A Study of the Effect of Privacy Assurance Mechanisms on Self-disclosure in Social Networking Sites from the View of Protection Motivation Theory

Completed Research Paper

Mohammadreza Mousavizadeh
University of North Texas
1155 Union Circle #311160
Denton, TX 76203 – 5017
mohammadreza.mousavizadeh@unt.edu

Dan J. Kim
University of North Texas
1155 Union Circle #311160
Denton, TX 76203 – 5017
dan.kim@unt.edu

Abstract

Along with recent advancement of web technologies, social networking sites (SNSs) affect people's life styles by enabling them to perform different activities which are not easy to do before. Predominant uses of SNSs allow users to quickly access and easily share personal information. In turn, users' information privacy issues become important challenge. Drawing upon Protection Motivation Theory, this research investigates the effect of privacy assurance mechanisms (i.e., privacy assurance statements and privacy customization features) on users' privacy concern and disclosure behavior. The results show that privacy assurance statements significantly influence SNS users' privacy concern by affecting users' assessment of threat susceptibility and effectiveness of assurance mechanisms; privacy customization features significantly influence users' self-efficacy and perceived effectiveness of assurance mechanisms; SNS users' privacy concern results form a risk calculus process in which users assess the threat and available coping mechanisms; and the effect of privacy concern on self-disclosure mediates by users' protection motivation.

Keywords: Privacy assurance mechanisms, privacy assurance statement, privacy customization, protection motivation theory, online privacy concern, and self-disclosure

Introduction

Along with recent advancement of web technologies, social networking sites (SNSs) affect people's life styles by enabling them to perform so many different activities which were not easy to do before. Ofcom technology tracker reports that over 50% of the internet users stated that using SNSs is one of the major reasons of using the Internet (Ofcom 2014). SNS users are able to quickly access and easily share personal information and opinions such as pictures of friends and family, and political views (Jiang, Heng and Choi 2013). Because of such predominant and rampant of SNSs, users' information privacy issues become important challenge not only for SNS users but also for the SNS service providers and governing organizations (Boyd and Ellison 2010).

Rainie, Kiesler, Kang and Madden (2013) report that more than 50% of the Internet users express that they are concerned with their information privacy; 66% of them posit that current law does not protect them against privacy threats. Moreover, results of a survey, conducted in the United States, reveal that among the SNS users who are concerned with information privacy, majority of them still disclose their personal information on SNSs (Madden, Fox, Smith and Vitak 2007). It seems that many SNS users tend to disclose their personal information in SNSs while they are still concerned with the privacy of their information. Thus, it is interesting to investigate why SNS users are still interested in sharing their information on SNSs while they are concerned with their privacy. We guess several reasons for this contradictory sharing behavior of SNS users. One possible reason is that SNSs are applying several privacy assurance mechanisms to ensure their users concerns with their privacy (Squicciarini, Paci and Sundareswaran 2010). Therefore, it is an interesting and timely issue to empirically test the effect of privacy assurance mechanisms on SNS users' privacy concern and behavioral intentions such as protection motivation and information disclose behavior.

Drawing upon the literature review on online privacy concern, we identify that while the information system research has made some progresses on understanding antecedents of SNS users' privacy concern, still there are some gaps that should be addressed. First, although practitioners applied different mechanisms to address privacy concern, there are some gaps in the literature regarding theory-oriented investigation of how these mechanisms affect online privacy concern (Bansal, Zahedi and Gefen 2008; Kim, Steinfield and Lai 2008; Squicciarini et al. 2010). Second, privacy assurance mechanisms are mostly investigated in the e-commerce context. Thus, there is a gap in the literature on how privacy assurance mechanisms affect SNS users' privacy concern and disclosure behavior. Third, protection motivation theory (PMT) has been applied in IS literature to study protection attitudes and behavior (e.g., Bulgurcu, Cavusoglu and Benbasat 2010; Crossler, Long, Loraas and Trinkle 2014; Herath and Rao 2009; Johnston and Warkentin 2010) without considering fear or risk as part of PMT (Floyd, Prentice-Dunn and Rogers 2000; Tanner Jr, Hunt and Eppright 1991). Hence, there is an opportunity to apply PMT in the SNS context to investigate online privacy concern and self-disclosure by applying the concept of fear from PMT. Finally, although PMT suggests that fear appeal process leads to change in attitude and behavior regarding a threat, most of previous studies only investigated fear appeal effect on protection related behaviors. Prior studies mostly investigated the effect of protection motivation on behavioral intention to uses protection mechanism. Our study may be able to investigate whether fear appeal process suggested by PMT can affect SNS users to not to disclose their information or just motivate them to protect their information by applying different types of protection mechanisms other than those they currently use.

