional blogging, micro blogging is a more rapid and real-time communication mode, which requires less invested time and generated content, as a result it allows users to update more frequently and it encourages more personal topics[25].

People talk about themselves or their lives is usually considered as self-disclosure. Self-disclosure is a voluntary act that reveals personal information to others[52]. Different from information or knowledge sharing, self-disclosure is more related to revealing personal information and to the issue of privacy [1] and it is good input for building a reliable and trustworthy SNS e-business recommendation system. However, self-disclosure in SNS has its contradictions. On one hand, participants in SNSs expect to disclose more information in a more private level for the sake of self-discovery, gaining social capital, building social identity [11][53]. On the other hand, self-disclosure in SNS is faced with potential privacy threats, such as using the account information to reset users' social security number and reveal private information like birthday or hometown[18].

As we all know, SNSs remain their attractiveness only if people are willing to disclose themselves and communicate with each other. People received the self-disclosure motivation from a social level and then they reveal their information or thoughts in different ways. We want to discovery the process that how people handle the relationship between the desire to disclose and the privacy risk and this may give some advice to the SNSs operating company. Therefore, we attempt to investigate the relation between privacy risk and self-disclosure behavior in SNSs and to understand how the users selectively reveal personal information in an environment with high privacy risk. By integrating Communication Privacy Management Theory, Disclosure Decision Model and Social Capital Theory, we propose a SNS user self-disclosure model. In particular, we propose that perceived privacy risk (PPR) and perceived information control ability (PICA) are the two key antecedents of user self-disclosure. We further suggest that the three dimensions of social capital, namely, relational dimension, cognitive dimension, and structural dimension, influence PPR and PICA respectively.

THEORETICAL BACKGROUND AND LITERATURE REVIEW

Self-disclosure Behavior

The concept of self-disclosure is originally defined in psychology literature as the process that individuals in society transfer personal information and share ideas and emotions [26][27]. Since then, the concept and effect of self-disclosure are widely discussed by scholars. The concept of self-disclosure has been recognized by many prior literature as a multi-dimensional construct, comprising dimensions including (a) the amount of self-disclosure, (b) the intentionality of the person to self-disclose information, (c) the honesty or accuracy of the message being self-disclosed, (d) the depth or intimacy of the message being self-disclosed, and (e) the positiveness or valence of the message being self-disclosed [46][51][52].

Focusing on user behavior in micro blogging websites, we define self-disclosure in SNSs as the process that participants in a social networking site transfer personal information and share ideas and emotion. Compared with traditional blogging, micro blogging is a more rapid and real-time communication mode, which requires less invested time and generated content, as a result it allows users to update more frequently and it encourages more personal topics [25].

Self-disclosure behavior in SNSs shares many commonalities with general information and knowledge sharing behavior. Similarly, the intention of sharing in SNS could be viewed as a function of two decisive factors. In the individual level, participants concern about the benefits they can get from information sharing. In the social level, SNS users may perceive themselves as members in the organization and have participation intentions[2]. However, self-disclosure is different from general information and knowledge sharing in the degree of personal information and emotion exposure, and thus the privacy issue might be more sensitive [1].

Intention to share on SNSs

As one of the crucial activities in SNSs, knowledge or information sharing has been studied by many scholars. On the aspect of individual consideration, participants might care more about the benefits they derive from sharing information. At the same time, SNS users are likely to perceive themselves as members of a group and form participation intentions [2]. Bagozzi and Dholakia modeled participants' intentions to participate together as a group as a function of individual and social determinants. Following their lead, many researchers, such as Dholakia, Bagozzi, and Pearo, have postulated some variables on these two determinants to develop participation theories in the context of virtual communities [11]. Individuals are not only concerned with how they can benefit from information sharing, but also consider group influence, which always generates common standards and pressures people to act.

Therefore, when we study the behavior of self-disclosure in SNSs, both individual and social factors are worth investigating. In the individual part we use the privacy theories to conclude individual behavior and the social capital theory, which was so popular in SNS research, is used to explain the social factors.

Self-disclosure and Privacy Risk

The process of self-disclosure inevitably involves with privacy. Prior research indicates that users' action would be affected by privacy or risk[15][32]. Petronio [39] proposes Communication Privacy Management Theory to explain how people manage their private information under the influence of individual and group. Privacy disclosure is a critical balance after people considering whether to reveal their privacy [7]. In other words, people will set up privacy boundary during the privacy information management process and disclose selectively. Omarzu (2000) propose Disclosure Decision Model to explain the cognitive process of self-disclosure decision. Self-disclosure is a strategic behavior in this model. After the disclosure purpose is settled, users will have subjective assessment of the utility and risk and decide the content, depth, breadth and duration of disclosure [37]. Both of two models consider self-disclosure as a rational decision-making process and have control and evaluation stages.

