Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2009 Proceedings

International Conference on Information Systems (ICIS)

2009

Influence of Social Context and Affect on Individuals' Implementation of Information Security Safeguards

Yu "Andy" Wu
University of North Texas, andy.wu@unt.edu

Sherry Ryan
University of North Texas, sherry.ryan@unt.edu

John Windsor
University of North Texas, john.windsor@unt.edu

INFLUENCE OF SOCIAL CONTEXT AND AFFECT ON INDIVIDUALS' IMPLEMENTATION OF INFORMATION SECURITY SAFEGUARDS

Research-in-Progress

Yu "Andy" Wu
University of North Texas
Dept. of ITDS
College of Business
Denton, TX 76203
Andy.wu@unt.edu

Sherry Ryan
University of North Texas
Dept. of ITDS
College of Business
Denton, TX 76203
Sherry.Ryan@unt.edu

John Windsor
University of North Texas
Dept. of ITDS
College of Business
Denton, TX 76203
John.Windsor@unt.edu

Abstract

Individuals' use of safeguards against information security risks is commonly conceptualized as the result of a risk-benefit analysis. This economic perspective assumes a "rational actor" whereas risk is subjectively perceived by people who may be influenced by a number of social, psychological, cultural, and other "soft" factors. Their decisions thus may deviate from what economic risk assessment analysis would dictate. In this respect, a phenomenon interesting to study is that on social network sites (SNSes) people tend to, despite a number of potential security risks, provide an amount of personal information that they would otherwise frown upon. In this study we explore how people's affect toward online social networking may impact their use of privacy safeguards. Since building social capital is a main purpose of online social networking, we use social capital theory to examine some potential contextual influence on the formation of the affect. More specifically, we adopt the perspective proposed by Nahapiet and Ghoshal (1998), *which views social capital as a composite of structural, relational, and cognitive capitals. Preliminary analysis of 271 survey responses shows that (a) a person's structural and relational embeddedness in her online social networks, as well as her cognitive ability in maintaining those networks, are positively related to her affect toward SNSes; (b) a person's affect toward SNSes moderates the relationship between her perception of privacy risk and the privacy safeguards she implements on the SNSes.*

Keywords: Information security, security safeguards, privacy, social network sites, social capital, affect, risk assessment

Introduction

Use of online technologies exposes users to a host of security threats (Lu, Hsu, and Hsu, 2005). Sensing these threats, a user may choose not to participate in online activities (Cho, 2004; Lu et al, 2005), adopt threat avoidance mechanisms (Liang and Xue, 2009), or deal with the aftermath (Liang and Xue, 2009; Son and Kim, 2008). To date, most of the literature on information security risk-related behaviors aims at organizational settings. The few studies on individual risk mitigation actions (e.g., Chellappa and Sin, 2005; Dinev, Bellotto, Hart, Russo, Serra, and Colautti, 2006; Dinev and Hart, 2006; Liang and Xue, 2009) appear to be an extension of the organizational assessment process to the individual level. As a result, individual safeguarding action is theorized as the result of an assessment process believed to be a rational cost-benefit analysis. We argue that the underlying "rational person" assumption is too simplistic for analyzing people's risk assessment and mitigation.

Cost-benefit analysis is a cognitive strategy that individuals adopt, consciously or subconsciously, when evaluating information security risks. Nevertheless, the individual risk assessment process cannot be fully understood without exploring the roles played by people's affective feelings toward technology and the context of technology use. Following the studies conducted by Slovic and colleagues (Alhakami and Slovic, 1994; Finucane, Alhakami, Slovic, and Johnson, 2000; Slovic, 2000; Slovic, Fischhoff, and Lichtenstein, 1977) on how affect influences risk-related judgments and decisions, we propose that a person's affect toward a particular online technology can impact her adoption of security safeguards. Furthermore, such affect is not formed based on the technology *per se*. Rather, it is a function of the context in which the user uses the online technology.

To test these relationships, we select social network sites (SNSes) as the focal online technology to study. This is because of two reasons. First, having emerged only during the past few years but enjoying phenomenal growth, SNSes attract numerous security attacks due to the nature and amount of personal information users provide on these sites. Second, SNSes are closely related to a person's emotions and feelings (Ellison, Steinfield, and Lampe, 2007; Helliwell and Putnam, 2004). Thus, it can be expected that people form strong affective feelings toward the SNSes, which in turn influence the user's use of privacy safeguards. Also, since the main reason people use SNSes is to maintain, develop, and enhance their social capital (Martinez Aleman and Wartman, 2009), we apply findings from social capital research to study the influence of contextual factors on affect. We integrate these into a nomological network (Figure 1) about the affect dimension of SNS users' use of privacy safeguards to fend off perceived risks.