To address the existing gaps, we focus on a set of privacy assurance mechanisms used on most SNSs and propose a risk calculus process in which these mechanisms affect SNS users' privacy concern and self-disclosure behavior. Therefore, the objectives of this research are:

- To study how privacy assurance mechanisms affect SNS users' protection motivation by applying PMT as the theoretical lens.
- To investigate the influence of privacy concern as part of the PMT on SNS users' protection motivation and self-disclosure.

This study formulates a conceptual research model by applying PMT as the overarching theory. PMT postulates that individuals' protection motivation is formed by a cognitive process. In this cognitive process individuals evaluate the effectiveness of the in hand coping mechanisms and the existing threat. The output of this cognitive process which is named fear appeal is the level of protection motivation in an

individual (Maddux and Rogers 1983; Rogers 1975). More specifically, PMT posits that an individual's protection motivation is the result of their fear of a threat and this fear is the consequence of the threat significance and coping power that an individual perceives.

In addressing our research objectives, we argue that the existing privacy assurance mechanisms on a SNS influence Users' appraisal of threat severity and vulnerability, and coping mechanisms. This appraisal process forms a level of privacy concern of users. Finally, their level of privacy concern affects their motivation to protect their information and disclose themselves on a SNS.

This study makes a number of contributions. (1) This work extends the information assurance literature by applying PMT to theoretically explain the risk calculus process in which users' privacy concern is formed. (2) This paper also introduces protection motivation as a mediator of the effect of privacy concern on self-disclosure which was overlooked by prior studies. (3) We also introduce privacy customization features exist on the SNS as another type of privacy assurance mechanism which have not been studied by previous research. (4) Although previous research has investigated privacy assurance mechanisms in e-commerce context, this study is one of the first studies that investigates privacy assurance mechanisms on SNSs. (5) SNSs may apply the findings of this study to decrease users' privacy concern and motivate them to share more personal information about themselves. To this end, they can provide more in-depth privacy assurance statements and design more customizable privacy related features to influence the risk calculus process that affects users' privacy concern.

Literature Review and Background Theory

Assurance Mechanisms, Privacy Concern, and Online Self-disclosure

Online privacy assurance refers to "mechanisms that directly or indirectly provide customers with assurances and guarantees that their private information will be protected and kept private by the website" (Bansal, Zahedi and Gefen 2015). SNS users can be considered as customers in this definition. Privacy assurance mechanisms have been studied in e-commerce context with different research constructs (Bansal et al. 2015): most studies explore the effect of privacy assurance statement as a primary privacy assurance mechanism on trust in e-commerce websites (Liu, Marchewka and Ku 2004; McKnight, Choudhury and Kacmar 2002; Wu, Huang, Yen and Popova 2012); some others investigate its effect on intention to disclose information (Meinert, Peterson, Criswell and Crossland 2006; Peterson, Meinert, Criswell and Crossland 2007; Wang, Beatty and Foxx 2004).

