Effects of Privacy Concern on Trust and Intention to Incremental Usage of Social Networking Systems

Glenn C. Caro[†] · Su Hyeon Namn[††] · Shin Cheol Kang[†††] · Hee Seok Song[†††]

사회네트워크에서 인지된 개인정보보호 수준이 신뢰와 추가적 사용에 미치는 효과

글렌 카로[†] · 남수현[††] · 강신철[†††] · 송희석[†††]

요 약

본 논문은 사회네트워크 (social network system, SNS)에 대한 사용자의 추가적 사용의도를 개인정보보호의 관점에서 고찰하였다. SNS에서 사용자는 SNS의 운영 시스템과 사용자간 정보의 교류가 이루어지는 SNS사이트라는 서로 다른 두 주체와의 상호작용을 통하여 개인정보의 보호 정도를 인지하게 되고, 이러한 인지정도는 사회네트워크시스템과 SNS사이트에 대한 신뢰에 각각 영향을 미치고, 이 신뢰는 사용자의 사용의도를 증가시킨다는 연구모델을 설정하고 가설을 검정하였다. 주요 연구 결과는 SNS 시스템과 SNS 사이트에 대해 사용자가 인지하는 개인정보보호의 수준은 SNS시스템과 SNS사이트에 대한 신뢰 수준에 통계적으로 유의한 영향을 미치는 반면, 사용자의 추가적 사용의도는 단지 SNS 시스템의 신뢰에 의해서만 영향을 받는 것으로 나타났다.

키워드 : 사회네트워크, 개인정보, 신뢰, 추가 사용 의도
(social network system, personal information, trust, intention to incremental usage)

1. Introduction

In a social network system (SNS) there are three entities; a social network system (SN-system) which the users interact through interfaces, a social network company (SN-company) which operates the social network system, and a social network site (SN-site) which refers to the network in which the users communicate with their friends or members.

As one of emerging web 2.0 technologies, online social network sites attract growing number of users who voluntarily participate in communicating and sharing their views and ideas among them. We also note that an

† PhD Program in Information Technology, Hannam Univ
Professor, Philippines State College of Aeronautics, Philippines
†† Professor, Dept of MIS (Corresponding Author), Hannam Univ
††† Professor, Dept of MIS, Hannam Univ
Submitted : 2008-10-31, Accepted : 2008-12-11
* Part of the research is performed by research fund from Hannam Univ (2008A053).

SNS is evolving from fun seeking to purpose driven like recruiting and job searches [28] voting, preference comparison, collective idea generation and so on ([32], [19]), relying on the power of networking of peers. Provision of personal information both to an SN-system when registering and to peers for networking is the key for the successful operation of an SNS.

At the center of the tension between SNS and users lie concerns about personal information protection and trust. In social network site there are two types of trust to be depended upon.

The first type is between SN-system and users and the second one is between a user and his or her peers in SN-site. In both cases the parties involved deal with personal information. As noted in [18], trust becomes an issue when there is dependency relationship.

Furthermore, characteristics of spontaneity, non-task oriented, and heavy dependence on personal information make the most popular original or modified technology acceptance model (TAM, [9][8][36][26][34][6][22]) need to be reexamined.

Research dealing with personal information protection and trust are limited to electronic commerce settings (see for example, [23][21]). We explore the relationship among concerns about personal information, trust and future intention to incremental usage by the framework of theory of reasoned action [12][18].

Organization of the paper is as follows: Theoretical background of related theories, privacy issues, and trust is provided in section 2. Propositions of our research framework and hypotheses are delineated in section 3. In section 4 research methods are given. In section 5 the results of our testing are given. In the final section 6 we include the conclusion, limitations of the research, and the future research direction.

2. Theoretical foundation

2.1 Privacy Issues on SN-system

Personal information privacy is defined as the ability of an individual to personally control information about oneself [25]. More specifically the right to information privacy includes the claim that certain information should not be collected by either government or firms and the controllability of the usage of collected information [20]. Since the definition does not specify the locus of the information, we redefine it as the information that an individual is able to control in terms of the disclosure to a third party or the consequent usage by the third party.

In most of SN-system, profiles of individual members are prepared at the registration. Daily logs are prepared by individuals along with their profiles. The user can put messages in the "wall" in Facebook or "comment" in Friendster of his or her friends. These are the main sources of private data in SNSs. Also when we consider the preemptive attempt by Facebook's Beacon program [33] to scan user's log and announce any product purchase by an individual to all the other members of the subject's network, the amount of private information involved is enormous.

In the literature privacy concerns are used in two different ways.