Both of the Communication Privacy Management Theory and Disclosure Decision Model view privacy risk as a countable factor users will take into account before self-disclosure, meanwhile both of theories include users' perceived information control ability. Research shows that first-order measurement factor of users' information privacy concerns are information collection, information control and consciousness [33]. While facing high level of privacy risk, people will tend to adopt stronger information control behavior [36].

Social Capital Theory

Social capital theory has been proposed to explain different prosocially behavior including community participation [50]. SNS provides different online interactive application such as friend lists, photo albums and search function, letting more and more people to establish and maintain their own social capitals in the social network [14][42]. There are three dimension of social capital, namely, structural dimension, relational dimension and cognitive dimension [9].

The structural dimension describes the pattern, density, connectivity and hierarchy of network [47]. The society and network relations decide who can be contact to and how did it achieve [47], these relations are formed when community members communicate with each other [49]. Burt [5] found individual who was in the center of network and has relation with more other members have the tendency to share continuously. In the internet environment, members have higher centrality will disclose more and reply helpfully [50].

The relational dimension is composed of norms [22][23][31], obligation [23][35], trust [9][23][24][35][41], and identification, which raise people's awareness of collective goals [23][35]. In SNS, trust is defined as the match degree of behavior and own interest users think while others using their private information.[28]. Trust can reduce the perceived privacy risk and enhance the wiliness to communicate and share [13][34].

The cognitive dimension means the resources which can promote the understanding between community members like shared goal, culture and ideas[9][24][55]. Tsai and Hoshal [48] found that shared vision is an important factor in cognitive dimension, it enhances group cohesion significantly and decides the group type. When the community shared vision was given, SNS users will be easy to find the common faith and disclose themselves.

RESEARCH MODEL AND HYPOTHESES

This study investigates the relation between privacy risk and self-disclosure behavior in SNSs and to understand how the users selectively reveal personal information in an environment with high privacy risk. Specifically, we propose that perceived

privacy risk (PPR) and perceived information control ability (PICA) are the two key antecedents of user self-disclosure. We further suggest that the three dimensions of social capital, namely, relational dimension, cognitive dimension, and structural dimension, influence PPR and PICA respectively. Our research model is presented in Figure 1.

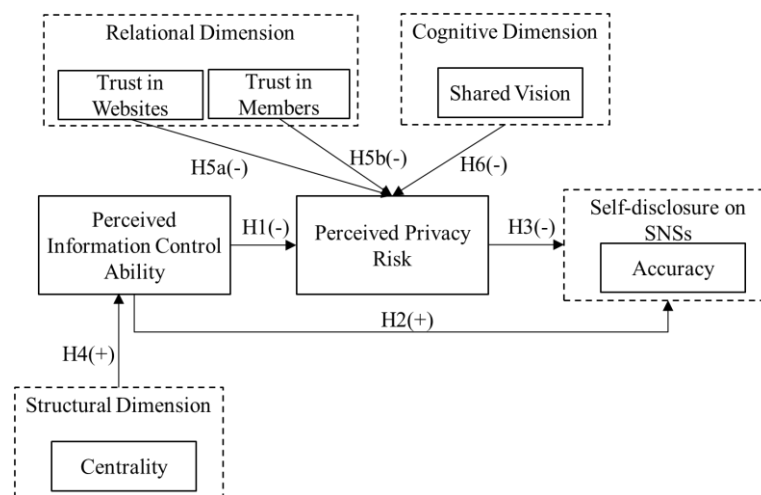


Figure 1 Research Model

Perceived Information Control Ability

In our study, perceived information control ability is defined as the confidence level of SNS users for the relevance of the disclosed information flow and privacy boundary. Research indicates that control is an important factor affecting privacy concerns [33]. Perceived control has a significant negative effect on privacy concerns [54]. In other words, people who have higher level of information control ability will perceive less privacy risk [15]. SNS users who have better information control can handle the information flow better and manage their privacy boundary better, thus they will face less privacy risk. Hence we hypothesized that:

H1: SNS users' perceived information control abilities are negatively associated with perceived privacy risks.

According to Communication Privacy Management Theory and Disclosure Decision Mode, the process of self-disclosure is dynamic and will change as the situation changes. Hence, information control ability may affect the accuracy of self-disclosure. The potential effect should be considered as speculative [43]. Most studies consider information control as a factor will affect the privacy risks but not self-disclosure. However, social network site has a more rapid and real-time communication mode and it may shorten the decision process. Hence we hypothesize that :

H2: SNS users' perceived information control abilities are positively associated with the accuracy of self-disclosure.