Self-disclosure refers to "what individuals voluntarily and intentionally reveal about themselves to others – including thoughts, feelings and experiences" (Posey, Lowry, Roberts and Ellis 2010). Self-disclosure is an activity that has several benefits and risks for the person who performs this activity (Xu, Teo, Tan and Agarwal 2009). Self-disclosure has been investigated in many contexts. A group of studies elaborated the factors that affect customers to disclose their information on e-commerce websites (e.g., Culnan and Armstrong 1999; Dinev and Hart 2004; Laufer and Wolfe 1977). Some other studies investigated the antecedents of information disclosure on SNSs (Chen 2013; Chen and Sharma 2015; Jiang et al. 2013; Posey et al. 2010).

Prior research posited different factors that affect online self-disclosure. Posey et al. (2010) suggested that social benefits and costs together with social norms and perceived collectivism influence online community users to disclose their personal information. Extroversion and internet risk are other factors that were suggested by previous studies as antecedents of self-disclosure (Chen 2013; Chen and Sharma 2015). Koohikamali, Gerhart and Mousavizadeh (2015) also argued that incentives may affect SNS users to disclose their location (as a type of personal information).

Different theories has been applied by previous studies to investigate self-disclosure behavior on online communities (Li 2012). Risks and benefits trade-off perspective was applied by several researchers to explain the antecedents of self-disclosure. Jiang et al. (2013) suggested that privacy concerns and social rewards are important antecedents of self-disclosure behavior on SNSs. The trade-off between disclosure-privacy benefits and risks was suggested as an important factor that affects self-disclosure on online communities (Xu et al. 2009). Prior researches posit several benefits of self-disclosure such as formation of intimacy with others (Altman and Taylor 1973), social acceptance or opinion leadership (Chen 2013), reduction in stress by emotional experiences (Greenberg and Stone 1992). Some other studies suggest

privacy concern as the main risk for individuals when they share their personal information on online communities (Dwyer, Hiltz and Passerini 2007; Ioinson and Paine 2007). Theory of reasoned action by Fishbein and Ajzen (1975) is another theoretical lens that was used by several studies to investigate the antecedents of self-disclosure behavior (Chen and Sharma 2015; Koohikamali et al. 2015).

Information privacy refers to "an individual's right to determine how, when, and to what extent information about the self will be released to another person or to an organization" (Buchanan, Paine, Joinson and Reips 2007). Many studies used different theoretical perspectives to study antecedents of privacy concern in online environment (Li 2012). Privacy calculus theory is one of the theories used by several studies to frame the antecedents of online privacy concern (Culnan and Armstrong 1999; Dinev and Hart 2004; Dinev and Hart 2006; Hann, Hui, Lee and Png 2007). This theory suggests that individuals intend to disclose information based on a calculus of positive and negative outcomes of disclosure behavior (Li 2012). Another theoretical lenses that has been used to study online privacy concern are personality theories (e.g., Bansal and Gefen 2010; Junglas, Johnson and Spitzmüller 2008; Korzaan and Boswell 2008). Studies that applied these theories aimed to investigate the personality related factors that affect individuals' online privacy concern.

Background Theory

PMT, developed by Rogers (1975), explains and predicts protection attitudes and behaviors of an individual who is exposed to a threat (Maddux and Rogers 1983; Rogers 1975; Weinstein 1993). This theory is one of those theories that has been used by researchers to investigate the privacy in different contexts (Chai, Bagchi-Sen, Morrell, Rao and Upadhyaya 2009; Dinev and Hart 2004; Junglas et al. 2008; Youn 2009). PMT suggests that there are three important component in fear appeal: (1) the severity of the threat' negative outcomes; (2) The probability that the threat occurs; and (3) the efficacy of protective responses (Rogers 1975). Maddux and Rogers (1983) revise the original version of PMT by adding self-efficacy as the forth component that affects protection motivation behavior. PMT suggests two cognitive processes that an individual carry out to cope with a threat: threat appraisal and coping appraisal. As the output of this process a level of fear from the threat is formed in an individual (Floyd et al. 2000; Maddux and Rogers 1983).