The first is to measure the dispositional personal perception toward privacy concern in general. The perception is not based on usage or knowledge of privacy protection by a specific system. Three types of individual privacy attitude such as privacy fundamentalists, privacy unconcerned, and privacy pragmatists were defined [17]. In this context the authors emphasized the pragmatists group for soliciting their data and privatization service provision[3]. Application of dispositional privacy concern of this type ranges from Internet privacy concern ([5][11][10]) and individuals' concern on organizational practice of data handling [30][3] to measuring privacy concerns across countries [26].

The second is the perception which reflects situational contexts of specific organizational or social information systems. Examples are the perception of privacy concern of users on an Internet shopping store [21][23][27]. Liu et al. [23] examined the level of privacy concern by the perceived privacy protection by an e-vendor.

Rationally the degree of privacy concern of

individuals is measured by privacy calculus, which involves the analysis of cost-benefit for releasing private information [17] and is a function of many factors such as personality, privacy attitude, type of information released, the recipients, controllability of the information disclosed, and the level of trust on the recipient.

System operators are responsible for appropriate usage of privacy data of customers. Solove [31] argued that there is knowledge asymmetry between system operators and customers for privacy data collection technicalities and the ways of usage: General customers do not have clear idea how his or her private data is collected and for what purposes his data will be used later.

Personal information collected by an SNS can be an important strategic asset as far as the information is collected and used as consented by customers [7]. It implies that organizational policy of personal information should be dealt with systematically in order for the company to build up trust of SNS members.

Much research on privacy has been done. For example, some deal with macro issues of privacy like the relationship of personal information privacy, cultural values, and information privacy regulations [25][4] about the low tendency of information disclosure by a person who prefers higher information transparency [3]. However few papers deal with privacy issues in SNS [1][6][11]. Liu et al. [23] investigated the relationship between privacy concerns, trust and the future usage in E-Commerce (EC) environment.

Based on the literature we propose two dimensions of privacy concern on SN-system; "Unauthorized secondary usage" [30] and "privacy controllability" to measure the perception of users toward the technical aspects of social network technology provided in terms of ease of use and functionality to control the level and visibility of personal information.

2.2 Privacy Issues on SN-site

Privacy concern toward peers in the SN-site is related to the misuses of personal information by peers who are "friended" by an individual.

In an experimental survey, an automatic script contacted 250,000 Facebook users to ask to be friended. Among those engaged 75,000 users accepted the offer and their profile information available to the stranger [1]. This means that an SN-site may be consisted of weak ties to untrustworthy individuals.

Consequently the personal information posted can be misused in such ways as unintended release to random strangers, identity theft, stalking [1], release of the information to a third party, and so on.

Regardless of the purposes of using a SN-site, for example, keeping relationship, space of expressing self, information sharing, etc. [6], if a user feels that the members of a network are not trustworthy in preserving peer private information, the level of trust in the network will be low. In this context we need to consider the antecedents of trust in a virtual group setting, which can be applied to privacy.

Three dimensions of the antecedents such as ability, benevolence, and integrity are proposed [24]. Ability is the degree of trustee's problem solving capability. Integrity refers to the degree of the trustee's keeping rules, norms, and so on so that the trustee's behavior can be predicted in advance. Benevolence is the degree of trustee's affection toward truster.

The concepts were applied to a global virtual team setting [16], where a specific task is given and coordination among the members of the participants is conducted by trust. Note that an SN-site is different from an organizational group which is either virtual or physical since the latter is a task oriented, but the former is used for socializing.

In this regard to measure the perception of how private information of an individual is dealt with by peers, we can borrow the concepts of benevolence and integrity, not ability since the primary role of an SN-site is not task oriented and thus the ability of trustee is not the major issue. In addition considering the spontaneity and loosely connected nature of peers, it is hard to enforce integrity in a group of peers.

Considering these, we propose "transparent usage" as the single construct of privacy concern about peers. Transparent usage is the perceived degree that the privacy information posted by an individual in SN-site

is not manipulated intentionally, and thus their usage by peers is transparent and used as expected.

2.3 Trust

Trust is defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the truster, irrespective of the ability to monitor or control that other party" [24]. Jarvenpaa et al. [16] defined trust as the expectation that others will behave as expected.

In SNS, users deal with two entities: SN-system and SN-site. These are two types of trustee which a user depends on. The first deals with impersonal trust [7] and the other with interpersonal trust [24]. Impersonal trust comes from the users'perception regarding the technical and managerial capabilities of SN-system itself. And interpersonal trust is built upon the dynamics of social network where users interact[35].

2.3.1 Impersonal trust

Literature of trust on information system is mostly centered on electronic commerce (EC) such as e-shopping malls.

Gefen et al. [15] defined trust as the consequent of a set of specific cognitive beliefs in ability, benevolence, and integrity of trustee, which are also proposed as antecedents of trust in [24].

Unlike the general conceptualization of trust as above, Liu et al. [23] measured trust in EC settings as the degree of trustworthiness of online bookstore in terms of the four dimensions recommended by Federal Trade Commission. Liu et al.'s instruments in [23] for measuring trust are rather specific and thus they combine those to derive an overall level of trust.