Social Network Sites and Related Risks

It is evident that SNSes have achieved cultural relevance worldwide (Martinez Aleman and Wartman, 2009). The past few years have seen dazzling growth in SNSes. For example, Facebook enjoys 50 billion page views per month. Through November of 2008, some social networking sites have experienced usage growth rates of 100% or more per year as measured by unique visitors (Schonfeld, 2007, 2008). However, while people flock to the various SNSes, it remains to be seen how many of them are taking heed of the plethora of security threats around online social networking. Most alarmingly, the wealth of personal information people supply on their SNS profiles is a hotbed for privacy-related attacks. For instance, SNS profiles can be hacked and "owned" by using a combination of coordinated exploits. By collecting and mining a person's data, an attacker is able to create a digital dossier that can be used against that person. The aggregated data also may be used to serve the ends of spammers and malware and spyware writers. Cyber and physical stalkers may use online personal data to keep track of their targets. Similarly, unscrupulous use of profile data may enhance the "credibility" of so call "social-engineers," who find their ways into corporate systems and networks by impersonating other people. Other privacy-related threats include damage to reputation due to surreptitious creation or use of profiles and images for other people; the increasingly popular practice among employers to "pre-screen" job applicants by examining their profiles; loss of control over one's own data to the SNS provider, etc. (ENISA, 2007; Jones, 2008; Maloncy, 2008; Mansfield-Devine, 2008; Martinez Aleman and Wartman, 2009; Whitaker, Evans, and Voth, 2009).

Unfortunately, due to the fast growth and a business model based on the number of users attracted, security and privacy have not been the first priority for SNS providers (ENISA, 2007). Therefore, one of the most serious risks to SNS users is loss of privacy. Whether done consciously or subconsciously, an SNS user forms a perception of the potential risk of compromised privacy. Based on Dinev and Hart (2006) and Son and Kim (2008), we define perceived privacy risk as the degree to which an individual believes that the personal information she provides online may be used improperly.

Out of concern for the perceived threats to her privacy, the user can take actions as privacy safeguards against the potential risks involved in their use of SNSes. These actions include: (a) thoroughly reading the privacy policy of the SNS; (b) managing personally identifiable information diligently; (c) changing the default privacy settings of the SNS; and (d) exercising caution before downloading and using SNS applications (ENISA, 2007; Martinez Aleman and Wartman, 2009).

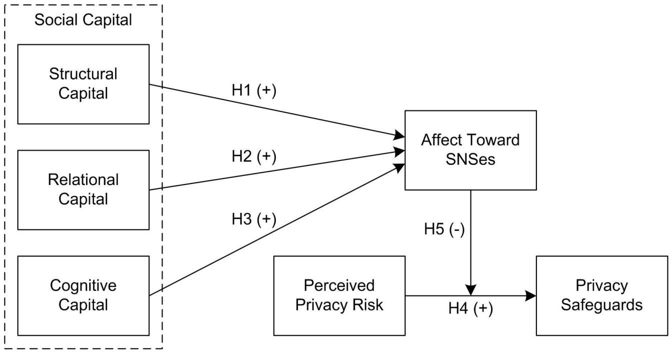

Figure 1. Research Model

Social Capital Theory

"Social capital is the goodwill available to individuals or groups. Its source lies in the structure and content of the actor's social relations. Its effects flow from the information, influence, and solidarity it makes available to the actor (Adler and Kwon, 2002, p. 23)." Generally, social capital is manifested as a positive outcome of relationships within a social network (Helliwell and Putnam, 2004). Social capital theory has gained a lot of exposure in a wide range of social science disciplines in recent years (Adler and Kwon, 2002). In information systems (IS) studies, its widest application is to explain the motivation for participation in knowledge sharing activities in which social capital is found to motivate people to share information and knowledge in the absence of direct, utilitarian rewards (e.g., Robert, Dennis, and Ahuja, 2008; Wasko and Faraj, 2005). Most business researchers examine social capital from a perspective developed by Nahapiet and Ghoshal (1998) that sees social capital as the composite of structural, relational, and cognitive components. We use this nomenclature to analyze people's use of SNSes.

Structural Capital

Also termed "structural embeddedness" (Lawson, Tyler, and Cousins, 2008), structural capital indicates the connections between individuals, i.e., the structural links created through the social interactions between individuals in a network (Wasko and Faraj, 2005). Wasko and Faraj (2005) gauge structural capital via an individual's degree of network centrality. Robert, Dennis, and Ahuja (2008) view it as a function of network intensity and decentralization. Lawson et al (2008) describe it through the density of network relationships, diversity of points of contact, and frequency of communications. Despite their different perspectives, researchers tend to agree that structural capital is manifested through some technical/tactical characteristics of a person's connection links. Thus, in the context of SNS use, we define structural capital as a person's structural embeddedness in her SNS-facilitated social network. It can be reflected by some characteristics of her communication links: (a) density – the number of links with other individuals; (b) intensity – the number of exchanges taking place over those links at a given time; (c) diversity – degree of heterogeneity of the individuals a person connects to; (d) centrality – degree to which the person dominates exchanges; (e) frequency – how often the person utilizes her connections, etc.