Generally, threat is defined as "something that is a source of danger that can bring harm (physical or mental) to an individual" (Junglas et al. 2008). According to PMT, threat appraisal is a process of estimating the severity and susceptibility of a threat while coping appraisal refers to the process of evaluating the efficacy of protection responses and the perceived self-efficacy of the individual who is exposed to the threat (Junglas et al. 2008). While the original and the revised versions of the PMT suggest that the threat and coping appraisal are parallel processes that happen concurrently (Maddux and Rogers 1983; Rogers 1975), a number of studies argue that these two processes are sequential (Scherer 1988; Tanner Jr et al. 1991). Tanner Jr et al. (1991) argue that threat appraisal must occur prior to other evaluations such as coping appraisal. PMT also addresses that there are two sources of information that influence the threat and coping appraisal: environmental and inter-personal sources of information. Environmental sources of information are verbal persuasion and observation and inter-personal sources consist of personality variables and prior experiences (Floyd et al. 2000).

Research Model and Hypotheses

In this study we applied PMT as the background theory to investigate self-disclosure behavior of SNS users. PMT was applied in several previous researches to study online privacy concern in different contexts (e.g., Mohamed and Ahmad 2012; Youn 2009). For example, Youn (2009) applied PMT to study privacy concern and factors influence website users to provide personal information to the websites. Thus, this study created the research model based upon PMT. Applying PMT, privacy assurance statement and privacy customization features on the SNS are considered as environmental sources of information that influence users' threat and coping appraisal. SNS users process these sources of information to evaluate vulnerability of and severity from the threat. They also evaluate the effectiveness of privacy assurance mechanisms and their self-efficacy based on these sources of information. Prior research named this evaluation process as risk calculus (Li 2012) in which users evaluate the threat significance and coping strength of themselves. The output of the risk calculus process is their perceived fear of or concern with sharing personal information on SNS. According to PMT, users' fear from threat (privacy concern)

influence their protection motivation and protection-related behavior (Maddux and Rogers 1983; Rogers 1975; Weinstein 1993).

Considering PMT as our theoretical lens in the context of SNSs, we propose our research model (see Figure 1). This research model proposes that privacy assurance mechanisms affect SNS users' privacy concern via the cognitive process of risk calculus; SNS users' privacy concern affects their protection motivation (As the output of PMT) and the self-disclosure behavior; and protection motivation mediates privacy concerns on self-disclose behavior.