Gefen et al. [15] proposed an integrated model augmenting the TAM model of IT with trust in the vendor for explaining intended use. In the integrated model, antecedents of trust are defined as familiarity with e-vendor, calculative-based belief, institution-based structural assurances and situational normality.

Laucer and Deng [21] examined the effect of privacy policy which is used as a proxy for organizational privacy practices on the three types of beliefs defined in [24] and used in [16]. Komiak et al. [18] investigated the role of trust for the adoption of recommendation agents.

2.3.2 Interpersonal Trust

Unlike the most of the research on trust deals with dyadic relationships regardless whether it is in impersonal or interpersonal, interpersonal trust in SNS involves social settings, which makes the research environment more complicated.

Fukuyama [13] defined trust as "the expectation that arises within a community of regular, honest, and cooperative behavior, based on commonly shared norms, on the part of the other members of that community." Unlike [24][16], Komiak & Benbasat [18] differentiated trust in terms of cognitive trust and emotional trust. Emotional trust corresponds to trust in general [24] and [16]. Cognitive trust is defined in terms of cognitive trust in competence and cognitive trust in integrity. Compared with [24] and [16], [18] didn't consider "benevolence" type of trust in their model.

Fukuyama [13] recognized social capital as capability created from trust in any size of group whether it is a family or a society. As in the social network in the physical world, online SN-site requires trust for social capital to be accumulated. If an SN-site handles privacy issues appropriately, users of the SN-site will feel more secured about their private data provision and usage, and consequently their interaction among themselves will be trustworthy, richer and stickier, which makes SNS's initiatives toward users become more effective.

However, no research dealing with privacy issues in SNS has been performed so far to accommodate both SN-system and peers in SN-site to ensure privacy protection and to foster social capital among the members of an online social network.

3. Research framework and hypotheses

Our research framework in <Figure 1> can be

justified both from theory of reasoned action (TRA, [12]) related frameworks and from related literatures.

First, the proposed framework follows the general model of belief-attitude-behavioral intention, which is stipulated by TRA and TAM. Based on the theoretical framework and using the lens of privacy concern, the causality of our model can be explained as follows: Privacy concerns (cognitive belief) on both SN-system and SN-site affect the level of trust (attitude) in both SN-system and SN-site. And trust influences the intention to incremental usage of SNS (behavioral intention).

Second, our model is related to privacy-trust-future intention model [23] which deals with impersonal trust in electronic commerce; the privacy concern model of Dwyer et al. [11] which separates trust in SNS into trust in SN-system and other members of SN-site trust model [24][16]. Our model integrates the privacy arising from the interaction of network members, or interpersonal privacy, and disposition to privacy along with the situational and impersonal privacy.

In the framework there are two paths leading to future intention to incremental usage of SNS via trust from privacy preservation by an SNS system and privacy preservation by peers of an SNS. Disposition to privacy affects both trust on SNS system and trust of peers on an SNS.

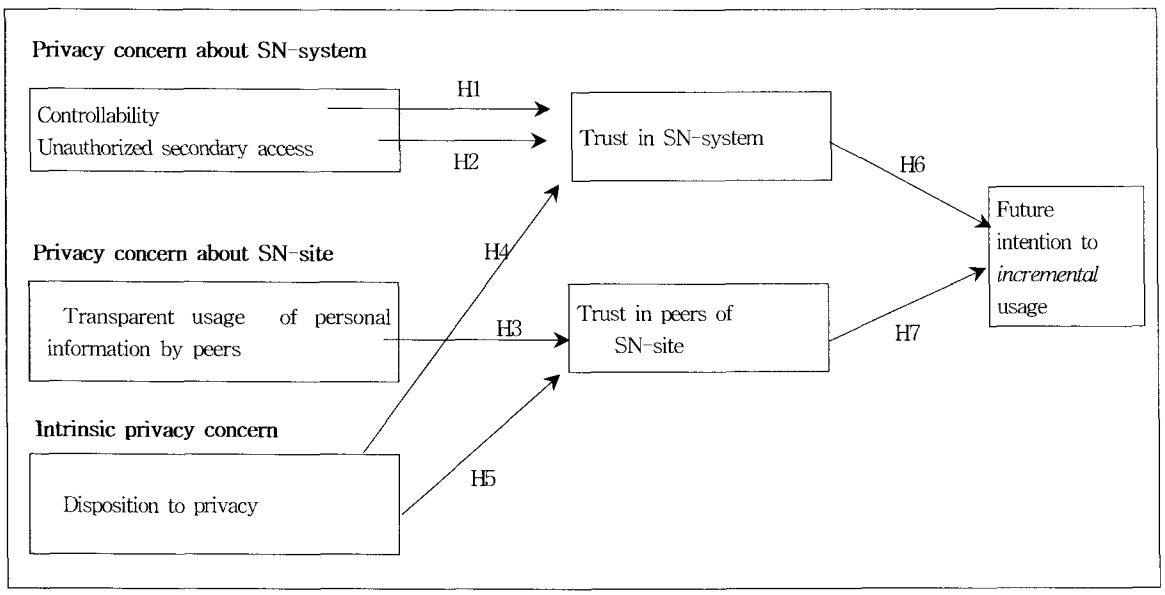
Note that both privacy preservation by an SN-system and privacy preservation by peers play the role of the antecedents of trust. Thus it can be interpreted as the belief in the degree of preserving privacy by an SN-system and peers of an SN-site.

