Interacting with Computers 22 (2010) 428–438

Contents lists available at ScienceDirect

Interacting with Computers

journal homepage: www.elsevier.com/locate/intcom

The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption

Dong-Hee Shin *

Department of Interaction Science, Sungkyunkwan University, 90327 International Hall, 53 Myeongnyun-dong 3-ga, Jongno-gu, Seoul 110-745, South Korea

ARTICLE INFO

Article history:
Received 7 December 2009
Received in revised form 11 April 2010
Accepted 16 May 2010
Available online 1 June 2010

Keywords:
Social network services
Perceived privacy
Perceived security
Trust
Web2.0

ABSTRACT

Social network services (SNS) focus on building online communities of people who share interests and/or activities, or who are interested in exploring the interests and activities of others. This study examines security, trust, and privacy concerns with regard to social networking Websites among consumers using both reliable scales and measures. It proposes an SNS acceptance model by integrating cognitive as well as affective attitudes as primary influencing factors, which are driven by underlying beliefs, perceived security, perceived privacy, trust, attitude, and intention. Results from a survey of SNS users validate that the proposed theoretical model explains and predicts user acceptance of SNS substantially well. The model shows excellent measurement properties and establishes perceived privacy and perceived security of SNS as distinct constructs. The finding also reveals that perceived security moderates the effect of perceived privacy on trust. Based on the results of this study, practical implications for marketing strategies in SNS markets and theoretical implications are recommended accordingly.

1. Introduction

Online SNS, such as MySpace, Facebook, and Twitter, have experienced exponential growth in membership in recent years (Barker, 2009). An SNS represents a virtual community in which people with shared interests can communicate by posting and exchanging information about themselves. Internet chat rooms or forums provide users with their own platform to create, build, and share information about activities and interests. The main types of SNS contain directories of some categories meant to connect friends and recommended systems linked to trust (Brocke et al., 2009). Popular methods now combine many of these, with MySpace and Facebook being the most widely used in North America. Twitter has played a critical role in updating real-time basis for the recent Haiti's devastating earthquake. Haitians used Twitter to get words of their situation out to the world, even as those with family in Haiti still could not reach loved ones via cell-phone.

While SNS offer a new range of opportunities for communication and real-time exchange of all kinds of information, privacy and security have emerged as critical issues in the SNS environment (Donath, 2007). A security issue occurs when a hacker gains unauthorized access to a site's protected coding or written language. Privacy issues, those involving unwarranted access of private information, do not necessarily involve security breaches. Anyone can gain access to confidential information by simply watching a user type a password. Both types of breaches often intertwine on social networks, especially since anyone who breaches a site's security network opens the door to easy access to private information belonging to any user. In practice, users often overlook or ignore security and privacy issues of SNS sites (Dwyer, 2007). Personal data about individuals become publicly available in an unprecedented way and extent, including huge quantities of digital pictures and videos. Individuals face possible loss of control over how others will use their data once published on the network. Conversations among users may be recorded indefinitely, can be searched, replicated, and altered, and may be accessed by others without the knowledge of those in the conversation. Publishing one's own personal data may in fact make it available to an entire subscriber community. Very little protection exists at present against copying any kind of personal data from profiles and using them for building personal profiles, or re-publishing the data elsewhere (Boyd, 2008a,b). Personal data from profiles may also leak outside the network when search engines index them. If attackers use an SNS to gather enough personal information to guess a user's password or other authentication mechanism, they can change the user's settings and personal history and track the user's comings and goings. Friends can even create an account and a persona for a real person. A computer security expert, using information publicly available from the Internet, did just that, and the impressive result even fooled the victim's sister (Dwyer, 2007). A malicious third party application that a user allows to run with social networking programs could do the same thing. In addition, some SNS providers make user data available

* Tel.: +82 2 740 1864; fax: +82 2 740 1856.
E-mail addresses: dshin1030@gmail.com, dshin@skku.edu

0953-5438/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.intcom.2010.05.001

to third parties via application programming interfaces, which third parties can then control. A concern continues to grow over security risks, such as the increased threat of identity fraud fostered by the wide availability of personal data in user profiles and by possible hijacking of profiles by unauthorized third parties (Dwyer et al., 2007).

Despite the burgeoning concern over privacy, only a few studies have explored issues of security and privacy in SNS, leading to a paucity of information on how privacy concerns and trust influence acceptance of SNS (Fogel and Nehmad, 2009). This study intends to examine SNS users' attitudes toward privacy and security and their impact on intention by focusing on how the role of trust affects user attitudes and behavior. Although a number of researchers have examined individual privacy concerns and company privacy policies in a diverse web environment (e.g., Hoffman et al., 1999; Jarvenpaa et al., 2000; Kim et al., 2008), we know little about how privacy and security factors in the SNS universe influence individual acceptance. This study proposes a new model that can be applied to social-networking technologies to generate a security and trust model of SNS acceptance. Using the model, the present study develops and validates ways to measure users' perceived privacy and perceived security of their SNS acceptance. The paper then theorizes on influencing trust in SNS use. A structural-equation modeling (SEM) analysis, supported by AMOS, tests the relational model of the antecedents and consequences of attitude toward SNS. The SEM approach allows this study to test vigorously the convergent, discriminant, and nomological validity of the model constructs or the extent to which predictions of the model are verified. When exploring the relationship between social-networking acceptance models, the paper addresses the following research questions:

RQ1: How do the SNS's perceived security and privacy affect people's intention to adopt an SNS?
RQ2: What are the antecedents of trust in the SNS context?
RQ3: What role does trust play in the use of SNS?

The two inquires lead to identifying the role of security and privacy in SNS intention and adoption. Kim et al. (2008) show that improved privacy measures on the web improve perceived security, which has a direct effect on intention to adopt online services. The research further shows that perceived trust is affected and, in turn, affects perceived security and privacy. The present study examines this premise in the SNS context, and the findings should interest both academics and practitioners. From a theoretical perspective, this study provides a new framework of an SNS adoption model by identifying antecedents of user intention to adopt an SNS relative to security and privacy. Although extensive research has looked at factors (like TAM factors such as usefulness, ease of use, and enjoyment) that drive people to adopt and use SNS in general (Boyd and Ellison, 2007; Byrne, 2007; Chiu et al., 2008; Hargittaii, 2007; Kim and Yun, 2007; Rosen and Sherman, 2006), SNS-adoption research focusing on security and privacy has been scarce (Dwyer et al., 2007). This study addresses this gap by examining users' beliefs about security and privacy in SNS. This scholarly contribution provides valuable practical insights for industry. The findings should guide vendors promoting SNS on building user trust by ensuring security assurance both at the Websites and within the individual SNS sites. SNS industries face the challenge of creating a safe and secure environment (Chiu et al., 2008). Interface designs and related elements are rarely examined as qualities in the context of *in situ* user interface. SNS developers should find this study's results useful for future work.

The remainder of the paper is organized as follows: Section 2 offers a literature review of SNS and privacy issues; Section 3 develops the hypotheses tested in the study and proposes the research model; Section 4 describes the research method used in this study; and Section 5 provides the results of empirical tests, followed by a discussion in Section 6. Finally, Section 7 ends with the study's limitations and directions and implications for future research.