Perceived Privacy Risk

Communication Privacy Management Theory has explained how people manage their private information under the influence of individual and group, people will set up the privacy boundary during disclosure process [7]. When the information risk is hard to predict accurately in SNS, people will take the perceived privacy risk as reference for privacy boundary. If users perceive high level of privacy risk in the SNS environment, they will modify the content, such as beautify or hide [32]. We therefore come up with the following hypothesis:

H3: SNS users' perceived privacy risks are negatively associated with the accuracy of self-disclosure.

Social Capital

The factor affecting self-disclosure can be divided to individual factors and social factors and we use social capital theory to interpret the social factors.

In the structural dimension, we use centrality as the measurement. The people who have higher level of centrality will have better control ability to group structure, group attributes and group behavior [3][5][45]. Higher level of centrality means better master degree of privacy information audiences and better perceived information control ability. Hence we hypothesize that:

H4: The centralities of SNS users are positively associated with their perceived information control ability.

In relational dimension, we adopt trust as measurement. Many researches found trust has significant negative influence on perceived privacy risk [13][34]. In the environment of social network sites, the research object of trust can be divided into two kind [13], one is trust on the websites [15][38], another is trust on members [21]. Because of the trust on the website and on the friends, individuals worry less about their private information will be misused or reveal and the perceived privacy risks become lower. Hence we hypothesize that:

H5a: SNS users' trust on websites is negatively associated with the perceived privacy risk.

H5b: SNS users' trust on members is negatively associated with the perceived privacy risk.

In cognitive dimension, we use shared vision as measurement. Shared vision enhances group cohesion significantly and decides the group type [48]. In SNS, users' subjective self-disclosure must associate with their values because of the originality. If individual has higher level of shared vision in the community, the disclosed content will be easier to accept by the audience

and the potential risk will be lower. Hence we hypothesize that:

H6: SNS users' shared visions are negatively associated with the perceived privacy risk.

METHODOLOGY

We used questionnaires to test our hypothesis. To ensure the face validity we adopted mature scale to measure relevant variables. We adjusted each item for the SNS situation and integrate the contents refer to existing literatures.

Table 1 shows the final scale of our questionnaire. A seven point Likert scale was used to measure each item. In the environment of internet, privacy concerns can be divided into abuse and finding[12]. Abuse refers to stolen or improper use of information and finding refers to information observation by improper audiences or information reveal. We choose the finding dimension as measurement because finding has widen range and suitable for the open platform in SNSs. For the measurement of centrality, we asked participants about their friends in SNSs but many participants didn't answer or could only provide approximate numbers. To reduce the uncertainty, we developed a static evaluation scale based on the concept of social enhancement[45]. Social enhancement refers to the acceptance and approval values participants get from other members and users' status enhancement after involvement [6]. Using the static evaluation of social enhancement process is similar with the concept of centrality. Both of the concepts are relevant with uses' status in the community and the relations with others.

The main research object of this study was Chinese college students. We sent 175 questionnaires and received 174. We built strict rules to filter our filled questionnaires and eventually 157 questionnaires were valid. In 157 questionnaires, 155 of them have one or more SNS accounts and 93.5% of them have a SINA micro blogging account. As there were 25 items in the scale, our sample size is 6.2 times of the items number and it is a bit poor for a covariance-based structural equation model(CB-SEM). In a partial least squares structural equation model(PLS-SEM), the minimum sample size should be large as ten times the largest number of formative indicators or the largest number of structural paths directed at a particular latent construct[19]. Our model and sample size met the requirements and could be further analyzed. Hence, We will use SPSS 19.0, SmartPLS 2.0 to analyze the data.

Table 1 Questionnaire items

Variable	No.	Question	Reference
Perceived Information Control Ability (PICA)	PICA1	I will provide accurate and private information only when the websites allows me to control it.	[15][30]
	PICA2	It's very important for me to control my personal information I provided to the website.	
	PICA3	I will provide accurate and private information only when the website control policy is validated or supervised by trusted third party.	
The Accuracy of Self-disclosure (AC)	AC1	My statements about my feelings, emotions, and experiences are always accurate self-perceptions.	[15][30]
	AC2	I always feel completely sincere when I reveal my own feelings and experiences.	
	AC3	I intimately disclose who I really am, openly and fully.	
	AC4	I am always honest in my self-disclosures.	
Perceived Privacy Risk (PPR)	PPR1	When I use SNSs , I have the feeling of being watched.	[12][15][20]
	PPR2	When I use SNSs , I feel all my operations have been tracked or monitored.	
	PPR3	I worry about others can find my following information in SNSs: My birthday and birth place; information of my close family members; home address, work place and phone number of the two; present and previous address and the phone number of the two; Personality traits and interests; Financial and social status.	
Centrality (CE)	CE1	I left a deep impression to other when using SNSs.	[45][50]
	CE2	I feel myself important when using SNSs.	
	CE3	I feel surrounded by friends who care about me when using SNSs.	
Trust on Websites (TW)	TW1	I think the SNSs platform is a trustworthy website for me.	[21][38][44]
	TW2	I can believe that SNSs platform can protect my privacy.	
	TW3	I can believe that SNSs platform will protect personal information from unauthorized use.	
	TW4	It's credible that SNSs platform will keep its promise.	
Trust on Members (TM)	TM1	Even there are opportunities, friends on SNSs won't exploit others.	[8][21][38]
	TM2	My friends on SNSs will keep their promise to others.	
	TM3	My friends on SNSs won't do anything on purpose to destroy communications.	
	TM4	The performance mode of my friends on SNSs is consistent.	
	TM5	My friends on SNSs are sincere during the interactions.	
Shared Vision (SV)	SV1	My friends on SNSs have common goals and hobbies.	[8]
	SV2	My friends on SNSs have similar views and interests.	
	SV3	My friends on SNSs have many similar places.	