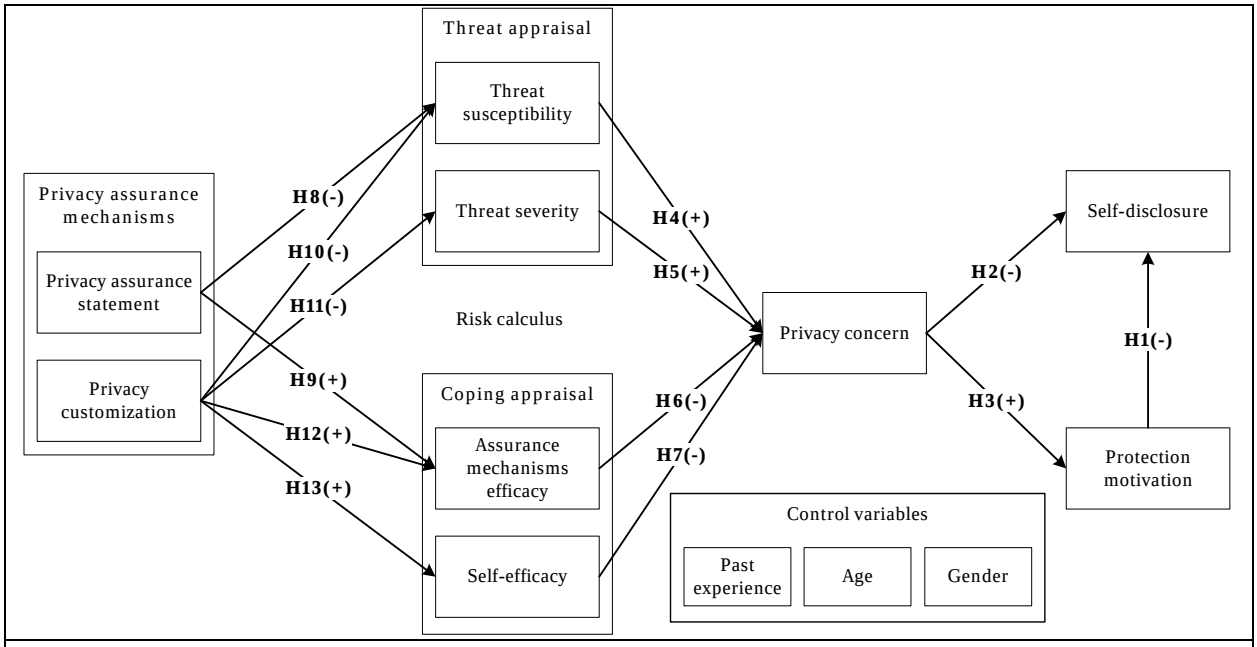

Figure 1. Reserach Model

PMT suggests that protection motivation refers to individual's intention to perform protection behavior (Boer and Seydel 1996; Norman, Boer and Seydel 2005). Theory of reasoned action argues that Behavioral intention regarding a behavior affects an individual to perform that behavior (Fishbein and Ajzen 1975). Therefore, when SNS users are more motivated to protect their information, they perform protective behaviors. According to Wurtele and Maddux (1987) individuals who are more motivated to perform protective behavior, employ "pre-caution strategy". In this strategy they act cautiously to be safe from the threat. Raman and Pashupati (2004) argue that individuals employ two different strategies to protect their privacy in the internet: approach, and avoidance. Approach strategy results in seeking for a solution and avoidance strategy lead users to refuse using internet. When SNS users want to protect their privacy on the SNS, it is more likely for them to employ avoidance strategy since they already evaluated the coping mechanisms and based on their evaluation they are motivated to protect their privacy. In other words, some SNS users are intent on protecting their information based on their appraisal of threats and coping mechanisms in that situation. These users know that there is only one solution for them to protect their information since they are already applying the existing assurance mechanisms. This solution is to not to disclose their personal information. Other SNS users who are not intent on protecting their information based on their appraisal of the SNS will not be that cautious regarding sharing their information. Hence, they are more likely to share their personal information on the SNS. So we hypothesized that:

H1: The amount of protection motivation SNS users feel negatively affects their self-disclosure behavior.

Dwyer et al. (2007) suggest that SNS users who are more concerned with their privacy, share their information less frequently on SNS compare to those who have not such concern. Privacy concern is suggested as an important impediment for internet users whenever they want to share their information on the internet (Youn 2009). Online privacy concern is defined as "individuals' concern about the threat

to their information privacy when submitting their personal information on the Internet" (Bansal et al. 2015). According to this definition, when SNS users perceive that the SNS cannot protect their information against a threat, they perceive more privacy concern. A possible reaction to this concern is to decide to not to share their personal information. Indeed, SNSs are supposed to provide protection over SNS users' information to address their privacy concerns otherwise users will not share their information on SNS (Chen 2013; Westin 1967). This protection is a claim made by SNS and SNS is supposed to act based on that. This leads to the following hypothesis:

H2: SNS users' privacy concern negatively affects their self-disclosure behavior.

According to PMT, people assess their coping strength and their vulnerability when they make decision to share information. This assessment results in a certain level of fear from Threat. PMT argues that the more individuals fear from a threat the more they will be motivated to perform a protection behavior (Boer and Seydel 1996; Floyd et al. 2000; Norman et al. 2005). Privacy concern in online communications refers to fear of being monitored, losing anonymity, identity theft, and so forth (Brown and Muchira 2004; Lee 2000; Milne and Culnan 2004; Miyazaki and Fernandez 2000; Miyazaki and Fernandez 2001; Youn 2009). Hence, SNS users who are more concerned with their privacy on a SNS, feel more fear from sharing information on SNS. Users' privacy concern (fear of threat) affects users' behavioral intention to disclose their information (Bansal et al. 2015; Pavlou 2003). To response to this concern those who have higher level of concern, are more intent to protect their information on that SNS. Thus, we suggest that:

H3: SNS users' privacy concern positively affects their motivation to protect their information.