Relational Capital

Relational capital stands for the congenial nature of the relationships in a collective. It exists when members have a strong identification with the collective, trust others in the collective, perceive an obligation to participate, and abide by its norms (Wasko and Faraj, 2005). Relational capital is indicative of the nature and quality of the relationships among people and how those relationships affect behavior (Robert et al, 2008). Common qualities observed include mutual trust, respect, and friendship (Kale, Singh, and Perlmutter, 2000). Consistent with these studies, we define relational capital as a person's perception of belonging to an amiable SNS-facilitated social network in which other members will reciprocate the person's benevolence. It can be reflected by the person's perception of the members in her social network: (a) degree to which person identifies herself with the network; (b) degree of commitment; (c) amiability; (d) trustworthiness of members; (e) reciprocity of behaviors among members, etc.

Cognitive Capital

Proper functioning of social networks and accumulation of social capital require some degree of shared understanding of the language and context (Wasko and Faraj, 2005). Ideally, a person should be able to navigate her network and tap the resources available through the network efficiently and effectively. This is more likely to occur when shared understanding exists among the members, because it reduces the amount of translation and learning needed. Cognitive capital is the part of social capital where such shared understanding is embedded. Researchers view cognitive capital as shared goals and culture (Krause, Handfield, and Tyler, 2007), shared understanding (Robert et al, 2008), shared code or paradigm that facilitates a common understanding (Tsai and Ghoshal, 1998), etc. Wasko and Faraj (2005) take another angle and suggest that cognitive capital is cultivated by (a) expertise and (b) length of participation, both of which also enhance a person's ability to navigate the network and utilize social capital. We define cognitive capital as a person's ease in understanding her SNS-facilitated social network as a result of interacting, over time, with network members sharing common goals, culture, and language. It can be reflected by the person's perception of the degree to which she and other members share (a) goals for using the network, (b) thought processes, (c) language used on the network; (d) her expertise and length in participation, etc.

Influence of Affect on Risk-Related Behaviors

At present, there appears to be a dearth of IS studies on how a person assesses security risks and takes risk-avoding actions (Liang and Xue, 2009). The exception is some in-depth, rigorous studies focusing on privacy concerns about providing personal information on websites (Chellappa and Sin, 2005; Dinev et al, 2006; Dinev and Hart, 2006; Son and Kim, 2008). The extant literature, moreover, usually assumes that an individual rationally weighs the benefits and potential losses due to online exposure and, based on this cost-benefit analysis, determines a course of action accordingly.

Dinev and Hart (2006) study the effect of conflicting considerations on people's willingness to provide personal information to transact on the Internet. They categorize loss-related considerations as "risk beliefs" and benefit-related considerations as "confidence and enticement beliefs." Both types of beliefs are then weighed against each other through a decision process that Dinev and Hart term "privacy calculus," whose roots they trace to Culnan and Armstrong (1999). The result of the calculus is information-giving behavior that maximizes positive outcomes and minimizes negative outcomes. Chellappa and Sin (2005) study a similar online behavior – individuals' use of personalization services provided by many websites. Their model is more parsimonious but underscored by the same cost-benefit analysis approach.

Most recently, Liang and Xue (2009) broach the technology threat avoidance theory (TTAT). They suggest that a person's threat avoidance behavior is essentially the result of two appraisal processes. Threat appraisal determines the person's threat perception by evaluating her susceptibility to and severity of the threat. Coping appraisal gauges the avoidability of the threat by taking into account perceived effectiveness of protective mechanisms, perceived costs of implementing them, and the person's self-efficacy in using the mechanisms. These appraisals influence the person's coping-related motivation and behavior. Although Liang and Xue do not have a clear tone of costs *vis-á-vis* benefits comparison, their proposal is true to the cost-benefit analysis roots in its probabilistic approach to assessment.

The basic steps in a cost-benefit analysis are (a) the arrival at the expected value of loss by summing up the (cost*probability) terms across all adverse alternatives; (b) the calculation of expected benefits; and (c) the comparison of the two (Fischhoff, 1977; Fischhoff, Lichtenstein, Slovic, Derby, and Keeney, 1981). This paradigm is echoed in business research (e.g., Culnan and Bies, 2003; Stone and Stone, 1990). The fundamental assumption of cost-benefit analysis is that people will faithfully follow what economic analysis dictates. In other words, they're "rational" (Fischhoff et al, 1981; Shostack and Stewart, 2008). However, evidence abounds that the basic cost-benefit model is not an accurate description of how people make decisions in actual practice (Fischhoff, 1977). In fact, one motivation for the Dinev and Hart (2006) study is the observation that sales over the Internet continue to increase despite people's privacy concerns. In general, economic Security models often break down when the user violates assumptions such as economic rationality (Shostack and Stewart, 2008).