The degree of privacy level is shown to be positively related to the level of trust [23][21]. Based on these findings we propose the following hypotheses:

H1 : The degree of privacy controllability of a user is positively related with the level of trust on SN-system.

H2 : User's perception toward unauthorized secondary use of personal data by the SN-system is negatively related with the level of trust on the SN-system.

In the trust model the theoretical relationship between antecedents of ability, benevolence, and integrity and trust has been has established [24] and shown to have a positive effect on trust [16]. Since we define the construct of privacy preservation of peers on SN-site as just transparent usage, which is adapted from benevolence, we develop the following hypothesis:



〈Figure 1〉 Privacy concern-trust-intention to incremental usage framework

H3: If the level of transparency of personal information usage by peers is high, the trust level of peers on SN-site will be high.

Gefen [14] showed disposition to trust, which is defined as the inclination to adopt a trusting stance toward others, is positively related to trust in E-commerce. Mayer et al. [24] also included truster's propensity as an antecedent of trust. Since we deal with the antecedents of trust in terms of privacy concern, we need to include the intrinsic privacy concern. That is, if a person's disposition to privacy is low, the person is more likely to trust both his SN-system and peers in the same network of his SN-site. Thus, we propose the following hypotheses:

H4: Online privacy concern is negatively related with the trust level of an SN-system.

H5: Online privacy concern is negatively related with the trust level of peers on SN-site.

The consequents of trust have been extensively studied. Trust leads to product inquiry and purchase in E-commerce setting [14], behavioral intention to uses such as repeated purchases, visits, recommendation to others, and positive remarks in online shopping center [23], customer satisfaction and customer loyalty [21] in online settings, and intended use in online shopping [15]. In an SNS environment it is shown that the level of trust in SN-system and the level of trust in other members of SN-site are positively related with the information sharing [11].

In our model we rename the behavioral intention which is widely used terminology in TRA and TAM research as future intention to incremental usage. The reason is that we measure not just continued usage, but increased usage in the future in terms of the number of friends, amount of time consumed, and recommendation to other persons. Based on these findings, we propose the following hypotheses:

H6. Trust level of an SN-system is positively related with the future intention to incremental usage.

H7: Trust level of peers in the same network of one's SN-site is positively related with the future intention to incremental usage.

4. Research Methods

A survey was conducted to test empirically the relationship among perceived privacy, trust and future intention to incremental usage. College students are used as samples for a surrogate of the user population of the social network sites.

4.1 The sample

The majors of students surveyed are diverse: arts, business, science, humanities, and engineering. Also the grades of the students range from freshmen to seniors. Among the students in the roster, we selected only who want to participate in the survey and who have used and thus been familiar with Cyworld, the most popular SNS in Korea. We believe the sample is not biased to represent the SNS population in Korea. The numbers of students participated in the survey are 185. Among those, 21 are discarded because of omitted responses and consistent responses of middle number.

Descriptive statistics of demographic and usage data are given in <Table 1>. Male accounted for 62%, and the age mode is between 21-25 years old. Majority of the respondents consider SNS as a tool for managing and communicating friends, followed by as a medium for self-expression. Respondents are quite exposed to SNS since about 75% of them have used their SNS for more than 2 years and about 80% of them have more than 40 friends in their SN-site, which implies that SNS is not a new information technology, but a mature one to them. So we can assume that they have enough experience to judge their belief on SN-system and peers of SN-site. It also justifies that we can measure the future intention to incremental usage beyond often-used future intention to usage.