Threat appraisal process refers to the assessment of possible threats which exist in the relationship between SNS user and the SNS as a potential sources of harm or lose (Solomon, Mikulincer and Benbenishty 1989). Threat appraisal is a cognitive process in which an individual assess the risks of performing a specific behavior. The result of this assessment is a certain level of risk or fear perceived by that individual (Folkman 1984). In the context of SNS, users assess the risks of sharing information in a similar way. SNS users evaluate severity of the potential negative outcomes of sharing personal information and their vulnerability to these potential outcomes. This assessment form the level of fear from sharing personal information on SNS. This fear of losing privacy named online privacy concern in online communications (Brown and Muchira 2004; Lee 2000; Milne and Culnan 2004; Youn 2009).

According to PMT literature, threat appraisal is the result of an assessment of threat severity and susceptibility (Rogers, Cacioppo and Petty 1983). Threat severity refers to the extent to which the SNS users are vulnerable to losing their privacy while the threat susceptibility refers to the probability of occurrence of a privacy threat (Johnston and Warkentin 2010). When SNS users believe that the privacy threat is more probable to happen, they feel more fear from sharing their information. In fact, they perceive that they are more likely to be subjected to negative consequences of sharing information. Similarly, the severity of the potential negative consequences of sharing on SNS intensify SNS users' fear of losing privacy. As a result, we suggest the following hypotheses:

H4: SNS users' perceived threat susceptibility positively affects their privacy concern.

H5: SNS users' perceived threat severity positively affects their privacy concern.

Coping appraisal process refers to someone's assessment of his/her ability to cope with a threat (Rogers et al. 1983). According to PMT individuals' perception of their ability to avert with the threat affect their perception about the effectiveness of the coping responses (Rogers 1975; Rogers et al. 1983). Therefore, they may perceive less fear of the threat when they believe that they are armed with effective coping mechanisms. Individuals' perception of having control over a specific situation is the result of their assessment of their coping ability in that situation. This perceived control affects individuals' perceived fear in that situation (Dinev and Hart 2004; Folkman 1984). In the SNS context, privacy refers to someone's right to disclose his/her information (Westin 1967). Individuals' control over their information is a condition of that right. SNS users' perception of coping ability against threat of losing information enhances their perceived control over the threat. Finally, SNS users, who have more control over their information, perceive less concern with their privacy.

PMT suggests that coping appraisal is broken to two separate processes: (1) to assess the effectiveness of the coping mechanisms that someone can use against a threat (response efficacy), and (2) to evaluate one's ability to apply coping mechanisms against a threat (self-efficacy) (Maddux and Rogers 1983;

Rogers et al. 1983). When SNS users feel that privacy assurance mechanisms are more effective, they perceive more control over their information. According to Bowman and Stern (1995), individuals' perceived control over a threat comes from their perception of the effectiveness of coping mechanisms. Additionally, self-efficacy is another important factor that affects someone's ability to protect his/her information by using coping mechanisms. Individuals' perception of their ability to use assurance mechanisms which are available on the SNS, affects their perceive control. Thus, they believe that they are able to control the threat whenever they are in a risky situation. These SNS users perceive less concern with sharing their information on the SNS. Therefore, we hypothesize:

H6: SNS users' perceived effectiveness of assurance mechanisms negatively affects their privacy concern.

H7: SNS users' self-efficacy negatively affects their privacy concern.