One reason for such violation of the rational-person assumption is people's affect. Their affective feelings toward events or objects related to a risk often influence their risk-related behaviors. We posit that affect can have two types of effects in information security setting. First, affect can skew a person's judgment of the consequences of potential risk, thus reducing her willingness to take safeguards against the risks. Finucane et al (2000) find that affect is an essential component and serves as a cue in many forms of risk-related decision making. People often use an "affect heuristic" instead of weighing the pros and cons or retrieving from memory many relevant examples. Application of affect heuristic can thwart the use of cost-benefit analysis because, interestingly, under the influence of affect, favorable outcomes often are blown out of proportion, leading the person to take riskier course of action. Second, even when the perceived risk is held constant, a person's affect can lead to different level of risk-taking/aversion. Although research on this effect is mixed (Deldin and Levin, 1986; Isen, Nygren, and Ashby, 1988; Isen and Patrick, 1983), it is certain that a person's risk-mitigation action is not a simple, linear function of the amount of risk she perceives. Therefore, the security safeguards a person implements depends not only the perceived security threats but also her affect toward the technology in use.

In the realm of information security, practitioner observations seem to confirm the judgment-clouding effect of affect. Anecdotal evidence suggests that emotions, feelings, and subjective perception often are what people rely on when they choose security technologies (Schneier, 2008). Unfortunately, there is a lack of academic research on this. Therefore, theorizing and empirical testing of the role of affect in information security risk-related behaviors is warranted.

Research Hypotheses

Only a few studies have investigated the dimensions of social capital as independent variables at the individual level (Yang, Lee, and Karnia, 2009) and none that we are aware has done so in a SNS context. Therefore, while our hypotheses are logical, they are exploratory in nature.

First we argue that if a person is strongly embedded in her SNS-facilitated social networks, it is expected that she becomes more inter-connected with other members in the network and has more resources to utilize. The individual is more likely to form a positive feeling about the SNS. Therefore,

H1: A person's structural capital is positively related to her affect toward the SNSes.[1]

The more relational capital a person accumulates via using SNSes, the more friendship she feels from a group of trustworthy and amiable people she identifies herself with. It is more likely that she entertains a positive emotion toward the SNSes. Therefore,

H2: A personal's relational capital is positively related to her affect toward SNSes.

The more cognitive capital a person has, the more likely that she and other members in her social networks share common goals, mental model, and language. Also, she is more at home with working with the SNSes to manage her social network. It is more likely for her to come to like the SNS. Therefore,

H3: A person's cognitive capital is positively related to her affect toward SNSes.

When a person perceives threats to her privacy posted by her use of SNSes, she is prone to taking actions to prevent the threats from materializing. Therefore,

H4: A person's perceived privacy risk is positively related to privacy safeguards she implements on SNSes.

As discussed above, affect can cause an individual to downplay the negative effect of risks. In the SNS context, the degree to which an individual implements privacy safeguards also is a function of her affective feeling toward the SNS. For a given level of perceived risk, higher level of affect reduces the influence of perceived risk on the

[1] Consistent with Compeau and Higgins (1999), we use the term "affect" to refer to positive feelings toward a technology.

safeguard adopted. Put differently, the relationship between perceived risk and safeguards depends on the level of affect. Therefore,

H5: A person's affect toward SNSes moderates the relationship between her perceived privacy risk and the privacy safeguards she implements on SNSes.

Methodology

Survey Development

We created a survey instrument to test our hypotheses. Wherever possible, we used scales adapted or taken from prior studies, carefully making necessary changes in wording to fit the context of SNSes. Structural capital was measured by five items that are based on Robert et al (2008) and Lawson et al (2008). Relational capital was measured by five items, based on Robert et al (2008), Wasko and Faraj (2005), and Kale et al (2000). Cognitive capital was measured by five items based on Wasko and Faraj (2005), Tsai and Ghoshal (1998), and Krause et al (2007). To measure affect toward SNSes, we adapted five items from Compeau and Higgins (1995; 1999) and Thompson, Higgins, and Howell (1991). Four items were adapted from Dinev and Hart (2006) to measure perceived privacy risk. To measure privacy safeguards, we developed five items based on ENISA (2007) and Martinez Aleman and Wartman (2009). All items were measured using five-point Likert scale.

The initial instrument was piloted by four IS researchers not involved with the project, who provided written and oral feedback. The piloting process tested the appearance of the survey, the clarity of questions and instructions, and the completeness of the survey. Based upon suggestions, additional demographic questions were added.

Survey Administration and Respondent Demographics

Undergraduate students in multiple sections of a core business course at a large public university in the U.S. were asked to complete the survey. We attempted to minimize the threat of social desirability/common method by stating at there were "no correct answers." In addition, each potential respondent was informed that all individual responses would be kept anonymous and that only aggregate data would be presented in the results.