2. Literature review: concerns over privacy in SNS

Online social networks represent a fast growing phenomenon and are emerging as the web's top application (Chiu et al., 2008). Millions of people have joined SNS, adding profiles that reveal personal information. One of the most popular online networking sites, Facebook, is designed as an online directory that connects people through social networks at schools (Dwyer et al., 2007). Designed to target high school and college students, Facebook registration used to require a university e-mail address. Data supports anecdotal evidence of heavy use of Facebook, ranking it 10th on the Internet in overall traffic (Baron, 2008). With 8.5 million users per month, about 60% of its registered users visit the site daily (Rosen and Sherman, 2006). Facebook and other SNS sites offer advantageous benefits, including the ability to meet new people, interact efficiently and cheaply with friends and family when circumstances make face-to-face contact difficult, reach a sizable population of other net workers when posting information, tap into other services provided through the site, and access others throughout the world (Ellison et al., 2006). With its immense popularity due to its many benefits, the shortcomings of the current social network deployments have come to light (Barnes, 2007). One of the glaring problems with existing web-based social networks is trust/security management (Acquisti and Gross, 2006). Users share a wide variety of information on SNS, which record all interactions and retain them for potential use in social-data mining (Donath, 2007). Users may open themselves to public scrutiny of their online personas and risk physical safety by revealing excessive personal information. For example, not only are Facebook profiles most often personally and uniquely identified, but also, by default, they show contact information and additional data rarely available on other networks on the web (Joinson, 2008). In most SNS, security, access controls, and privacy are weak by design; the easier it is for people to join and to find points of contact with other users, the higher the utility of the network to the users themselves, and the higher its commercial value for the network's owners and managers. Facebook's platform allows third-party developers to author and market applications to Facebook' s users. More than 20,000 Facebook applications have been developed, with 95% of the user base having run at least one application (Barnes, 2007). These applications pose additional risks. Users may have a false sense of security because of the applications' association with a site they trust. Yet developers release the vast majority of these applications without prior review by the site.

Indeed, inherent privacy risks are associated with SNS, including: (1) inability to control access to the information users post effectively; (2) inability to control the information others post about users effectively; (3) access to sites without identity verification tools; and (4) identity theft, although adequate software protection on users' computers can safeguard against misuse of profile data by third parties. A more recent risk in social networking involves social phishing. A phisher can look at any one of a growing number of SNS to mine information about relationships and common interests in a group or community. Most popular SNS sites identify "circles of friends" that allow a phisher to harvest large amounts of reliable social network information. The fact that the terms of service of these sites may disallow users from abusing their information for spam, phishing, and other illegal or unethical activities is, of course, irrelevant to those who would create fake and untraceable accounts for such malicious purposes (Jagatic et al., 2007).

For the clear conceptualization and operationalization, definitions for key terms in light of SNS are provided as following:

- *Security*: In SNS, security refers to users' perception on security, that is perceived security, which is defined as the extent to which a user believes that using a SNS application will be risk-free.
- *Privacy*: In accordance to previous studies (e.g., Boyd, 2008a,b), privacy in SNS context can be defined as control over the flow of one's personal information, including the transfer and exchange of that information. The protection of the user's privacy to be the main objective for SNS. Privacy within SNS is often not expected or is undefined (Dwyer, 2007).
- *Trust*: Trust in SNS 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 trustor, irrespective of the ability to monitor or control that other party. In SNS, trust is a critical determinant of sharing information and developing new relationships.

3. Research model and hypothesis development: security and trust model in SNS

3.1. Attitude toward SNS

The Theory of Reasoned Action (TRA) suggests that a person's performance of a specified behavior is determined by his or her behavioral intention to perform the behavior, and behavioral intention is jointly determined by the person's attitudes and subjective norms (Ajzen and Fishbein, 1980). The best predictor of behavior is intention, which is the cognitive representation of a person's readiness to perform a given behavior, and it is considered the immediate antecedent of behavior. The TRA defines *attitude toward a behavior* as an individual's positive or negative feeling about performing the target behavior, while *subjective norm* refers to a person's perception that most people who are important to him or her think he or she should or should not perform the behavior in question. In addition, a person's attitude toward a behavior is determined by his or her salient beliefs and evaluations. Given the wide applicability of the TRA in emerging technologies, it is expected that general causalities found in the TRA also apply in a social networking context (Fig. 1).

H1. Attitude toward SNS has a positive effect on the intention to use SNS.

3.2. Perceived security

Online social networking has been criticized because users lack trust in site security (Dwyer, 2007). Given the rising concern over security in SNS (Acquisti and Gross, 2006), this study explores the effect of users' perceived security on intention to use SNS. Yenisey et al. (2005) define *perceived security* as the degree to which people believe in the security of a particular SNS. Therefore, we can interpret subjective security as the mirror image of risk affinity (Dewan and Chen, 2005). Security in interactive spaces does not depend on technical security measures alone (Roca et al., 2009). Kim (2008) shows that the feeling of security is largely determined by the users' feelings of control in an SNS system. Cheung et al. (2005) examined barriers to mobile payment adoption and argued that the lack of subjective security surfaces as the most frequent reason for a refusal to use. Pousttchi (2003) argues that an infringement of subjective security will prevent consumers from using a particular procedure. Linck et al. (2006) developed a set of constructs that explains the nature of subjective security.

In line with previous studies, the current study approaches perceived security from a broader perspective that includes not only technical aspects, such as confidentiality and authentication (Flavian and Guinaliu, 2006), but also the user's comprehensive sense of security and well-being. Of SNS, it can be said that individuals' perceptions of security can differ from real security levels. Although a scientific assessment of security is based on technological solutions, it is the customers' perceptions of security that influence trust and intention (Linck et al., 2006). Previous studies have discovered the role of perceived security in an e-commerce and mobile commerce context, only a few studies have applied it to an SNS context (Acquisti and Gross, 2006; Dwyer, 2007). It is important to establish measures of perceived security and its relationship to trust in the SNS context. Hypotheses regarding perceived security aim to determine how the seal of trust is influenced by perceived security and how perceived security influences the intention to use SNS.

H2. Perceived security positively affects users' trust in SNS.

H3. Perceived security positively affects users' attitude toward SNS.

Perceived security can be confused with perceived privacy. Much of the current debate over privacy concerns a subset of privacy in general, namely electronic or data privacy. In turn, many discussions about data privacy raise the issue of security, which often means information security, and a subset thereof, computer security. Confusion between data privacy and computer security can hinder a user's attempts to achieve excellence in either area. In this study, perceived security is defined as the ability to protect data against unauthorized access, whereas perceived privacy is defined as the ability of an individual to manage information about themselves and thereby reveal themselves selectively.

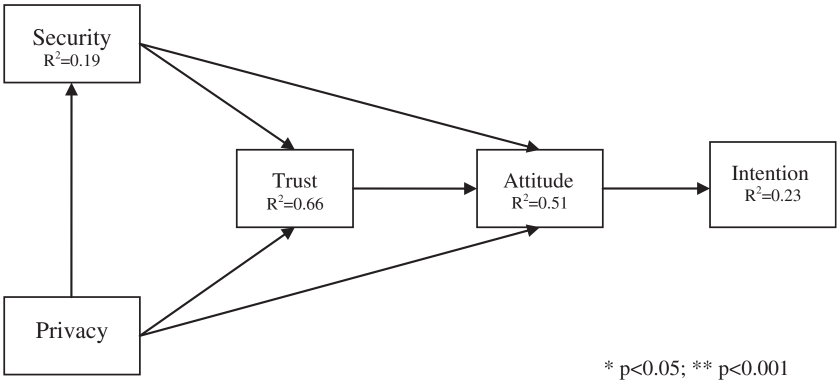

Fig. 1. Research model.