Privacy assurance mechanisms are considered as coping mechanisms to SNS users that enable them to protect themselves against threats of information disclosure (Bansal et al. 2015). Privacy assurance statement refers to one of the main messages and arguments that websites communicate with their users to ensure the adequacy of their protection measures against users' privacy threats (Bansal et al. 2015). In fact, in the context of this study privacy assurance statement refers the extent to which privacy assurance statement communicates SNS service providers' efforts and commitments toward preventing threats against users' privacy. According to Rogers and Thistlethwaite (1970), individuals who are exposed to threats seek to find assurance against those threats. Thus, SNS users seek to find information about how the SNS protect them against privacy threats. The more protection that SNS users perceive from the statement the less they perceive the privacy threat to be susceptible. The reason is that the privacy statement reflects how and for what purposes customer's information will be used. therefore, privacy assurance statement affects users to have better assessment of the risks of information disclosure behavior (Bansal et al. 2008). It means that the presence of privacy assurance statement helps them to better evaluate the susceptibility of privacy threats since they are more informed about SNS's privacy policy. In fact, the privacy statement assures SNS users that their information will be safe on the SNS and it will be used for the purposes that do not have any negative consequences for them. Consequently, we posit that:

H8: Privacy assurance statement negatively affects SNS users' perceived threat susceptibility.

Assurance mechanisms efficacy refers to effectiveness of the assurance mechanisms which are available on the SNS (Witte 1992) such as privacy assurance mechanisms or privacy customization features. Privacy assurance statement on a SNS affects its users' evaluation of the coping mechanisms on the SNS. Presence of privacy assurance statement on a SNS reflects that the SNS aims to protect its users' personal information (Stutzman, Capra and Thompson 2011) and for this purpose that SNS develops several predefined processes. The main goal of Privacy assurance statement is to improve the awareness of SNS users regarding the SNS activities to protect users' privacy. Therefore, users understanding about this statement affects their perceive effectiveness of the SNS's assurance mechanisms. Thus, we suggest that:

H9: Privacy assurance statement positively affects SNS users' perceived effectiveness of privacy assurance mechanisms.

Privacy customization in this study refers to users' efforts to use technological features, available on the SNS, to protect their information privacy by controlling the flow of their information in SNS (Xu, Teo, Tan and Agarwal 2012). Those users' who set their privacy preferences are less likely to have any privacy issues compare to those who do not. Individuals employ "pre-caution" strategy in order to protect themselves from threat (Maddux and Rogers 1983). Similarly SNS users limit the access of other users to their personal information to decrease the probability of the occurrence of privacy threat. Therefore, SNSs which enable users to customize their privacy preferences decrease their users' perceived threat susceptibility. Additionally, this cautious behavior of SNS users affect their perceived vulnerability to privacy threats. The reason is that the cautious users protect their information to be accessible by those trustable users. Thus, they will not lose their privacy as much as those who do not customize their privacy preferences. Consequently, we hypothesize that:

H10: Privacy customization features which are available on SNSs negatively affect SNS users' perceived threat susceptibility.

H11: Use of privacy customization features which are available on SNSs negatively affects SNS users' perceived threat severity.

When SNS users are able to change their privacy preferences on SNS (ability to specify who can see your posts, photos, and etc.), they perceive more control over the information they disclose on the SNS (Stutzman et al. 2011). Perceived control affects SNS users' perception regarding the effectiveness of the assurance mechanisms (Arcand, Nantel, Arles-Dufour and Vincent 2007). The privacy customization features on the SNS help users to cope with the risk of unauthorized access to their information. Therefore, these features affect their assessment of the coping mechanisms on the SNS. SNS users who are able to customize their privacy preferences are more likely to share their information. The reason is that they perceive that the SNS privacy customization feature is effective and is able to protect their privacy. If they did not have such perception they would not share their information on SNS. Additionally, SNS users' perceived control over their information affects their self-efficacy. They perceive that they are able to protect their information by using these features (Stutzman et al. 2011). In fact, these features influence users' perception of their ability to control others' access to their information. Users' perceived control influences their assessment of the coping mechanisms. As a result, we hypothesized that:

H12: Use of privacy customization features which are available on SNSs positively affects SNS users' perceived effectiveness of privacy assurance mechanisms.

H13: Use of privacy customization features which are available on SNSs positively affects SNS users' self-efficacy.