A priori power analysis using G*Power 3 (Faul, Erdfelder, Lang, and Buchner, 2007) showed that 119 responses were needed to achieve .95 power in detecting medium size effect, which was set at .15 as suggested by Cohen (1988). We collected 310 survey responses. Out of the 310 respondents, 22 stated that they did not use SNSes at all. Another 17 respondents answered 1s, 3s, or 5s to all of the questions, a sign of invalid answers. After excluding these irrelevant or invalid responses, we had 271 usable responses, exceeding the required sample size as indicated by the *a priori* power analysis.

The mean of the respondent age is 22.3. Of them 53.20% are male and 46.80% female. Those who are employed full-time make up 20.7% of the sample; employed part-time, 51.3%; and unemployed, 26.6%. 8.6% consider themselves "expert" users of SNSes; 64.6% "intermediate" users; and 25.1% "novice" users. On average, the respondents spend 1.138 hours per day on SNSes, which are the result of3.15 log-ins to the sites per day. Put differently, the average respondent spends about 21.68 minutes each time they log in to an SNS.

Preliminary Analysis

First, we conducted a principal component analysis (PCA). After examining items with unsatisfactory loadings, for each construct, we retained three items with the highest loadings. Retained items showed satisfactory loadings in the second run of PCA.

The retained items are – **Structural Capital**: (1) I have a lot of "friends" on my SNS. (2) I have a lot of exchanges with my "friends" on my SNS. (3) I use my SNS very frequently. **Relational Capital**: (1) I have a strong sense of belonging to my SNS. (2) I feel a great deal of loyalty to my SNS. (3) I feel a great deal of friendship on my SNS. **Cognitive Capital**: (1) My "friends" on my SNS and I share the same goals for using my SNS. (2) My "friends" on my SNS and I and I think alike. (3) My "friends" on my SNS and I use the same type of expressions. **Affect toward SNSes**: (1) I like using my SNS. (2) Using my SNS is fun. (3) Interacting with my friends has become more interesting since I joined my SNS. **Perceived Privacy Risk**: (1) I am concerned about putting information and pictures on my SNS profile because of what others might do with it. (2) I am concerned about putting information and pictures on my SNS profile because it could be used in a way I did not foresee. (3) I am concerned that my private information that I put on my SNS might show up elsewhere on the Internet. **Privacy Safeguards**: (1) I diligently manage personally identifiable information related to my pictures on my SNS. (2) I looked into the default privacy settings on my SNS and adjusted them to fit my preferences. (3) I am very careful about downloading and using web applications (e.g., "widgets on Facebook") in my SNS.

We then performed partial least square (PLS) analyses on the retained items. PLS was used because it is proper for theory building and exploratory studies (Gefen, Straub, and Boudreau, 2000).

Assessment of the Measurement Model

The adequacy of the measurement model is determined by examining reliability and convergent and discriminant validities (Hulland, 1999). The reliability of all the constructs falls within the range from .8290 to .9311, greater than the generally accepted threshold of .70 (Hair, Black, Babin, Anderson, and Tatham, 2006). Convergent validity provides a measure of the variance shared between a construct and its indicators. It is gauged by examining whether items load with significant *t*-values on its construct and the significance level of .05 or higher is desired (Gefen and Straub, 2005). Significance level of .01 is observed of the loadings of all of our items. Convergent validity also is demonstrated by the square root of the average variance extracted (AVE) higher than .50. (Fornell and Larcker, 1981). In our study, the square roots of AVEs are between .7860 and .9047. There are two procedures for assessing discriminant validity. First, the squared roots of the AVEs should be higher than all of the correlations between any two constructors (i.e., the off-diagonal correlations) (Chin, 1998; Gefen and Straub, 2005). The AVE squared-roots reported above also are higher than all inter-construct correlations. Second, each within-construct item must load highly on the construct it is intended to measure and cross-loadings need to be lower than the within-construct item loadings. In our study, this is observed in the loadings tables. In summary, our measurement model appears to be valid, in terms of reliability and convergent and discriminant validity.

Assessing the Structural Model

Since we hypothesized moderation effect in our model, we used hierarchical regression to test our structural model (Cohen, Cohen, West, and Aiken, 2003; Keith, 2006). The first regression was run without the moderation effect. In the second regression, we included the moderation effect by creating an interaction term between the moderator (affect) and the predictor latent variable whose effect is moderated, i.e., perceived privacy risk. As proposed by Chin, Marcolin, and Newsted (2003), an interaction term was created by multiplying the indicators for those latent variables. This newly created latent variable was then added as a predictor of the criterion variable (privacy safeguards). The following table shows the preliminary analysis results:

Table 1. Structural Model Analysis Results

Step 1	Structural capital (SC) Relational capital (RC) Cognitive capital (CC) Affect toward SNSes (AF) Perceived privacy risk (PR) Privacy safeguards (PS)	R^2: AF .616 PS .293	SC → AF 0.427*** RC → AF 0.287*** CC → AF 0.242*** AF → PS 0.447*** PR → PS 0.215***
Step 2	SC, RC, CC, AF, PR, PS† AFxPR	R^2: AF .636 PS .308 (ΔR^2 =.015)	AFxPR → PS -0.126* AF → PS 0.421*** PR → PS 0.213***

Notes: *** p <.001, ** p <.01, * p <.05 †All coefficients are significant (p < .001) and similar in magnitude to those in Step 1. Only two are listed because they are used in the equation for moderation effect (see next page).