3.3. Perceived privacy

Privacy implications associated with online SNS depend on the level of identifiability of the information provided, its possible recipients, and its possible uses (Dwyer, 2007). Research in the Information Systems (IS) field has argued that information privacy—along with related user concerns—is one of the most important issues in today's technology-based environment (Miyazaki and Fernandez, 2001). The concept of privacy is in itself not new and has generally been defined as an individual's ability to control the terms by which their personal information is acquired and used (Metzger, 2004). The degree to which SNS users feel that an SNS site protects their privacy may also have an impact on their trust of the site. SNS site content influences perceptions of a site's privacy protection through such elements as privacy statements and seals (Kim et al., 2008; Palmer et al., 2000). Research suggests that enhancing perceptions of Website privacy protection via features such as privacy statements and seals may increase regard for the company and trust. For example, Culnan and Armstrong (1999) found that revealing information collection procedures increases consumers' feelings of security and trust. Similarly, Kim et al. (2008) found that having an easy-to-understand privacy policy, which explains how the company will use customer information, predicts trust of a Website. Surveys have found that people are more willing to provide personal information to Websites if they post privacy statements or display privacy seals (Hoffman et al., 1999). Together, these findings suggest that the degree to which SNS users believe an SNS site protects their privacy will positively influence their overall regard for and trust of the company's SNS site. Based on these studies, we can hypothesize:

H4. Perceived privacy positively affects users' trust in SNS.

H5. Perceived privacy positively affects users' attitudes toward SNS.

SNS users may believe that assurances can be guaranteed if the security of the SNS can be guaranteed. This implies that only perceptions of security influences trust in SNS use and any role of privacy perceptions on trust in SNS use is mediated by the user's perceived security. Thus, it can be proposed that the effect of perceived privacy on trust in SNS is mediated by perceived security.

H6. Perceived privacy positively or negatively affects users' perceived security.

3.4. Trust

Reflecting the increasing importance of trust in SNS (Dwyer et al., 2007), this study proposes trust as a central concept: as a subsequent variable of perceived security and privacy and as an antecedent variable to attitudes toward SNS. 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 trustor, irrespective of the ability to monitor or control that other party (Dwyer et al., 2007).

In human interactions, trust has always been an important factor in exchanges involving risk. As trust has been a critical factor in IS (McKnight et al., 2002), it has been extensively addressed as a research topic from different viewpoints and to different levels of analysis. In normal, everyday, face-to-face interactions, trust is a critical determinant for sharing information and developing new relationships (Coppola et al., 2004; Jarvenpaa and Leidner, 1998; Piccoli and Ives, 2003). Trust is also important for successful online interactions. E-commerce research has found trust strongly related to information disclosure (Metzger, 2004). Papadopoulou (2007) shows a positive impact of trust on attitude and intentions. The higher the customers' trust in the web, the less effort customers will exert to scrutinize details of the site to assess its authenticity of services. On a trusted site, because users assume the authenticity of the online service, they will not waste time and cognitive effort and thus will experience higher ease of use. The impact of trust on attitudes is based on the credibility dimension of the trust. Studies of interpersonal exchange situations confirm that trust is a precondition for self-disclosure because it reduces perceived risks involved in revealing private information (Metzger, 2004).

Recently, trust has taken center stage as a serious issue in SNS (Gambi, 2009; Maheswaran et al., 2007); thus it is timely and reasonable to test that trust of a SNS site influences disclosure of personal information to that site. If trust is particularly significant to the process of social interaction, then it is important to ask what fosters trust of a SNS site. Possible factors include seal of trust, perceptions of SNS-site privacy protection, perception of security, users' overall online privacy concerns, and intention to use (Jarvenpaa et al., 2000; Joinson, 2008; Metzger, 2004).

H7. Trust positively affects users' attitudes toward SNS.

4. Research methodology

To have general ideas about users' factors, pre-survey interviews conducted: (1) to cross-validate factors identified from the literature; (2) to learn about context-specific factors; and (3) to guide the survey question design. Interview respondents were selected from students enrolled in IS courses at an east coast university in the US. The selection of interviewees was based on the principle of purposeful sampling—a great deal of information can be obtained from a limited number of participants (Creswell, 2003). A total of 19 students were interviewed. The sample consists of 10 female and 9 male students from different departments and in different academic years. Although the use of a college student sample is not ideal, there is some evidence that college students are, in many ways, similar to SNS users more generally (Hargittaii, 2007). A student sample is justified given that social networking-site users fit the demographics of college students between the ages 18 and 30. Participants were asked to write down their thoughts about privacy, security, risk, and attitudes toward SNS on sticky notes and then post the notes under the four categories provided by the researchers.

Based on the initial survey, a pretest was conducted to confirm the validity and the reliability of the survey. Students enrolled at the same university participated in the pretest for extra course credit ($N = 39$). Respondents were asked about any difficulty they may have encountered in the survey (ambiguous questions or terms). They were also asked about their opinion of the survey in general. Feedback and information from the pretest were used to develop a final survey questionnaire. Finally, quantitative research experts reviewed and modified the wording of items based on the pilot test outcomes.

After the pretest, a survey agency conducted a three-week online survey to evaluate the research model (see Appendix A for survey). Respondents were asked to rate each item on a five-point Likert scale, where one meant *strongly disagree* and five meant *strongly agree*. The contracted agency gathered 370 responses (response rate was 23%). After eliminating insincere responses through data filtering, 323 valid and usable responses were selected as the sample. Of the respondents, 53.5% were female and 45.9% were male. All participants said they use SNS regularly and spend about 1 h per week online on average. Respondents were asked to indicate their primary uses of SNS. All the questionnaires used in this survey have been validated in previous studies. SPSS 10.0 is used for analysis of a descriptive statistics.

4.1. Measurements

All the measures in the present study are based upon previously validated measures and are considered reliable. The measures of behavioral intention to use and attitude were adapted from previous studies related to the Technology Acceptance Model (TAM) model, mainly from Davis (1989) and modified to fit the specific technology studied. Trust was measured with items used by Fogel and Nehmad (2009). To address the elements of perceived security, this study used Yenisey et al. (2005) measures. Perceived privacy was measured with items from Buchanan et al. (2007) and Metzger (2004).

All of the constructs in this study were examined in terms of reliability, convergent validity, and discriminant validity. Reliability was evaluated using the composite reliability values. Hair et al. (1998) recommended an acceptance level of 0.7 for the composite reliability. As summarized in Table 1, all of the constructs in the model are greater than 0.88 and meet this criterion. For convergent validity, two criteria should be met as suggested by Fornell and Larcker (1981): (1) all of the factor loadings should not only be significant but also should exceed 0.7 and (2) average variance extracted (AVE) by each construct should exceed the variance due to measurement error for that construct, i.e., AVE should be greater than 0.5. As listed in Table 2, most items exhibited loadings greater than 0.7 on their respective constructs. All AVEs were larger than the variance due to measurement error. Thus, the two criteria for convergent validity were met (Bagozzi and Phillips, 1991). Discriminant validity evaluates the extent to which a concept and its indicator variables differ from another concept and its indicator variables. Discriminant validity was examined using criteria suggested by Fornell and Larcker (1981): the square root of the AVE should be greater than the correlation shared between the construct and other constructs. Table 2 presents the correlations among constructs, with the square root of the AVE on the diagonal. The shared variance (correlation) between each pair of constructs was less than the average variances extracted (diagonal values), providing evidence of discriminant validity.