DATA ANALYSIS AND DISCUSSION

Descriptive Statistics

We will use the 155 valid questionnaires which have SNS account for further analysis. There are 63 males and 92 females in the participants. 123 participants' education degree is bachelor and 28 participants are master. The average age of the sample is 22.05, ranging from 18 years old to 28 years old. 90.97% participants have registered their SNSs account for more than 6 months. In SNS, only 35.48% people will use their real names but 56.8% people will upload personal real photos and 67.74% people will provide real contact information.

Reliability and Validity

Cronbachs Alpha is acceptable when it's higher than 0.7[17] and it show model have good reliability . As the result in Table 2 we know all the α statics are higher than 0.7 expect perceived information control ability(PICA).Other indicator of PICA have passed the test, so its scale and data are effective. The composite reliability statics of all variables have reached the threshold value of 0.7 [19]. All of the AVE statics are higher than 0.5 and the model have a good convergent validity[16]. Table 3 shows the cross loading of each item, the loading of each variable's item is bigger than other cross loading. Meanwhile, in Table 4 we know the AVE square root of each variable is far higher than the correlation coefficient with other variables and it means the model has good discriminant validity[16]. In a word, the result of reliability and validity is acceptable and further analysis can be continued.

Table 2 Reliability and validity measurement

	Item	Loading	Standard error	T-statistic	AVE	Composite Reliability	Cronbachs Alpha
PICA	PICA1	0.83	0.09	9.19	0.59	0.81	0.66
	PICA2	0.75	0.13	5.88			
	PICA3	0.73	0.13	5.41			
AC	AC1	0.80	0.08	9.80	0.67	0.89	0.84
	AC2	0.82	0.09	9.58			
	AC3	0.80	0.11	7.43			
	AC4	0.85	0.10	8.70			
PPR	PPR1	0.85	0.04	21.99	0.68	0.87	0.77
	PPR2	0.87	0.03	28.03			
	PPR3	0.76	0.06	11.93			
CE	CE1	0.85	0.21	4.13	0.73	0.89	0.83
	CE2	0.84	0.21	3.93			
	CE3	0.88	0.17	5.12			
TW	TW1	0.75	0.06	13.03	0.70	0.90	0.86
	TW2	0.87	0.04	19.85			
	TW3	0.87	0.05	16.94			
	TW4	0.85	0.06	14.81			
TM	TM1	0.84	0.26	3.27	0.72	0.93	0.90
	TM2	0.88	0.25	3.49			
	TM3	0.89	0.24	3.71			
	TM4	0.81	0.21	3.87			
	TM5	0.81	0.21	3.82			
SV	SV1	0.80	0.29	2.72	0.72	0.88	0.88
	SV2	0.99	0.30	3.36			
	SV3	0.73	0.30	2.40			

Table 3 Crossing loading

	PICA	AC	PPR	CE	TW	TM	SV
PICA1	0.83	0.19	0.10	0.18	0.30	0.07	0.03
PICA2	0.75	0.08	0.15	0.16	0.08	0.00	0.09
PICA3	0.73	0.04	0.15	0.11	0.04	-0.07	-0.08
AC1	0.20	0.80	-0.12	0.12	0.14	0.14	0.11
AC2	0.09	0.82	-0.13	0.23	0.24	0.16	0.20
AC3	0.05	0.80	-0.11	0.29	0.32	0.29	0.20
AC4	0.10	0.85	-0.18	0.23	0.34	0.22	0.10
PPR1	0.18	-0.10	0.85	-0.01	-0.30	-0.04	0.05
PPR2	0.05	-0.18	0.87	-0.05	-0.27	-0.08	-0.02
PPR3	0.17	-0.14	0.76	-0.06	-0.26	-0.18	0.02
CE1	0.15	0.16	-0.08	0.85	0.23	0.17	0.18
CE2	0.11	0.22	0.01	0.84	0.24	0.25	0.23
CE3	0.22	0.24	-0.04	0.88	0.24	0.12	0.23
TW1	0.24	0.39	-0.25	0.34	0.75	0.37	0.18
TW2	0.12	0.19	-0.30	0.19	0.87	0.36	0.12
TW3	0.13	0.19	-0.31	0.20	0.87	0.34	0.07
TW4	0.20	0.28	-0.26	0.22	0.85	0.42	0.21
TM1	0.06	0.22	-0.07	0.18	0.46	0.84	0.26
TM2	0.02	0.26	-0.08	0.20	0.41	0.88	0.38
TM3	-0.03	0.19	-0.14	0.13	0.37	0.89	0.34
TM4	-0.01	0.20	-0.10	0.15	0.34	0.81	0.47
TM5	0.08	0.15	-0.06	0.20	0.29	0.81	0.48
SV1	0.12	0.17	0.00	0.18	0.21	0.50	0.80
SV2	0.01	0.16	0.03	0.24	0.15	0.41	0.99
SV3	0.09	0.19	0.00	0.22	0.21	0.45	0.73