As indicated by the results from the first regression, the model without moderation effect explains 61.6% of the variance in affect toward SNSes and 29.3% of the variance in privacy safeguards. All three components of social capital – structural, relational, and cognitive capital – are found to be significantly and positively related to affect toward SNSes, lending support to H1, H2, and H3. H4, which suggests that a person is more likely to adopt privacy safeguards if she perceives higher risk, is supported. The second regression shows that by including the moderation effect of AF on PR → PS, the complete model explains an additional 1.5% of the variance in privacy safeguards. Using the method described in Mathieson, Peacock and Chin (2001), the effect size f^2 for PS is calculated as $(R^2_{\text{Step2}} - R^2_{\text{Step1}})/(1-R^2_{\text{Step2}}) = .015/.692 = .0217$. The pseudo $F(4, 266) = f^2*(n - k -1) = .0217(266) = 5.7722$. Therefore, the additional 1.5% additional variance explained by the complete model is significant at the .001 level.

When the moderation effect is significant, the regression equation can be algebraically rearranged so that either variable can be said to moderate the relationship between the other variable and the criterion variable. To resolve this equivocality, it is recommended that researchers pre-designate one of the two variables as the moderator on theoretical grounds (Sharma, Durand, and Gur-Arie, 1981). Following this guideline and based on our literature review, we hypothesized AF as the moderator. Also, with the presence of significant moderation effect, the moderated relationship is no longer "main effect" but "conditional effect" instead (Aiken and West, 1991; Jaccard and Turrisi, 2003), i.e., its slope is different for each feasible value of the moderator. For this reason, although the regression coefficient of AF is significant, it would be meaningless to interpret it because we have hypothesized, *a priori*, that it is the cause of the conditional effect that PR has on PS. Therefore, AF should not also have "conditional effect" on PS. The coefficient, however, is part of the equation showing the conditional effect: PS = (.213 - .126*AF)*PR + .421*AF. As can be seen from the equation, the slope of regressing PS on PR depends on the magnitude of AF. Following Aiken and West (1991) and Cohen, Cohen, West, and Aiken (2003), we plotted the regression lines at three values of AF: mean, mean + 1 SD, and mean - 1 SD (Figure 2). Clearly, when the level of AF is higher, for the same level of perceived risk, an individual is not as likely to adopt safeguards, and vice versa. Therefore, H5 is supported.

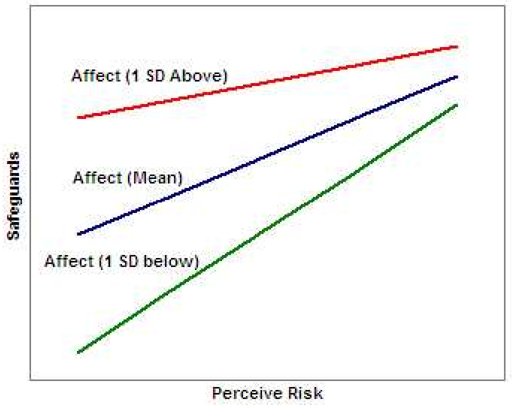

Figure 2. Moderation Effect of Affect

Potential Contribution and Conclusion

Our research findings will contribute to an under-studied area in IS research – individual risk assessment and actions related to online activities. In the setting of social network sites, our preliminary findings show that affect toward the sites could lessen people's use of security safeguards. Holding the risks involved constant, the stronger their affective feelings toward the technology, the less likely people will implement safeguards to protect themselves against the risks.

Our study also will contribute to the social capital literature. Currently, IS researchers primarily use social capital to explain knowledge sharing. We extend the application of social capital in IS by connecting it with a construct in the area of technology adoption – affect. Also, our analysis validates the applicability of the three-component view of social capital. The parsimonious measurement scales we developed and validated can be easily adapted by future IS researchers in their social capital-related research. In addition, heretofore, scant social capital research has been conducted in virtual environments; our research responds to a call from Yang, Lee, and Karnia (2009) to explore social capital in such a context.

References

Adler, P. S. and Kwon, S.-W. "Social capital: Prospects for a new concept," *Academy of Management Review* (27:1), 2002, pp. 17-40.

Aiken, L. S. and West, S. G. *Multiple Regression: Testing and Interpreting Interactions*, Sage Publications, Thousand Oaks, CA, 1991.

Alhakami, A. and Slovic, P. "A psychological study of the inverse relationship between perceived risk and perceived benefit," *Risk Analysis* (14:6), 1994, pp. 1085-1096.