4.2 The survey instruments

The instruments along with related literature for

〈Table 1〉 Descriptive Statistics of the Sample

Attribute	Value	Distribution	Percentage	Attribute	Value	Distribution	Percentage
Gender	Male	101	61.6	Number of friends in SN-site	< 40	34	20.7
	Female	63	38.4		41-80	47	28.7
					81-120	31	18.9
					121-160	27	16.5
					> 160	25	15.2
Age	< 20	38	23.2	Usage level - Number of weekly visits to SNS - Number of minutes staying at SNS per visit		Mean 9.43 23.13	Standard deviation 11.7 36.24
	21-25	86	52.4				
	26-30	40	24.4				
Reason for using SNS	Managing friends	83	50.6				
	Self-expression	46	28.0				
	For fun	26	15.9				
	Others	9	5.5				

〈Table 2〉 Itemized instruments of constructs

Construct	Symbol	Description / (- indicates reverse order)	Literature
Controllability (CONTR)	CONTR1	Degree of SN-system's provision of appropriate technologies to control the visibility of personal data to the network.	Privacy issues in Acquisti et al. [1]
	CONTR2	Degree of ease to use control interface	Facebook's interface in [2]
Unauthorized Secondary Usage (UASU)	UASU1	(-) Degree of exploitation of personal data for selfish purpose by SNS	Reworded from Smith et al. [30]
	UASU2	(-) Possibility of sales of personal data to outsiders	
	UASU3	(-) Possibility of sharing personal data with other companies without permission	
Transparent usage (TU)	TU1	(-) Peers'usage of personal for their own purposes	Our own
	TU2	(-) Degree of releasing personal information to a third party by peers	
	TU3	Degree of usage of personal information as it is, not in exaggerated way	Dwyer et al. [11]
	TU4	Degree of getting permission when release of personal information is needed	Our own
	TU5	Recognition peers for the importance of privacy protection	
Disposition to privacy concern (DPC)	DPC1	(-) Degree of concern about online identity theft	Buchanan et al. [5]
	DPC2	(-) Degree of concern about credit card number interception in Internet usage	
	DPC3	(-) Degree of concern about email forward to others	
	DPC4	(-) Degree of concern in general using the Internet	
Trust in SN-system (TSYS)	TSYS1	Degree of dependability of SNS for caring of personal data	Reworded from Lauder & Deng et al. [21] and Gefen [14]
	TSYS2	Degree of comfort for giving personal information to SNS	
	TSYS3	Degree of SNS for doing its job right	
Trust in peers of network (TNET)	TNET1	Degree of dependability of peers	Reworded from Jarvenpaa et al. [16]
	TNET2	Fulfillment of duty and responsibility for use of personal information	
	TNET3	Consideration of peers each other	
Future intention to incremental usage (FIIU)	FIIU1	Willingness to increase the usage of SNS	We added "incremental" from Chung et al. [6]
	FIIU2	Willingness to increase the number of friends	
	FIIU3	Willingness to recommend SNS usage to others	

dispositional privacy concerns, privacy preservation by SN-system, privacy preservation by peers on SN-site, trust in SN-system, trust in peers in SN-site, and future intention to incremental usage are summarized in <Table 2>.

All of the instruments are measured by a seven-point Likert type scale where 1=strongly disagree, and 7=strongly agree.

4.3 Measurement Assessment

To assess measurement we need to test validity and

reliability. Validity can be defined as the degree to which it measures what it is supposed to measure [29]. Validity establishment requires three types of validity such as content and construct related.

Seven of the student in our sample and the three co-authors of this research participated in checking content validity of the measures. Students raised the question that how they know whether the SN-company exploits personal information or not. To solve the problem we included in the questionnaire the remark "The question asks your subjective judgment, not your knowledge of the facts". We also found that the questions with negative verbs may introduce confusions. In the survey we changed from negative sentences into positive ones.

Construct validity refers to the degree to which the responses of instruments collectively capture the construct. Construct validity can be detailed into convergent and divergent validity.

For construct validity we performed factor analysis to see whether the instruments are converged to a specific construct and separated into different factors. The results of a factor analysis extracted by the principal component method with varimax rotation are given in <Table 3>. The instruments are factored into seven specific factors with loadings greater than 0.6,

<Table 3> Factor analysis for construct validity test

Instrument	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6	Factor 7
DPC2	.881						
DPC3	.830						
DPC1	.794						
DPC4	.789						
UASU3		.913					
UASU2		.912					
UASU1		.857					
TU1			.724				
TU2			.694				
TU4			.667				
TU3			.619				
TU5			.549				
FIIU2				.870			
FIIU3				.842			
FIIU1				.805			
TSYS3					.799		
TSYS2					.795		
TSYS1					.760		
TNET2						.846	
TNET1						.842	
TNET3						.794	
CONTR2							.875
CONTR1							.838
Eigenvalue	5.170	3.306	2.315	2.044	1.669	1.176	1.069
% variance explained	22.48	14.37	10.07	8.89	7.26	5.11	4.65
Cummulative %	23.48	36.85	46.92	55.81	63.06	68.18	72.83

<Table 4> Internal consistency reliability

Construct	Symbol	# of instruments	Cronbach's alpha	Construct	Symbol	# of instruments	Cronbach's alpha
Controllability of SN-system	CONTR	2	0.727	Trust in SNS system	TSYS	3	0.831
Unauthorized secondary Usage	UASU	3	0.918	Trust in peers of network	TNET	3	0.842
Transparent usage	TU	5	0.730	Future intention to incremental usage	FIIU	3	0.819
Disposition to privacy concern	DPC	4	0.855				

except TU5, which justifies the convergent and divergent validity.