5. Results

5.1. Model fit

The measurement model fit was assessed by a confirmatory factor analysis (CFA). Eight common model-fit measures were used to estimate the measurement model fit: (1) chi-square/degree of freedom (χ^2/df), (2) the goodness-of-fit index (GFI), (3) root mean square error of approximation (RMSEA), (4) root mean square residual (RMR), (5) normed fit index (NFI), (6) non-normed fit index (NNFI), and (7) comparative fit index (CFI). As Table 3 shows, all the model-fit indices satisfy their respective acceptance criteria suggested in the prior literature (Hair et al., 1998). Therefore, we can conclude that the measurement model has good fit with the data collected. Table 3 also shows the common model-fit indices, recommended values, and results of the test of structural model fitness. A comparison of all fit indices with their corresponding recommended values (Hair et al., 1998) indicates a good model fit.

Table 2
Principal component analysis with varimax rotation.

Component	1	2	3	4	5	6	7
PP1	**0.773**	0.134	0.189	0.299	0.123	0.152	0.239
PP2	**0.747**	0.292	0.232	0.045	0.211	0.134	0.135
PP3	**0.700**	0.219	0.264	0.370	0.233	0.023	0.272
PS1	0.163	0.287	0.243	**0.810**	0.150	0.151	0.363
PS2	0.262	0.194	0.301	**0.751**	0.180	0.121	0.116
PS3	0.227	0.224	0.273	**0.762**	0.190	0.338	0.258
T1	0.199	0.329	0.119	0.229	0.253	**0.815**	0.225
T2	0.099	0.263	0.109	0.444	0.629	**0.863**	0.256
T3	0.279	0.192	0.171	0.383	0.240	**0.737**	0.327
A1	0.292	0.231	0.240	0.114	**0.796**	0.198	0.084
A2	0.199	0.192	0.291	0.196	**0.790**	0.166	0.215
A3	0.093	0.201	0.181	0.047	**0.729**	0.250	0.187
IT1	0.134	0.189	0.299	0.123	0.152	0.239	**0.772**
IT2	0.292	0.232	0.045	0.211	0.134	0.135	**0.742**
IT3	0.219	0.264	0.370	0.233	0.023	0.272	**0.701**
α-Value	0.8883	0.8961	0.8477	0.8511	0.9101	0.8877	0.8672
AVE	0.74	0.69	0.73	0.77	0.72	0.71	0.78

Note: Numbers in bold shows loading coefficients for items in each construct.

5.2. Structural paths and hypotheses tests

To test structural relationships, the hypothesized causal paths were estimated, and all seven hypotheses were supported. Table 4 shows these results, which generally support the proposed model and illustrate key roles of trust in the model. The results highlight the important roles of perceived security and privacy in determining users' intentions to use SNS. Perceived security showed the greatest effect on attitude ($\beta = 0.59$, $t = 4.021$), followed by perceived privacy ($\beta = 0.47$, $t = 2.459$). The model also shows a significant effect of trust on attitude, supporting H7. H6 (the effect of privacy on security) is supported, which implies privacy as a mediating effect on the relation between security and trust.

Fig. 2 also illustrates the explanatory powers of constructs. The model finds that perceived privacy accounts for 19% of the variance in perceived security. Perceived privacy and perceived security, taken together, explain 66% of the variance in trust. Trust, together with security and privacy, explained 51% of the variance in attitude toward behavior, which in turn explained 23% of the variance of intention. The 23% R^2, a relatively low indicator, implies other possible underlying paths in the model.

Table 1
Cronbach's Alpha reliability and correlations and AVE.

Construct	Cronbach's Alpha	AVE and squared correlations					
		AVE	PP	PS	TR	AT	INT
Perceived privacy (4 items)	0.8872	0.69	**0.81**				
Perceived security (3 items)	0.9311	0.72	0.73	**0.81**			
Trust (3 items)	0.8873	0.71	0.59	0.76	**0.89**		
Attitude (3 items)	0.8289	0.61	0.64	0.69	0.53	**0.80**	
Intention (3 items)	0.9102	0.81	0.47	0.45	0.37	0.52	**0.90**

* Diagonal elements (in bold) are the square root of the average variance extracted (AVE). Off-diagonal elements are the correlations among constructs. For discriminant validity, diagonal elements should be larger than off-diagonal elements (Joreskog and Sorbom, 1996).

* Cumulative% of variance: 73.1%.

Table 3
Fit indices for the measurement model and structural model.

Fit statistics	Measurement model	Overall model	Recommended value
χ^2/df	2.742	2.733	<5
GFI	0.906	0.905	>0.90 (Bagozzi and Yi, 1988)
AGFI	0.831	0.824	>0.80 (Etezadi-Amoli and Farhoomand, 1996)
RMSEA	0.073	0.071	<0.06 (Joreskog and Sorbom, 1996)
RMR	0.054	0.055	<0.08 (Bentler, 1990)
CFI	0.942	0.963	>0.90 (Joreskog and Sorbom, 1996)
NFI	0.930	0.947	>0.90 (Fornell and Larcker, 1981)
NNFI	0.942	0.952	>0.90 (Bagozzi and Yi, 1988)

Table 4
Summary of hypothesis tests.

Hypothesis	Path coefficient	*t*-Value	Support
H1: Attitude → Intention	0.41**	5.120	Yes
H2: Security → Attitude	0.59**	4.021	Yes
H3: Security → Trust	0.53**	6.717	Yes
H4: Privacy → Trust	0.26*	2.001	Yes
H5: Privacy → Attitude	0.47*	2.459	Yes
H6: Trust → Attitude	0.21*	0.314	Yes
H7: Privacy → Security	0.50**	4.423	Yes

* $p < 0.05$.
** $p < 0.001$.

5.3. Comparison of the attitude towards the individual SNS

As the research model show significant results, this study is interested in pursuing further question whether the attitudes towards the individual SNS regarding levels of privacy/security and use are different. For this, it broke down the data according to individual SNS.

Among the 323 responses, two groups of users (Facebook and MySpace) were compared as they were comprised of most respondents (Facebook: 119, 36.8% and MySpace: 111, 34.3%). As the two SNSs represent dominant services in the market, it is worthwhile to compare the data of the two sites. With *t*-test, means and standard deviations were used to examine SNS differences in each variable (Table 5). While there was no significant SNS differences in attitude and intention, users did differ on privacy with the MySpace users being considerably less concerned with privacy and Facebook users indicating fairly high privacy levels (privacy $t[235] = -12.01$, $p < 0.01$). In addition, the result of the *t*-test was significant for security with Facebook users being more secured than the MySpace users ($t[193] = -9.17$, $p < 0.01$). Along with security and privacy, trust was shown a little difference between the two groups of users ($p < 0.05$). However, the *t*-test result was not significant for the dependent variables (attitude and intention), suggesting that there were no significant differences between Facebook and MySpace users in the extent of usage time and satisfaction. This is an intriguing finding that privacy and security are somewhat different between Facebook and MySpace. The reason for this may be that originally Facebook was a private community for college students, thus, it was set up with a great deal more privacy. Alternatively, MySpace has been targeted to a larger target group and therefore was more open to many visitors. The *t*-test result is consonant with a common notion that Facebook is a much more secure community. However, Myspace also has security features that can be set to protect user privacy.