Chellappa, R. and Sin, R. "Personalization versus privacy: An empirical examination of the online consumer's dilemma," *Information Technology and Management* (6), 2005, pp. 181-202.

Chin, W. W. "The partial least square approach for structural equation modeling," in *Modern Methods for Business Research* (G. A. Marcoulides (Ed.), Lawrence Erlbaum Associates, Mahwah, NJ. 1998, pp. 295-336.

Chin, W. W., Marcolin, B. L. and Newsted, P. R. "A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study," *Information Systems Research* (14:2), 2003, pp. 189-217.

Cho, J. "Likelihood to abort an online transaction: Influences from cognitive evaluations, attitudes, and behavioral variables," *Information & Management* (41), 2004, pp. 827-838.

Cohen, J. *Statistical Power Analysis for the Behavioral Sciences*, Lawrence Erlbaum Associates, Hillsdale, NJ, 1988.

Cohen, J., Cohen, P., West, S. G. and Aiken, L. S. *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences*, Lawrence Erlbaum Associates, Mahwah, NJ, 2003.

Compeau, D. R. and Higgins, C. A. "Computer self-efficacy: Development of a measure and initial test," *MIS Quarterly* (19:2), 1995, pp. 189-211.

Compeau, D. R. and Higgins, C. A. "Social cognitive theory and individual reactions to computing technology: A longitudinal study," *MIS Quarterly* (23:2), 1999, pp. 145-158.

Culnan, M. J. and Armstrong, P. "information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Organization Science* (10:1), 1999, pp. 104-115.

Culnan, M. J. and Bies, R. J. "Consumer privacy: Balancing economic and justice considerations," *Journal of Social Issues* (59:2), 2003, pp. 323-342.

Deldin, P. J. and Levin, I. P. "The effect of mood induction in a risky decision-making task," *Bulletin of the Psychonomic Society* (24:1), 1986, pp. 4-6.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. and Colautti, C. "Privacy calculus model in e-commerce - A study of Italy and the United States," *European Journal of Information Systems* (15), 2006, pp. 389-402.

Dinev, T. and Hart, P. "An extended privacy calculus model for e-commerce transactions," *Information Systems Research* (17:1), 2006, pp. 61-80.

Ellison, N. B., Steinfield, C. and Lampe, C. "The benefits of Facebook "friends:" Social capital and college students' use of online social network sites," *Journal of Computer-Mediated Communication* (12), 2007, pp. 1143-1168.

ENISA. *Security Issues and Recommendations for Online Social Networks*, European Network and Information Security Agency, Crete, Greece, 2007.

Faul, F., Erdfelder, E., Lang, A.-G. and Buchner, A. "G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences," *Behavioral Research Methods* (39:2), 2007, pp. 175-191.

Finucane, M. L., Alhakami, A., Slovic, P. and Johnson, S. M. "The affect heuristic in judgments of risks and benefits," *Journal of Behavioral Decision Making* (13), 2000, pp. 1-17.

Fischhoff, B. "Cost benefit analysis and the art of motorcycle maintenance," *Policy Sciences* (8), 1977, pp. 177-202.

Fischhoff, B., Lichtenstein, S., Slovic, P., Derby, S. L. and Keeney, R. L. *Acceptable Risk*, Cambridge University Press, Cambridge, UK, 1981.

Fornell, C. and Larcker, D. "Evaluating Structural equation models with unobservable variables and measurement error," *Journal of Marketing Research* (18), 1981, pp. 39-50.

Gefen, D. and Straub, D. "A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example," *Communications of the AIS* (16), 2005, pp. 91-109.

Gefen, D., Straub, D. and Boudreau, M.-C. "Structural equation modeling and regression: Guidelines for research practice," *Communications of the AIS* (7:7), 2000, pp. 1-78.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. and Tatham, R. L. *Multivariate Data Analysis*, (6th ed.) Prentice Hall, Upper Saddle River, NJ, 2006.

Helliwell, J. F. and Putnam, R. D. "The social context of well-being," *Philosophical Transaction of the Royal Society* (359), 2004, pp. 1435-1446.

Hulland, J. "Use of partial least squares (PLS) in strategic management research: A review of four recent studies," *Strategic Management Journal* (20:2), 1999, pp. 195-204.

Isen, A. M., Nygren, T. E. and Ashby, F. G. "Influence of positive affect on the subjective utility of gains and losses: It is just not worth the risk," *Journal of Personality and Social Psychology* (55:5), 1988, pp. 710-717.

Isen, A. M. and Patrick, R. "The effect of positive feelings on risk-taking: When the chips are down," *Organizational Behavior and Human Performance* (31), 1983, pp. 194-202.

Jaccard, J. and Turrisi, R. *Interaction Effects in Multiple Regression*, (2nd ed.) Sage Publications, Thousand Oaks, 2003.