The internal consistency reliability for all the constructs was checked by Cronbach's alpha which is shown in <Table 4>.

5. Results

The main purposes of the study are to investigate the explaining power of privacy concerns about SN-system and SN-site on trust in SN-system and SN-site, respectively. Also we are interested in the relationship between the two types of trust and the future intention to incremental usage. To test our hypotheses, stepwise multiple regression technique is used. In <Table 5> the models to be tested, R2, R2 change, standardized beta, standard error of beta, t value and variance inflation factor are provided.

MODEL 1:

Relationship between privacy concern about SN-system and trust in SN-system is explained as expected since the model explains about 27%. Concern about SN-system's unauthorized secondary usage (UASU) is the most influential variable, followed by controllability of personal information exposition by users (CONTR).

The implication of the importance of UASU of SN-system is that users judge their trust on SN-system in terms of belief that their SN-company does not use personal data for its own purposes. Compared with UASU, the effect of controllability (CONTR) on trust of SN-system is not so high. The reason might be that the interface of Cyworld is rather straightforward to control the extent of publicity of their personal information. One incident of low controllability was noticed in Facebook, where when users want to cancel their membership, the users found that they had very difficult time to get their profiles to be deleted [2].

On the other hand, dispositional privacy concern (DPC) does not explain any, which is contrary to the findings of [14] in E-commerce and Mayer et al.'s proposition [24] in organizational environment. Mayer et al. [24] argue that dispositional judgment will only affect positively on trust before a trustor discovers other information about trustee. Based on [24], the most of the users in our sample have much experience in their SNS. Thus, we believe that the dispositional effect disappeared. From this model we see that our hypotheses of H1 and H2 are accepted, but H4 is not.

MODEL 2:

Trust in SN-site, the second type of trust in SNS is only measured by transparent usage of personal information (TU) by peer members. The model fitness is 20%, lower than that of MODEL 1.

〈Table 5〉 Statistics of models tested

Model	R^2	R^2 change	beta	S.E.	t	VIF
MODEL 1:						
TSYS=UASU+CONTR+DPC	.268					
UASU		.195	.415	.049	5.940**	1.065
CONTR		.072	.268	.057	3.894**	1.033
DPC		.001	-.019	.052	-0274	1.063
MODEL 2:						
TNET=TU+DPC	.203					
TU		.202	.449	.068	6.375*	1.003
DPC		.001	-.010	.054	-.144	1.003
MODEL 3:						
FIIU=TSYS+TNET	.082					
TSYS		.074	.245	.093	3.105*	1.096
TNET		.008	.091	.090	1.151	1.096

** : significance level at 1%, *: significance at 5% level

We note that SNS is not task-oriented and the peers change dynamically by invitation of new friends and deleting existing ones. So their view of friends on TU can be divergent. For the same reason, the internal reliability of TU construct is not so high. We believe much future research is needed to improve MODEL 2, first identifying more reliable antecedents of trust in SN-site and instruments of trust of SN-site. The difficulty may arise from the fact that an SNS is used for diverse purpose as seen in section 4.1.

There are three types of SNS: LinkedIN is the Chamber of Commerce Luncheon, Facebook is the after-hours party, and MySpace is the all night rave [35]. We believe Cyworld is similar to Facebook or MySpace. If it is used in focused system or work organization like group project in [16], the explainability might be much higher. In the same way, we conjecture that the model would be more fitting to LinkedIn than MySpace, since in LinkedIn reciprocal relationship based on integrity and benevolence is very important for providing personal information and making recruit related decision. Another interpretation might be that the peers are closely tied together in a single organization or a fraternity group in Cyworld. Thus they don't concern much about the exposure of their personal information. However if they think the weak ties through which one is exposed to distant circles, then they may think the issues in different ways.

Dispositional privacy concern (DPC) is also insignificant as in MODEL 1. Users might interpret the risk involved in their personal daily life information which is posted and exchanged is much lower compared with their identification information such as residence number, phone number, and address. In summary, our hypotheses of H3 is accepted, but H5 is not.

MODEL 3:

Future intention to incremental usage (FIIU) is intention to behavior, which is affected by attitude in theory reasoned action. Unfortunately the model fitness is very low, less than 10%. About 90% of the R2 is due to trust in SN-system (TSYS), making the coefficient of TNET insignificant, which is equivalent to the acceptance of H6, but not H7.