6. Discussion

The goal of this study was to develop a groundwork model of trust-based SNS acceptance to explain the factors contributing to the development of individual attitude and behavioral intentions to use SNS. For this purpose, this study developed a theoretical framework describing the trust-based decision-making process and tested the proposed model using a structural-equation modeling technique on SNS-user behavior data collected via a web survey. Consistent with prior literature that investigated the effect

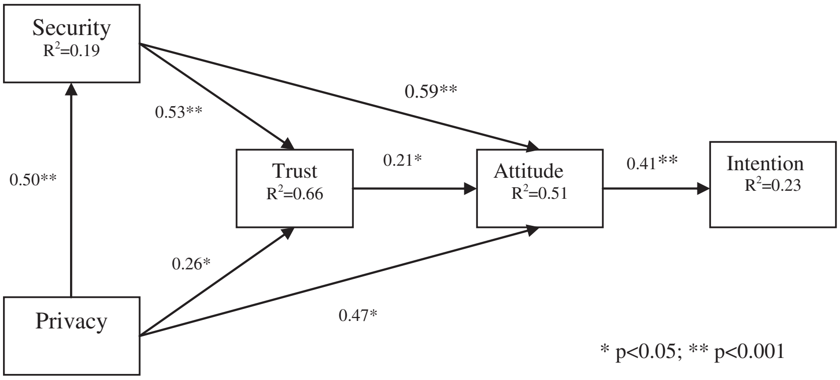

Fig. 2. Research result.

Table 5
Difference test results.

Variables	*t*	df	Sig (2-tailed)	Mean difference	Std. error difference	95% CI lower	95% CI upper
Security	−9.17	228	0.000**	−0.401	0.033	−0.500	−0.349
Privacy	−12.01	228	0.000**	−0.417	0.040	−0.524	−0.311
Trust	13.042	228	0.004*	−0.131	0.042	−0.209	−0.044
Attitude	3.301	228	0.421	0.395	0.036	−0.115	−0.156
Usage	0.962	228	0.339	−0.041	0.042	−0.124	0.038
Intention	1.322	228	0.282	0.103	0.043	0.028	0.182

* $p < 0.05$.
** $p < 0.01$.

of security and trust (e.g., Dwyer et al., 2007; Gambi, 2009; Maheswaran et al., 2007; Roca et al., 2009), evidence from this research provides empirical support for the proposed model. The results offer help in understanding users' attitudes and the intention of SNS in terms of privacy dimension and clarify implications for the development of effective SNS services and applications. The results of the measurement and structural-model test lend support to the proposed research model. The structural model provided a good fit to the data, and most path coefficients in the model were found statistically significant, in line with previous findings in IS and TAM literature (e.g., Gefen and Straub, 2004; Liu et al., 2005; Nijite and Parsa, 2005; Papadopoulou, 2007; Pavlou and Gefen, 2004;). Overall, the results show that the model demonstrates good predictive powers and explain behavioral intentions in SNS.

The research develops the constructs of perceived privacy and perceived security as the chief determinants of trust in SNS acceptance. Two significant predicators reflect current SNS trends: (1) users have concerns about the vulnerability of SNS security and privacy breaches when they use SNS and (2) perceived security and perceived privacy directly affect trust in SNS use. Of the two factors affecting attitude, perceived security, shows a much stronger effect on attitude than perceived privacy, implying a unique relationship between the two. This finding is slightly different from previous studies (Barnes, 2007; Dwyer et al., 2007; Flavian and Guinaliu, 2006), which have argued privacy over security.

From the high level of its effect on attitude, it can be inferred that trust apparently plays a role in enhancing intention. The findings support previous research on trust, as users reported that being confident was important and stressed the value of being able to explore new things in online environments (Hassanein and Head, 2007). Considering the high significance of perceived security, we can say that enhanced feelings of security will result in improved perception of trust. Recent research on trust indicates that trust plays important roles in determining a person's behavioral intention and actual behavior (Gambi, 2009; Pavlou and Gefen, 2004; Wu and Liu, 2007). The findings of this study advance previous studies by clarifying the relationship among trust, security, and privacy in an SNS context. The results show that trust relates significantly to perceptions of security, supporting H3. While a moderate correlation exists between perceived privacy and trust supporting H4, a significant effect of perceived privacy on perceived security also exists, supporting H7. This effect, together with validated H3 (perceived security to trust), implies a clear mediating effect of perceived privacy on trust through perceived security. This mediating effect is consistent with Palmer et al. (2000) finding on the mediating role of trust on the web.

Interestingly, the level of effect of privacy on trust is not as significant as previous studies have showed (H4). The moderately supported hypothesis contradicts previous studies that found highly significant effects of privacy on trust (e.g., Dwyer et al., 2007; Gauzente, 2004; Teltzrow et al., 2007). In the SNS context, users' perceived privacy does not mechanically convey trust. This can be explained as SNS users may think protecting privacy alone is not enough to trust SNS, instead, they may expect the services secure enough to trust SNS. With increasing ID fraud on SNS, people may consider simple privacy protection insufficient to completely trust SNS sites; they may want some security measures to mediate their concerned privacy and to enhance their feeling of trust. This inference nicely suits the mediating effect found in H4 and H7.

6.1. A modified model

Given the high effect from privacy to security, it can be reasonably inferred the reverse effect from security to privacy (Fig. 3). In fact, the two are conceptually inextricably related ones. In the case of SNS, the two may be even more complicated. In this light, a mutual relation should have been established in the initial model. A modified model is proposed by expanding the mutual influence of privacy and security. For the modified model, a new data set was collected and analyzed. The results show rather different magnitudes of effects from the initial model, while maintain fundamental relationships among the variables.

Most notably, the effect of privacy to security was increased by 0.19, resulting in the improved coefficient of 0.69. Conversely, the effect of security to privacy was found to be highly significant ($\beta = 0.48$), establishing a reciprocal relation of security and privacy. The effect size from privacy to security is much larger than the converse effect, which implies that privacy is a subset of security. Indeed, a new test shows that security and privacy indeed similar concepts like two sides of the same coin.

A modified model also revealed another two reciprocal relations: security and trust; and privacy and trust. By establishing the reciprocal effects, the initial effects were significantly improved: from security to trust ($\beta = 0.53 \rightarrow \beta = 0.62$) and from privacy to trust ($\beta = 0.26 \rightarrow \beta = 0.49$). Especially, the effect change from privacy to trust is notable implying that the initial one-way influence was lacking. The inclusion of the two missing relations (effect from trust to security and effect from trust to privacy) normalized the relationship among security, trust and privacy. Recently, there has been a research attempt to establish the relation of security-related variables (security, privacy, risk and trust) by clarifying subtle differences of these similar factors. In this light of trend, the modified model contributes to the literature by establishing the relations of security-related factors.

In the modified model, R^2 was improved from 0.19 to 0.28 (security), from 0.66 to 0.69 (trust), and from 0.51 to 0.59 (attitude). In addition, the rest of path coefficients of each path were increased either slightly or greatly.