Table 4 Correlation coefficient and AVE square roots

	PICA	AC	PPR	CE	TW	TM	SV
PICA	0.77						
AC	0.15	0.82					
PPR	0.17*	-0.17*	0.83				
CE	0.20*	0.25**	-0.05	0.86			
TW	0.20*	0.30**	-0.34**	0.28**	0.85		
TM	0.01	0.24**	-0.12	0.19**	0.44**	0.84	
SV	0.03	0.17*	0.02	0.25**	0.17**	0.44**	0.85

Note: 1. In the lower triangular region there are correlation coefficient between variables and in the diagonal there are the AVE square roots of variables. 2.** indicates significant at the 0.01 level, * indicates significant at the 0.05 level.

Hypothesis Testing

Using SmartPLS 2.0, we set 155 as the sample size and 3000 as the repeat count in Bootstrap test. Finally we have the path analysis result in Table 5. Five of seven original hypotheses have been supported and one of them is reverse.

Table 5 The Result of Hypothesis Testing

Hypothesis		Parameter Estimates	Mean	Standard Deviation	T Statistics	Conclusion
H1	PICA -> PPR	0.25	0.24	0.08	3.23	Support(Reverse)
H2	PICA -> AC	0.18	0.19	0.09	2.03	Support
H3	PPR -> AC	-0.20	-0.21	0.09	2.13	Support
H4	CE -> PICA	0.20	0.22	0.08	2.40	Support
H5a	TW -> PPR	-0.41	-0.41	0.09	4.67	Support
H5b	TM -> PPR	0.02	0.01	0.13	0.19	Not Support
H6	SV -> PPR	0.08	0.07	0.13	0.59	Not Support

Note: T=1.65, p=0.1; T=1.96, p=0.05; T=2.58, p=0.01. [19]

Discussion

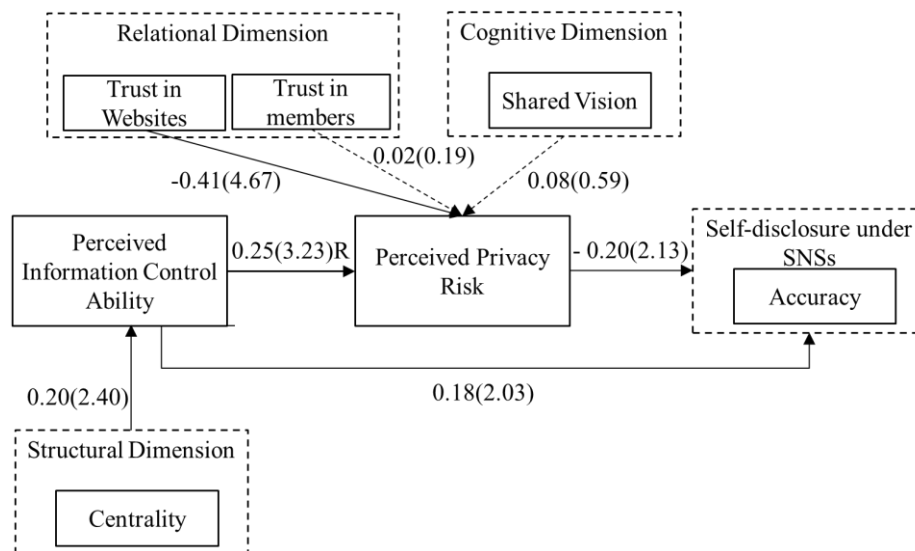


Figure 2 Hypothesis testing results

In Figure 2, the data in each path was showed in the format of "path parameter (T statics)". Five hypothesizes are supported while one of them is reverse with the original hypothesis.