Independent of our model, we regressed FIIU against the number of years with SNS, frequency of visits, and the number of friends. The results are: The longer a user has been with an SNS, the less the user becomes loyal to the SNS. But when a user is more active in terms of frequency of visits and the number of friends, the result says that the SNS becomes more sticky. Is it the consequence of user's inertia to a specific system? The question is what makes the users more active. From user's perspective, the value can be obtained from the peer network, not much from SN-system itself.

We believe that SNS is not just a place for fun-seeking, but it should be developed as for a platform where trust driven social capital is accumulated. In this regard, future research may consider a mediating variable, social capital, between trust in SN-site and future intention to incremental usage. Then the strength of the link from trust to future intention to incremental usage in MODEL 3 can be stronger.

For an SNS to grow not from the popularity but from real value to users, the result of MODEL3 should be interpreted as a dilemma for general-type SNS like Cyworld and MySpace.

6. Conclusion, limitations and future work

We examined the effects of privacy concerns toward SN-system and SN-site on trust of SN-system and SN-site, which is again hypothesized to affect the future intention to incremental usage. To our knowledge this is the first attempt to examine the role of privacy concern on both impersonal and interpersonal trust.

The major findings of our research are as follows: Our models confirm that the privacy issues of impersonal system affect significantly the level of trust in SN-system. It also indicates that belief in transparent usage of personal information by peers has positive relationship with the level of trust in interpersonal SN-site. Disposition to privacy concerns

does not affect both impersonal and interpersonal trust.

Impersonal trust model is more convincing than interpersonal trust model in terms of model fitness. The low model fitness of interpersonal trust might be due to such characteristics of Cyworld as non-task oriented, diverse usage purposes of peers, and general-purpose.

For the future intention to incremental usage, it is positively and significantly affected by trust in SN-system, not by trust in SN-site. We provided the sources of insignificant relationship and low model fitness which can be guidelines for enhanced future research.

We note the limitations of this research. First the sample is restricted to a student body so the generalizability of the models may be limited, especially in LinkedIn type SNS where many users are in their 30's and 40's. The second point is that for an exploratory purpose we only tested our research framework in <Figure 1> by a piecemeal approach. In the future a structural analysis will be required to claim the validity of the model itself. The third point is that in the literature the antecedents of the construct, trust in SN-site, are not well developed. We derived our own, but we focused the antecedent on transparent usage of personal information by peers. To explain diverse factors affecting trust in SN-site, a further study is required.

To extend the current research we can choose an SNS with specific purpose-driven, like LinkedIn to investigate the interpersonal trust. One more research area is to look at the cultural difference of privacy concern-trust model. Since an SNS becomes more globally deployed, system designers should take into account the cultural difference in their system design.

References

[1] Acquisti, A. and Gross, R. (2005) "Information Revelation & Privacy in Online Social Networks - The Facebook case)" In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, Alexandria, VA, USA, pp.71-80.

[2] Aspan, M., (2008), "How Sticky Is Membership on Facebook? Just Try Breaking Free", New York Times, Feb 11, 2008.

[3] Awad, N. and Krishnan, M. (2006), "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization," MIS Quarterly, 30(1), pp.13-28.

[4] Bellman, S. (2004), "International Difference in Information Privacy Concerns: A Global Survey of Consumers", The Information Society, 20, pp.314-324.

[5] Buchanan, T., Paine, C., Joinson, A., and Reips, U. (2007) "Development of measures of online privacy concern and protection for use on the Internet", Journal of the American Society for Information Science and Technology, 58(2), pp.157-165.

[6] Chung, Y. and C. Jung (2007), "A study of the effects of perceived characteristics on satisfaction and continuous usage intention in personal communities", The Journal of Information Systems, 16(3), pp. 133-159, in Korean.

[7] Culnan, M. and Armstrong, P. (1999), "Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation", Organization Science, 10(1), pp.104-115.

[8] Davis, F., Bagozzi, R., and Warshaw, P. (1989), "User Acceptance of Computer Technology: A comparison of Two Theoretical Models." Management Science, 35(8), pp.982-1003.

[9] Davis, F. (1989), "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology", MIS Quarterly, September, pp.319-339.

[10] Dinev, T., P. Hart, P. and Mullen, M. (2008), "Internet privacy concerns and beliefs about government surveillance - an empirical investigation", Journal of Strategic Information Systems, vol 17, pp. 214-233.

[11] Dwyer, C., Hiltz, S., and Passerini, K. (2007), "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace", Proceedings of AMCIS 2007, Keystone, CO.

[12] Fishbein, M. and Ajzen, I. (1975), Belief, Attitude,

Intention and Behavior: An Introduction to Theory and Research, Addison Wesley, MA.

[13] Fukuyama, F. (1995), Trust, A Free Press Paperbacks.

[14] Gefen, D. (2000), "E-commerce: the role of familiarity and trust", Omega, 28, 725-737.