Given the highly supportive relations among security, privacy and trust, a correlation test might be necessary to confirm the rela-

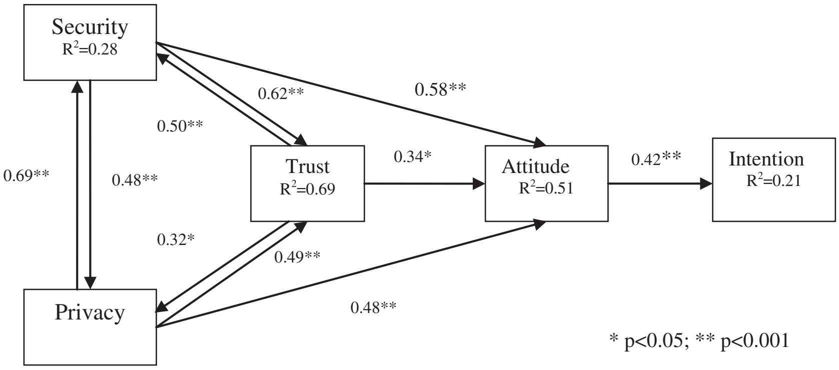

Fig. 3. A modified model incorporating reciprocal relations.

Table 6
Correlation matrix among security, privacy, and trust.

	SE1	SE2	SE3	PR1	PR2	PR3	TR1	TR2	TR3
SE1	1								
SE2	.48*	1							
SE3	.61**	.74**	1						
PR1	.46*	.50*	.52*	1					
PR2	.51*	.34	.46*	.60**	1				
PR3	.49*	.53*	.41	.79**	.68**	1			
TR1	.42	.34	.32	.43	.49*	.53*	1		
TR2	.41	.43	.54*	.38	.26	.33	.43*	1	
TR3	.59*	.42	.30	.49	.33	.44	.50*	.62**	1

* $p < 0.05$.
** $p < 0.001$.

tions. A correlation test can help to identify possible multicollinearity problems. The greatly increased coefficient estimates might be due to multicollinearity as the three variables are conceptually very similar and possibly redundant. The simplest method for detecting multicollinearity is the correlation matrix, which can be used to detect if there are large correlations between pairs of explanatory variables. A correlation test shows that the three are significantly correlated, but there is no significant multicollinearity among them (Table 6).

7. Implications

The results highlight several implications for IS researchers as well as SNS service providers. From a theoretical perspective, the study adds to the understanding of the multi-dimensional constructs of trust, security, and privacy. Dwyer (2007) calls for empirical research to understand the link between the role of trust and its antecedents in SNS. In investigating overall trust in SNS use, the study proposes perceived privacy and perceived security as antecedents of trust, subsequently greatly affecting attitude and intention. The finding further implies that the trust affected by perceived privacy and perceived security might play a role in the nature and type of information that a user willingly shares with SNS communities. Although a number of studies have found the role of privacy and security in the development of trust in e-commerce context (e.g., Cheung et al., 2005; Connolly and Bannister, 2007; Kim, 2008), few studies have explored the topic in the SNS context, leaving this illusive question unanswered: To what extent are users concerned about privacy and security? While future studies should further develop this point, the theoretical strengths of this study lie in the investigation of SNS services with a new model. This research extends previous work on SNS by providing empirical evidence, and the findings shed light on the positive potential of the new TAM theory in new emerging web-based knowledge services. This underscores that new services should be rooted in user-centered approach to understand user interfaces and user experiences more closely. SNS gives TAM researchers some interesting possibilities for verification of their previous results. This research can be useful to the TAM field, as it provides a picture of how users attempt to put their media use in the best light. The TAM has not been extensively applied outside the workplace; this study illustrates the robustness of the model and highlights the role security and privacy play in technology acceptance, adding to security motivation literature on the SNS.

These findings could then be used in the TAM research where the results are not so readily verifiable; the findings could provide useful insight into how users responded to the initial survey. This could lead to a more comprehensive view of how people use SNS, and, more importantly, how they perceive the services over SNS. In this regard, future studies should investigate additional motivations served by SNS; how do individuals make sense of content from new web technologies compared to the cognitions, emotions, and predispositions people derive from counterpart legacy technologies? Researchers must also be willing to explore the direction of causality by examining changes over time with a longitudinal design, because SNS services continuously evolve. Finally, future studies investigating comparative data with other types of service usage can provide additional insights on the social and cultural impact of new SNS in Web3.0.

This study sheds light on developing a new theory by grounding new variables in a TAM, by developing a new model, and by applying it in emerging SNS contexts. Web2.0 researchers are increasingly interested in modeling context-specific, as opposed to generic, behaviors with certain technological artifacts. Such context dependence has been alluded to in the domain of user behavior, as well as in researchers' acknowledgement that evaluative criteria differ in technology product, users, and situation. The new variables of perceived security and perceived privacy are found valid and significant in this study. This result ensures a consistent model of the drivers of social technology and stable theory development. Hence, the model makes an important contribution to emerging literature on social-technology adoption.

Industry can draw practical implications of these findings in terms of strategies and new models for SNS businesses. As this study confirmed the vital role of security and privacy in developing trust, industry players may put more efforts to understand users' perception on security-related factors and how the factors are formed and influence users' attitude. The attitude towards the individual SNS can be differently influenced by the different levels of privacy/security. Industry can develop a delicate security–trust mechanism that operates different security policy in SNS depending on different individuals who have the differing level of acceptable (tolerable) privacy breach.

Most significantly, SNS providers need to establish a trust relationship with consumers by developing and promoting comprehensive standards and ensuring that participants of privacy-seal programs adhere to those standards. The finding that security affects behavioral intention through attitude indicates that vendors should establish user trust in SNS security by ensuring that their services are conducted in accordance with users' expectations; namely, that they provide reliable services and that they keep their promises and commitments. SNS providers should inform potential users that risk taking and privacy concerns are potentially relevant and important concerns before individuals sign up and create social networking Websites. SNS sites need explicit policies and data protection mechanisms to deliver the same level of social privacy found offline. Along the lines with this study's suggestions, Facebook began an attempt to recapture lost trust from its users by turning to democratic governance—letting its members vote on user terms and even its advertising terms and conditions. It also introduces a new service of automated systems that spot and take down thousands of fake or malicious accounts every week (Barker, 2009). Other SNS providers have put in place a range of privacy and security-enhancing tools. The trust relationship between sites and users is key to the success of tomorrow's networks.

In conclusion, considering the ever-changing nature of the web environment, this study offers help in understanding security behaviors associated with social networking and in understanding the implications for developing effective models. As users accept SNS as a new way to entertain and inform themselves, escape from reality, and communicate with others, and as firms provide enabling platforms for users, SNS might evolve into a brilliantly effective application. However, to continue their popularity, SNS have several challenges to overcome, and user acceptance is probably the most important one. SNS developers need a better understanding of individual perceptions concerning the level of trust and the influence of security on intention to use. This study suggests that the findings provide a good basis for the industry to develop a service evaluation framework to determine the adoption potential of new services under Web3.0. The proposed framework offers an effective tool to understand market potential through an analysis of users' needs and prototyping market profiles. The model is well suited for developing such a framework for services adopted for functional reasons and services directed specifically at innovative user attitudes.