There is existing research shows that perceived control has negative influence on privacy concern[54]. Fogel and Nehmad also think people have stronger information control ability will perceive less privacy risk[15]. Different from their studies, our research result shows that perceived information control ability has positive influence on perceived privacy risk. In a 2009 research of Facebook, there are no significant relation between information control ability and self-disclosure[10]. Different from this research we found there are significant positive relations between perceived information control ability and the accuracy of self-disclosure. We focus on these two hypothesizes different from former researches and think there may be four reason. Firstly, the rapid and real-time communication mode of micro blogging shortens the self-disclosure process. Secondly, as many privacy society events happened, users had more concerns of privacy risk and adopted more strict information release rule. Meanwhile we measurement the perceived information control ability but not real ability and this may reflect the awakening of people privacy concerns. Thirdly, SNSs platform provide more functions for users to control information, such as the audience choice function(appears in Facebook in 2010 and SINA micro blogging in 2012). Fourthly, users take some measures to strengthen information control, for example they can release different content in different kinds of SNSs. We think these two changing path is interesting and worth further study.

Former research indicates that people have higher level of centrality in the community will have stronger control ability of group structure, group attributes and group behavior[3][5][45]. Our research finds that the user's centrality has positive influence on perceived information control ability and we clear the relationship between the two variables.

Trust has significant negative influence on perceived privacy risk [13][34]. The result of our study shows the factors which have negative influence on perceived privacy risk is trust on websites but not trust on members or shared vision in the environment of SNSs. We think the reason may be that most participants' SNSs accounts are in SINA micro blogging platform. The information people released in SINA micro blogging can be read by public and users may not know the true identity of the audience. So the effective trust is still stay at the website level but not member level, and the share vision platform haven't been fully constructed yet.

CONCLUSIONS AND IMPLICATIONS

By integrating Communication Privacy Management Theory, Disclosure Decision Model and Social Capital Theory, we propose a SNS self-disclosure model by identifying perceived information control ability (PICA) and perceived privacy risk (PPR) as two key antecedents of self-disclosure in SNSs. Further, the three dimensions of social capital are identified to be the antecedents of PICA and PPR.

As there were already some articles investigate the self-disclosure behavior in SNS and mainly focused on the effect or performance of self-disclosure. For example, scholars found the interaction effect between self-disclosure and social connection will directly predict Facebook communication and indirectly predict relational closeness[29]. As self-disclosure plays an important part in SNSs, our research focused on the decision process of self-disclosure behavior. From theoretical perspective, this research investigates self-disclosure in SNSs by integrating three theories from different perspectives. Second, this research constructs a self-disclosure model by including both the individual and social factors. Third, we clarify the significant relationship between centrality and perceived information control ability. Last but not least, we found the factor effects perceived privacy risk is trust on websites but not trust on members or shared vision and this may relate to the characteristic of micro blogging.

From practical perspective, our research results may provide some suggestions to the development of SNSs. We discovered the audience choice function can enhance users' information control ability. It's an affirmation for the release of the audience choice function to the operating company(e.g. the group application in Facebook, audience choice function in SINA micro blogging, etc.). Meanwhile, our self-disclosure model gave some directions to promote the accuracy of self-disclosure in SNSs, such as the explicitness of perceived privacy risk. There could be some privacy risk analysis plug-in in SNSs. Finally, we found that, arguably, the trust of SNSs was stay at the platform level but not member level. Future research could be conducted to further verify this issue.