[15] Gefen, D., Karahanna, E., and Straub, D. (2003), "Trust and TAM in online shopping: An integrated model", MIS Quarterly 27(1), pp.51-90.

[16] Jarvenpaa, S., Knoll, K. & Leidner, D. (1998), "Is anybody out there? Antecedents of trust in global virtual teams", Journal of Management Information Systems 14(4), pp.29-64.

[17] Kobsa, A.(2007) "Privacy-Enhanced Personalization.", Communications of the ACM, 50(8), pp.24-28.

[18] Komiak, S and Benbasat, I. (2006), "The effects of personalization and familiarity on trust and adoption of recommendation agents", MIS Quarterly 30(4), pp.941-960.

[19] Kuznick, M., E. Singer & J. Goldman (2008), "Sick Transit Gloria" in Breakthrough Ideas for 2008, Harvard Business Review, February 2008, pp.26-27.

[20] Laudon, K. and Traver, C. (2007), E-Commerce, Prentice Hall.

[21] Lauer, T., Deng, X., (2007), "Building online trust through privacy practices", International Journal of Information Security, 6, pp.323-331.

[22] Lee, J. S., H. Cho, G. Gay, B. Davidson, and A. Ingraffea (2003). "Technology Acceptance and Social Network in Distance Learning." Educational Technology & Society 6 (2), pp.50-61.

[23] Liu, C., Marchewka, J.T., Lu, J., and Yu, C (2004) "Beyond concern: a privacy-trust-behavioral intention model of electronic commerce", Information & Management 42, pp.289 - 304.

[24] Mayer, R., J. Davis, and F. Schoorman (1995), "An integrative model of organizational trust", The Academy of Management Review, 20(3), 709-734.

[25] Milberg, S., Burke, S., Smith, H., and Kallman, E. (1995) "Values personal information privacy, and regulatory approaches.", Communications of the ACM,38(12), 1995, pp.65-84.

[26] Moon, J. W. and Kim, Y. G., (2001) "Extending the TAM for a World-Wide-Web context." Information & Management 38, pp.217-230.

[27] Perez, J. (2006), "Social networks influence online holiday shopping", Computerworld, December 25, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9006759.

[28] Rosenbloom, S. (2008), "Status: looking for work on Facebook", New York Times, May 1, 2008.

[29] Rosenthal, R. and Rosnow, R., Essentials of Behavioral Research: Methods and Data Analysis, McGraw-Hill, 1991.

[30] Smith, H., S. Milberg, & S. Burke (1996), "Information privacy: measuring individuals' concerns about organizational practices", MIS Quarterly, June 1996, pp.167-196.

[31] Solove, D. (2004), The Digital Person, New York University Press.

[32] Stalnaker, S. (2008), "Here comes the P2P economy" in Breakthrough Ideas for 2008, Harvard Business Review, February 2008. pp.17.

[33] Story, L & Stone, B. (2007), "Facebook Retreats on Online Tracking", New York Times, November 30, 2007.

[34] Van der Heijden, H. and T. Verhagen (2002), "Measuring and assessing online store image: a study of two online bookshops in the Benelux", 35th Hawaiian International Conference on System Sciences (HICSS).

[35] Tribble, S, "The Social Network as a Career Safety", New York Times, August 14, 2008.

[36] Viswanath, V. and F. Davis (2000), "A theoretical extension of the technology acceptance model: Four longitudinal field studies", Management Science 46(2), pp.86-204.

Glenn C. Caro

1991 Southwestern Univ, Philippines, B.S., Computer Science
2003 Hannam Univ, M.S. in IT
Currently PhD student in Information Technology, Hannam Univ
1991-Present Professor, Philippines State College of Aeronautics, Philippines
Research Interests : social networking system, database management
E-Mail : glendoncaro@yahoo.com

Su Hyeon Namn

1982 Korea Univ, B.A., Statistics
1988 Texas Tech Univ, MBA
1996 Rutgers Univ, PhD., Management
1996-Present Professor, Dept of MIS, Hannam Univ
Research Interests : network application, knowledge management
E-Mail : namn@hnu.kr

Shin Cheol Kang

1982 Korea University, BA, Management
1987 SUNY (Buffalo), MBA
1990 Univ of Nebraska (Lincoln), Ph.D., MIS
1990-1994 Professor, Mokwon Univ
1995-Present Professor, Dept of MIS, Hannam Univ
Research Interests : systems design, process reengineering
E-Mail : cko@hnu.kr

Hee Seok Song

1987 Korea Univ, B.A, Management
1989 KAIST, M.S, Management Science
2003 KAIST, Ph.D., Management Engineering
2003-Present Professor, Dept of MIS, Hannam Univ
Research Interests : data mining, CRM
E-Mail : hssong@hnu.kr