8. Limitations

This study contributes to the literature by formulating and validating the proposed model to investigate the role of security perception in SNS adoption and provides useful information for both academia and industry. Nonetheless, a number of common limitations persist, and empirical studies, including methodological, sampling, and interpretive limitations and some of the findings require further discussion. Firstly, the responding users might not represent the whole population because predominant users of SNS remain young people. The subjects of the study were recruited as representatives of young users. Thus, this study does not provide a comprehensive picture of entire SNS communities; rather, it just provides a snapshot of a subset of customers. Methodologically, it would have been better to examine user motivations from different groups of users with a longitudinal investigation.

Secondly, the research model is not a comprehensive model as it missed important paths. One missing effect is that the path from security to privacy. A user's perceived security of an SNS clearly influences their perceived privacy. In other words, one's feeling that an SNS will maintain privacy is dependent on how secure the SNS actually is. This relationship can be reciprocal, but it can be driven more by the path from security to privacy and less by the opposite direction. Thus, the model is clearly missing fundamental paths, which future studies should investigate further.

Related to this point, the model is composed of too many conceptually similar constructs, with very high correlations, suggesting that the findings in this study may be a result of inaccurate measures. While the contribution of this study may lie in attempting to focus on security/privacy/trust matter of SNS, most results are not breakthrough findings that privacy and security significantly influence trust and attitude can be understood at a common sense level. Future studies should come up with a more sophisticated instruments based on a more thorough conceptual difference.

Thirdly, the current study did not consider external factors (different Internet infrastructure, service provisions, and content quality). Wide differences in services across different SNS may exist, and user expectation and experiences may differ accordingly. Related to this point, the current study did not include individual differences that potentially influence SNS adoption as factors in SNS acceptance (e.g., demographics, user experience, and personal characteristics). Given a significant increase variance of usage in IS research, future studies can take into account demographic variables as covariates.

Possibly, perceptions of security and privacy can be subject to gender biases, global and cultural biases, and user expertise. These dimensions may provide interesting recommendations on the difference in trust-building mechanisms adopted for different genders and cultures. These limitations pose a challenge for the analysis, particularly different attitudes and intention patterns. Given a significant increase in variance of usage in many studies, it may be essential to include individual variables. A closer inspection of individual differences and their direct and indirect effects on SNS usage offers rich opportunities for future research. Future studies can investigate the differences further incorporating such external factors.

Lastly, as an exploratory attempt, this study set out with a simplified, parsimonious model. It did not research complicated relations among factors, such as those between perceived security and intention, perceived privacy and intention, and trust and intention. In particular, prior studies have indicated a direct effect of trust on intention. It is worthwhile to research this effect, because the intention variance explained by attitude is only 23% (R^2) in the model. Thus, it is reasonable to infer other possible effects on intention. These possibly significant links can serve as a starting point for future studies; it might be helpful to unravel the complex multi-dimensional functions of human security in the SNS environment.

Despite several limitations, this study offers a stepping stone on the path to understanding social-software user behavior. Many issues remain unresolved and many questions remain unanswered as SNS of Web2.0 evolve to Web3.0. SNS on Web2.0 lean toward the social side of the online world, and we expect SNS on Web3.0 to involve developed applications leaning more toward focused groups with specialized features. This study took an exploratory step at examining user experiences on still-emerging social software and found a number of metrics reliable and nomologically valid.

Acknowledgements

This research was supported by World Class University (WCU) program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (Grant No. R31-2008-000-10062-0). This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (NRF-2010-B00171). The paper was supported by Faculty Research Fund, Sungkyunkwan University, 2009.

Appendix A. Survey instrument

Constructs	Measure items	Sources
Perceived privacy	PP1: I am confident that I know all the parties who collect the information I provide during the use of SNS PP2: I am aware of the exact nature of information that will be collected during the use of SNS PP3: I am not concerned that the information I submitted on the SNS could be misused PP4: I believe there is an effective mechanism to address any violation of the information I provide to SNS	Buchanan et al. (2007) and Metzger (2004)
Perceived security	PS1: I believe the information I provide with SNS will not be manipulated by inappropriate parties PS2: I am confident that the private information I provide with SNS will be secured. PS3: I believe	Yenisey et al. (2005)

Appendix A (*continued*)

Constructs	Measure items	Sources
	inappropriate parties may deliberately view the information I provide with this SNS	
Trust	TR1: SNS is a trustworthy social network TR2: I can count on SNS to protect my privacy TR3: SNS can be relied onto keep its promises	Fogel and Nehmad (2009)
Attitude	A1: I would have positive feelings towards SNS in general A2: The thought of using SNS is appealing to me A3: It would be a good idea to use SNS	Davis (1989)
Intention to use	I1: I intend to use SNS in the future I2: I intend to visit SNS sites as much as possible I3: I intend to continue using SNS in the future	Davis (1989)

References

Acquisti, A., Gross, R., 2006. Imagined communities: awareness, information sharing, and privacy on the Facebook. In: Golle, P., Danezis, G. (Eds.), Proceedings of 6th Workshop on Privacy Enhancing Technologies. Robinson College, Cambridge, UK, pp. 36–58.

Ajzen, I., Fishbein, M., 1980. Understanding Attitudes and Predicting Social Behavior. Prentice Hall, Englewood Cliffs, NJ.

Bagozzi, R., Phillips, L., 1991. Assessing construct validity in organizational research. Administrative Science Quarterly 36 (3), 421–458.

Bagozzi, R.P., Yi, Y., 1988. On the evaluation of structural equation models. Journal of the Academy of Marketing Science 16, 74–94.

Barker, V., 2009. Older adolescents' motivations for social network site use. CyberPsychology and Behavior 10 (3), 478–481.

Barnes, S., 2007. A privacy paradox: social networking in the US. First Monday 11 (9). <http://www.firstmonday.org/issues/issue11_9/barnes/index.html> (retrieved 08.09.07).

Baron, N.S., 2008. Always On: Language in an Online and Mobile World. Oxford University Press, Oxford, New York.

Bentler, P.M., 1990. Comparative fit indices in structural models. Psychological Bulletin 107, 238–246.

Boyd, D., 2008a. Facebook's privacy trainwreck: exposure, invasion, and social convergence. Convergence 14 (1), 13–20.

Boyd, D., 2008b. Facebook's privacy trainwreck. Convergence 14 (1), 13–20.

Boyd, D.M., Ellison, N.B., 2007. Social network sites: definition, history, and scholarship. Journal of Computer-Mediated Communication 13 (1). article 11.

Brocke, J., Richter, D., Riemer, K., 2009. Motives for using social network sites: an analysis of SNS adoption among students. In: BLED 2009 Proceedings, Paper 40. <http://aisel.aisnet.org/bled2009/40> (accessed 14.02.09).

Buchanan, T., Paine, C., Joinson, A.N., Reips, U.-D., 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), 157–165.

Byrne, D.N., 2007. Public discourse, community concerns, and civic engagement: exploring black social networking traditions on BlackPlanet.com. Journal of Computer-Mediated Communication 13 (1). article 16.

Cheung, C., Chan, G., Limayem, M., 2005. A critical review of online purchase behavior: empirical research. Journal of E-Commerce in Organizations 3 (4), 1–19.

Chiu, P., Cheung, C., Lee, M., 2008. Online social networks: why do we use Facebook? Communications in Computer and Information Science 19, 67–74.

Connolly, R., Bannister, F., 2007. Consumer trust in Internet shopping in Ireland: towards the development of a more effective trust measurement instrument. Journal of Information Technology 22, 102–118.