Jones, G. "Facebook leaves users open to spam attacks," *Revolution* (September 2008), 2008, p. 6.

Kale, P., Singh, H. and Perlmutter, H. "Learning and protection of proprietary assets in strategic alliances: Building relational capital," *Strategic Management Journal* (21), 2000, pp. 217-237.

Keith, T. Z. *Multiple Regression and Beyond*, Allyn and Bacon, Boston, MA, 2006.

Krause, D. R., Handfield, R. B. and Tyler, B. B. "The relationships between supplier development, commitment, social capital accumulation and performance improvement," *Journal of Operations Management* (25), 2007, pp. 528-545.

Lawson, B., Tyler, B. B. and Cousins, P. D. "Antecedents and consequences of social capital on buyer performance improvement," *Journal of Operations Management* (26), 2008, pp. 446-460.

Liang, H. and Xue, Y. "Avoidance of information technology threats: A theoretical perspective," *MIS Quarterly* (33:1), 2009, pp. 71-90.

Lu, H.-P., Hsu, C.-L. and Hsu, H.-Y. "An empirical study of the effect of perceived risk upon intention to use online applications," *Information Management & Computer Security* (13:2), 2005, pp. 106-120.

Maloncy, P. "Social networking throws up vital role for information security staff," *Computer Weekly* (May 6, 2008), 2008, pp. 1-2.

Mansfield-Devine, S. "Anti-social networking: Exploiting the trusting environment of Web 2.0," *Network Security* (November 2008), 2008, pp. 4-7.

Martinez Aleman, A. M. and Wartman, K. L. *Online Social Networking on Campus: Understanding What Matters in Student Culture*, Routledge, New York, NY, 2009.

Mathieson, K., Peacock, E. and Chin, W. W. "Extending the technology acceptance model: The influence of perceived user resources," *The DATA BASE for Advances in Information Systems* (32:3), 2001, pp. 86-112.

Nahapiet, J. and Ghoshal, S. "Social capital, intellectual capital, and the organizational advantage," *Academy of Management Review* (23:2), 1998, pp. 242-266.

Robert, L. P., Dennis, A. R. and Ahuja, M. K. "Social capital and knowledge integration in digitally enabled teams," *Information Systems Research* (19:3), 2008, pp. 314-334.

Schneier, B. *Schneier on Security*, Wiley Publishing, Indianapolis, IN, 2008.

Schonfeld, E. *Social site rankings*. 2007, Retrieved April 12, 2009, from <http://www.techcrunch.com/2008/12/31/top-social-media-sites-of-2008-facebook-still-rising/>.

Schonfeld, E. *Top social media sites of 2008 (Facebook still rising)*. 2008, Retrieved April 12, 2009, from <http://www.techcrunch.com/2008/12/31/top-social-media-sites-of-2008-facebook-still-rising/>.

Sharma, S., Durand, R. M. and Gur-Arie, O. "Identification and analysis of moderator variables," *Journal of Marketing Research* (18), 1981, pp. 291-300.

Shostack, A. and Stewart, A. *The New School of Information Security*, Addison-Wesley, Upper Saddle River, NJ, 2008.

Slovic, P. "Trust, emotion, sex, politics and science: Surveying the risk-assessment battlefield," in *The Perception of Risk* (P. Slovic (Ed.), Earthscan, London, UK. 2000.

Slovic, P., Fischhoff, B. and Lichtenstein, S. "Behavioral decision theory," *Annual Review in Psychology* (28), 1977, pp. 1-39.

Son, J.-Y. and Kim, S. S. "Internet users' information privacy-protective responses: A taxonomy and a nomological model," *MIS Quarterly* (32:3), 2008, pp. 503-529.

Stone, E. F. and Stone, D. L. "Privacy in organizations: Theoretical issues, research findings, and potection mechanisms," in *Research in Personnel and Human Resources Management* (Vol. 8), K. M. Rowland & G. R. Ferris (Eds.), JAI Press, Greenwich, CT. 1990, pp. 349-411.

Thompson, R. L., Higgins, C. A. and Howell, J. M. "Personal computing: Toward a conceptual model of utilization," MIS Quarterly (15:1), 1991, pp. 124-143.

Tsai, W. and Ghoshal, S. "Social capital and value creation: The role of interfirm networks," Academy of Management Journal (41:4), 1998, pp. 464-476.

Wasko, M. M. and Faraj, S. "Why should I share? Examining social capital and knowledge contribution in electronic networks of practice," MIS Quarterly (29:1), 2005, pp. 35-57.

Whitaker, A., Evans, K. and Voth, J. B. Chained Exploits: Advanced Hacking Attacks from Start to Finish, Addison-Wesley, Upper Saddle River, NJ, 2009.

Yang, S., Lee, H. and Karnia, S. "Social capital in information and communications technology research: Past, present, and future," Communications of the AIS (25:23), 2009, pp. 194-220.