REFERENCES

- [1] Altman, I. & Taylor, D. A. (1973) *Social penetration: The development of interpersonal relationships*, Holt, Rinehart & Winston, Oxford.
- [2] Bagozzi, R. P. & Dholakia, U. M. (2002) 'Intentional social action in virtual communities', *Journal of interactive marketing*, Vol. 16, No. 5, pp. 2-21.
- [3] Borgatti, S. P. & Foster, P. C. (2003) 'The network paradigm in organizational research: A review and typology', *Journal of management*, Vol. 29, No. 145, pp. 991-1013.
- [4] Boyd, D. M. & Ellison, N. B. (2008) 'Social network sites: definition, history, and scholarship', *Journal of Computer-Mediated Communication*, Vol. 13, No. 21, pp. 210-230.
- [5] Burt, R. S. (1995) *Structural holes: The social structure of competition*, Harvard University Press.
- [6] Cheung, C. M., Chiu, P.-Y. & Lee, M. K. (2011) 'Online social networks: Why do students use Facebook?', *Computers in Human Behavior*, Vol. 27, No. 161, pp. 1337-1343.
- [7] Child, J. T., Pearson, J. C. & Petronio, S. (2009) 'Blogging, communication, and privacy management: Development of the blogging privacy management measure', *Journal of the American Society for Information Science and Technology*, Vol. 60, No. 132, pp. 2079-2094.
- [8] Chiu, C. M., Hsu, M. H. & Wang, E. T. G. (2006) 'Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories', *Decision support systems*, Vol. 42, No. 18, pp. 1872-1888.
- [9] Chow, W. S. & Chan, L. S. (2008) 'Social network, social trust and shared goals in organizational knowledge sharing', *Information & Management*, Vol. 45, No. 20, pp. 458-465.
- [10] Christofides, E., Muise, A. & Desmarais, S. (2009) 'Information disclosure and control on Facebook: are they two sides of the same coin or two different processes?', *CyberPsychology & Behavior*, Vol. 12, No. 139, pp. 341-345.
- [11] Dholakia, U. M., Bagozzi, R. P. & Pearo, L. K. (2004) 'A social influence model of consumer participation in network- and small-group-based virtual communities', *International Journal of Research in Marketing*, Vol. 21, No. 2726, pp. 241-263.
- [12] Dinev, T. & Hart, P. (2004) 'Internet privacy concerns and their antecedents-measurement validity and a regression model', *Behaviour & Information Technology*, Vol. 23, No. 150, pp. 413-422.
- [13] Dwyer, C., Hiltz, S. R. & Passerini, K. (2007) 'Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace', *AMCIS*, pp. 339.
- [14] 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*, Vol. 12, No. 4, pp. 1143-1168.
- [15] Fogel, J. & Nehmad, E. (2009) 'Internet social network communities: Risk taking, trust, and privacy concerns', *Computers in Human Behavior*, Vol. 25, No. 131, pp. 153-160.
- [16] Fornell, C. & Larcker, D. F. (1981) 'Evaluating structural equation models with unobservable variables and measurement error'. *Journal of marketing research*, No. 34, pp. 39-50.
- [17] George, D., & Malley, P. (1999). *SPSS for Windows Step by Step: A Simple Guide*. Prentice Hall.
- [18] Gross, R. & Acquisti, A. (2005) 'Information revelation and privacy in online social networks', *ACM*, pp. 71-80.
- [19] Hair, J. F., Ringle, C. M. & Sarstedt, M. (2011) 'PLS-SEM: Indeed a silver bullet', *The Journal of Marketing Theory and Practice*, Vol. 19, No. 156, pp. 139-152.
- [20] Hsu, S. & Shih, D. (2009) 'A model for exploring individual's self-disclosure online', *International Review on Computers and Software*, Vol. 4, No. 116, pp. 594-599.
- [21] Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). 'The value of privacy assurance: an exploratory field experiment', *MIS Quarterly*, Vol. 31, No. 1, pp. 19-33.
- [22] Hutchings, K. & Michailova, S. (2004) 'Facilitating knowledge sharing in Russian and Chinese subsidiaries: the role of personal networks and group membership', *Journal of Knowledge Management*, Vol. 8, No. 41, pp. 84-94.
- [23] Huysman, M. & De Wit, D. (2004) 'Practices of managing knowledge sharing: towards a second wave of knowledge management', *Knowledge and process management*, Vol. 11, No. 42, pp. 81-92.
- [24] Inkpen, A. C. & Tsang, E. W. K. (2005) 'Social capital, networks, and knowledge transfer', *The Academy of Management Review*, Vol. No. 43, pp. 146-165.
- [25] Java, A., Song, X., Finin, T. & Tseng, B. (2009) 'Why we twitter: An analysis of a microblogging community'. *Advances in Web Mining and Web Usage Analysis*, No. 101, pp. 118-138.
- [26] Jourard, S. M. (1959) 'Self-disclosure and other-cathexis', *The Journal of Abnormal and Social Psychology*, Vol. 59, No. 47, pp. 428.