Coppola, N., Hiltz, S.R., Rotter, N., 2004. Building trust in virtual teams. IEEE Transactions on Professional Communication 47 (2), 95–104.

Creswell, J.W., 2003. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, second ed. Sage Publications, Thousand Oaks, CA.

Culnan, M.J., Armstrong, P.K., 1999. Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation. Organization Science 10 (1), 104–115.

Davis, F., 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly 13 (3), 319–340.

Dewan, S., Chen, L., 2005. Mobile payment adoption in the US. Journal of Information Privacy and Security 1 (2), 4–28.

Donath, J., 2007. Signals in social supernets. Journal of Computer-Mediated Communication 13 (1), 231–251.

Dwyer, C., 2007. Digital relationships in the MySpace generation: results from a qualitative study. In: Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS), Hawaii, 2007.

Dwyer, C., Hiltz, S., Passerini, K., 2007. Trust and privacy concern within social networking sites: a comparison of Facebook and MySpace. In: Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado, August 9–12 2007.

Ellison, N., Steinfield, C., Lampe, C., 2006. The benefits of Facebook friends: social capital and college students' use of online social network sites. Journal of Computer-Mediated Communication 12 (3). article 1.

Etezadi-Amoli, J., Farhoomand, A.F., 1996. A structural model of end user computing satisfaction and user performance. Information and Management 30 (2), 65–73.

Flavian, C., Guinaliu, M., 2006. Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. Industrial Management and Data Systems 106 (5), 601–620.

Fogel, J., Nehmad, E., 2009. Internet social network communities: risk taking, trust, and privacy concerns. Computers in Human Behavior 25, 153–160.

Fornell, C., Larcker, V.F., 1981. Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research 18, 39–50.

Gambi, S., 2009. The development of trust within close relationships formed within social network sites. In: Proceedings of the WebSci'09: Society On-Line, Athens, Greece, March 18–20 2009.

Gauzente, C., 2004. Web merchants' privacy and security statements: how reassuring are they for consumers? A two-sided approach. Journal of Electronic Commerce Research 5 (3), 181–198.

Gefen, D., Straub, D.W., 2004. Consumer trust in B2C e-commerce and the importance of social presence: experiments in e-Products and e-Services. Omega 32 (6), 407–424.

Hair, J.F., Anderson, R.E., Tatham, R.L., Black, W.C., 1998. Multivariate Data Analysis, fifth ed. Prentice Hall, Englewood Cliffs, NJ.

Hargittaii, E., 2007. Whose space? Differences among users and non-users of social network sites. Journal of Computer-Mediated Communication 13 (1). article 14.

Hassanein, K., Head, M., 2007. Manipulating social presence through the web interface and its impact on consumer attitude towards online shopping. International Journal of Human–Computer Studies 64 (12), 1230–1242.

Hoffman, D.L., Novak, T.P., Peralta, M., 1999. Building consumer trust online. Communications of the ACM 42 (4), 80–85.

Jagatic, T., Johnson, N., Jakobsson, M., Menczer, F., 2007. Social phishing. Communications of the ACM 50 (10), 94–100.

Jarvenpaa, S., Leidner, D., 1998. Communication and trust in global virtual teams. Journal of Computer-Mediated Communication 3 (4).

Jarvenpaa, S.L., Tractinsky, N., Vitale, M., 2000. Consumer trust in an Internet store. Information Technology and Management 1, 45–71.

Joinson, A.N., 2008. Looking at, looking up or keeping up with people? Motives and use of Facebook. In: Proc. CHI 2008. ACM Press, pp. 1027–1036.

Joreskog, K.G., Sorbom, D., 1996. LISREL 8: Users reference guide. Scientific Software International, Chicago.

Kim, W., 2008. Applying the technology acceptance model and flow theory to Cyworld user behavior. CyberPsychology and Behavior 11 (3), 378–382.

Kim, K.-H., Yun, H., 2007. Cying for me, Cying for us: relational dialectics in a Korean social network site. Journal of Computer-Mediated Communication 13 (1). article 15.

Kim, D., Steinfiled, C., Lai, Y., 2008. Revisiting the role of web assurance seals in business-to-consumer electronic commerce. Decision Support Systems 44 (4), 1000–1015.

Linck, K., Pousttchi, K., Wiedemann, D.G., 2006. Security issues in mobile payment from the customer viewpoint. In: Proceedings of the 14th European Conference on Information Systems (ECIS 2006), Gothenburg, Sweden.

Liu, C., Marchewka, J., Lu, J., Yu, C., 2005. Beyond concern: a privacy–trust–behavioral intention model of electronic commerce. Information and Management 41 (2), 289–304.

Maheswaran, M., Tang, H.C., Ghunaim, A., 2007. Towards a gravity-based trust model for social networking systems. In: 27th International Conference on Distributed Computing Systems Workshops, June, 2007, pp. 24–34.

McKnight, D.H., Choudhury, V., Kacma, C., 2002. Developing and validating trust measures for e-commerce: an integrative typology. Information Systems Research 13 (3), 334–359.

Metzger, M., 2004. Privacy, trust, and disclosure: exploring barriers to electronic commerce. Journal of Computer-Mediated Communication 9 (4). <http://jcmc.indiana.edu/vol9/issue4/metzger.html>.

Miyazaki, A.D., Fernandez, A., 2001. Consumer perceptions of privacy and security risks for online shopping. The Journal of Consumer Affairs 35 (1), 27–44.

Nijite, D., Parsa, H.G., 2005. Structural equation modeling of factors that influence consumer internet purchase intentions of services. Journal of Services Research 5 (1), 43–59.

Palmer, J.W., Bailey, J.P., Faraj, S., 2000. The role of intermediaries in the development of trust on the WWW. Journal of Computer-Mediated Communication 5 (3). <http://jcmc.indiana.edu/vol5/issue3/palmer.html>.

Papadopoulou, P., 2007. Applying virtual reality for trust-building e-commerce environments. Virtual Reality 11 (2), 107–127.

Pavlou, P.A., Gefen, D., 2004. Building effective online marketplaces with institution-based trust. Information Systems Research 15 (1), 37–59.

Piccoli, G., Ives, B., 2003. Trust and the unintended effects of behavior control in virtual teams. MIS Quarterly 27 (3), 365–395.

Pousttchi, K., 2003. Conditions for acceptance and usage of mobile payment procedures. In: Proceedings of the International Conference on Mobile Business, Vienna, Austria, pp. 201–210.

Roca, J.C., García, J.J., de la Vega, J.J., 2009. The importance of perceived trust, security and privacy in online trading systems. Information Management and Computer Security 17 (2), 96–113.

Rosen, P., Sherman, P., 2006. Hedonic information systems: acceptance of social networking websites. In: Americas Conference on Information Systems, AMCIS 2006 Proceedings, pp. 1218–1223.

Teltzrow, M., Meyer, B., Lenz, H., 2007. Multi-channel consumer perceptions. Journal of Electronic Commerce Research 8 (1), 18–31.

Wu, J., Liu, D., 2007. The effects of trust and enjoyment on intention to play online games. Journal of Electronic Commerce Research 8 (2), 128–140.

Yenisey, M.M., Ozok, A.A., Salvendy, G., 2005. Perceived security determinants in e-commerce among Turkish University students. Behaviour and Information Technology 24 (4), 259–274.