- [27] Jourard, S. M. & Lasakow, P. (1958) 'Some factors in self-disclosure', *The Journal of Abnormal and Social Psychology*, Vol. 56, No. 49, pp. 91.
- [28] Kramer, R. M. (1999) 'Trust and distrust in organizations: Emerging perspectives, enduring questions', *Annual review of psychology*, Vol. 50, No. 52, pp. 569-598.
- [29] Ledbetter, A. M., Mazer, J. P., DeGroot, J. M., Meyer, K. R., Mao, Y., & Swafford, B. (2011). 'Attitudes toward online social connection and self-disclosure as predictors of Facebook communication and relational closeness'. *Communication Research*, Vol. 38, No. 1, pp. 27-53.
- [30] Leung, L. (2002) 'Loneliness, self-disclosure, and ICQ ("I Seek You") use'. *CyberPsychology & Behavior*, Vol. 5, No. 3, pp. 241-251.
- [31] Liu, A. Q. & Besser, T. (2003) 'Social Capital and Participation in Community Improvement Activities by Elderly Residents in Small Towns and Rural Communities', *Rural Sociology*, Vol. 68, No. 58, pp. 343-365.
- [32] Livingstone, S. (2008) 'Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression', *New media & society*, Vol. 10, No. 130, pp. 393-411.
- [33] Malhotra, N. K., Kim, S. S. & Agarwal, J. (2004) 'Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model', *Information Systems Research*, Vol. 15, No. 136, pp. 336-355.
- [34] Mietzner, S. & Lin, L. (2005) 'Would you do it again? Relationship skills gained in a long-distance relationship'. *College Student Journal*, Vol. 39, No. 66, pp. 192-200.
- [35] Nahapiet, J. & Ghoshal, S. (1998) 'Social capital, intellectual capital, and the organizational advantage'. *Academy of management review*, No. 69, pp. 242-266.
- [36] Okazaki, S., Li, H. & Hirose, M. (2009) 'Consumer privacy concerns and preference for degree of regulatory control'. *Journal of Advertising*, Vol. 38, No. 135, pp. 63-77.
- [37] Omarzu, J. (2000) 'A disclosure decision model: Determining how and when individuals will self-disclose'. *Personality and Social Psychology Review*, Vol. 4, No. 134, pp. 174-185.
- [38] Pan, Y. & Zinkhan, G. M. (2006) 'Exploring the impact of online privacy disclosures on consumer trust', *Journal of Retailing*, Vol. 82, No. 142, pp. 331-338.
- [39] Petronio, S. S. (2002) *Boundaries of privacy: Dialectics of disclosure*, Suny Press.
- [40] Pfeil, U., Arjan, R. & Zaphiris, P. (2009) 'Age differences in online social networking—A study of user profiles and the social capital divide among teenagers and older users in MySpace', *Computers in Human Behavior*, Vol. 25, No. 22, pp. 643-654.
- [41] Requena, F. (2003) 'Social capital, satisfaction and quality of life in the workplace', *Social indicators research*, Vol. 61, No. 76, pp. 331-360.
- [42] Resnick, P. (2001) 'Beyond bowling together: Sociotechnical capital', *HCI in the New Millennium*, No. 77, pp. 247-272.
- [43] Senior, V., Weinman, J. & Marteau, T. M. (2002) 'The influence of perceived control over causes and responses to health threats: A vignette study', *British journal of health psychology*, Vol. 7, No. 141, pp. 203-211.
- [44] Shin, D.H. (2010) 'The effects of trust, security and privacy in social networking: a security-based approach to understand the pattern of adoption', *Interacting with Computers*, Vol. 22, No. 151, pp. 428-438.
- [45] Sutanto, J., Tan, C.-H., Battistini, B. & Phang, C. W. (2011) 'Emergent leadership in virtual collaboration settings: A social network analysis approach', *Long Range Planning*, Vol. 44, No. 148, pp. 421-439.
- [46] Tardy, C. H., Hosman, L. A. & Bradac, J. J. (1981) 'Disclosing self to friends and family: A reexamination of initial questions', *Communication Quarterly*, Vol. 29, No. 89, pp. 263-268.
- [47] Tichy, N. M., Tushman, M. L. & Fombrun, C. (1979) 'Social network analysis for organizations'. *Academy of management review*, No. 90, pp. 507-519.
- [48] Tsai, W. & Ghoshal, S. (1998) 'Social capital and value creation: The role of intrafirm networks', *Academy of Management Journal*, Vol. 41, No. 356, pp. 464-476.
- [49] Wang, J. C. & Chiang, M. J. (2009) 'Social interaction and continuance intention in online auctions: A social capital perspective', *Decision Support Systems*, Vol. 47, No. 93, pp. 466-476.
- [50] Wasko, M. M. & Faraj, S. (2005) 'Why should I share? Examining social capital and knowledge contribution in electronic networks of practice', *MIS Quarterly*, No. 124, pp. 35-57.
- [51] Wheelless, L. R. (1978) 'A follow-up study of the relationships among trust, disclosure, and interpersonal solidarity', *Human Communication Research*, Vol. 4, No. 97, pp. 143-157.
- [52] Wheelless, L. R. & Grotz, J. (1976) 'Conceptualization and measurement of reported self-disclosure', *Human Communication Research*, Vol. 2, No. 96, pp. 338-346.
- [53] Xu, C., Ryan, S., Prybutok, V. & Wen, C. (2012) 'It is not for fun: An examination of social network site usage', *Information & Management*, Vol. 49, No. 16, pp. 210-217.
- [54] Xu, H. (2007) 'The effects of self-construal and perceived control on privacy concerns', International Conference on Information Systems, pp. 125.
- [55] Yli-Renko, H., Autio, E. & Sapienza, H. J. (2001) 'Social capital, knowledge acquisition, and knowledge exploitation in young technology-based firms', *Strategic Management Journal*, Vol. 22, No. 98, pp. 587-613.