In addition, this study includes several control variables such as age, gender, and past experience in the research mode because prior studies has reported the potential impacts of age, gender, and past experience on the self-disclosure(Chen and Sharma 2015; Wakefield 2013).

Research Methodology

Measurement

Most of the items in our measurement model were adopted from prior studies. We defined some new items to measure a number of new constructs we proposed in this study (See Appendix 1). The reason was that we did not find appropriate items in previous literature for those constructs. Moreover, we measured all items by using 7-points Likert scale.

Data Collection

The data was collected from undergraduate students of a large university in southwest United States. Students were voluntarily participated in online surveys with course credits. 256 students participated in our survey. Other than currently active users of SNSs, there were no other filtering criteria in this study. After removing incomplete and invalid responses, we ended up with a sample of 241 respondents indicating a usable sample size rate of 94.1%. Table 1 shows a summary of demographic information of the respondents. As shown in the table, ages is heavily weighted toward 18-25 years old (80.1%). Undergraduate students are mostly young and educated. According to Lenhart, Purcell, Smith and Zickuhr (2010), this age group fits within the largest group of SNS users.

Table 1. Demographic Information of Survey Respondents.		
Gender	120 Male (49.8%)	121 Female (50.2%)
Age	193 respondents are within age group 18-25 years (80.1%)	
Dispensable Income per year	175 respondents have less than $15000 dispensable income (72.6%)	

Data Analysis

To test our research model we applied structural equation modeling by using Smart PLS 2.0. Partial Least Square (PLS) measures the direction of relationships and those strengths by using metric properties of the measurement scale (Barclay, Higgins and Thompson 1995). This study applied three steps of analysis: (1) An assessment of measurement model by evaluating item reliability and validity, (2) a check for the

presence of common method bias, and (3) a structural model assessment to evaluate the model's predictive power.

Measurement Model Assessment

To check the adequacy of the measurement model, this study examined items reliability and validity (Hulland 1999). The reliability of each construct is assessed by analyzing the Cronbach's alpha, and composite reliability. Values above 0.7 typically indicate acceptable reliability of the measurement model (Nunnally and Bernstein 1978; Nunnally, Bernstein and Berge 1967). Average Variance Extracted (AVE) is also used to test for the convergent validity. AVE values above the benchmark of 0.70 are generally deemed as adequate and show that the latent variable explains more than half of the variation in the indicators (Fornell and Larcker 1981). The diagonal values on Table 2 represent the square root of AVE. These are measures for the variance shared between a construct and its indicators and explain the convergent validity of the measurement model. The values of Cronbach's alpha, composite reliability, and AVE, demonstrate the internal consistency and convergent validity of the measurement model.

To test for the discriminant validity of the measurement model, this study applied two methods. First, AVE values are supposed to be greater than the off-diagonal correlations which is true in our case (see Table 2). Second, the related items of each construct are supposed to load highly on the factor the construct measures and cross-loadings are supposed to be lower than the within construct loadings (See Appendix 2) (Ko, Kirsch and King 2005).

Table 2. Correlation Matrix

Construct	AVE	CR	CA	1	2	3	4	5	6	7	8	9
1. Self-disclosure	0.71	0.91	0.89	**0.84**								
2. Protection motivation	0.73	0.93	0.91	-0.20	**0.85**							
3. Privacy concern	0.85	0.96	0.94	-0.07	0.38	**0.92**						
4. Threat susceptibility	0.81	0.95	0.94	-0.09	0.11	0.43	**0.90**					
5. Threat severity	0.85	0.96	0.94	-0.11	0.23	0.27	0.26	**0.92**				
6. Assurance mechanisms efficacy	0.86	0.95	0.92	0.15	0.08	-0.23	-0.31	-0.04	**0.93**			
7. Self-efficacy	0.88	0.96	0.93	0.23	0.15	-0.02	-0.14	0.01	0.43	**0.94**		
8. Privacy assurance statement	0.86	0.95	0.92	0.19	-0.12	-0.22	-0.33	-0.06	0.60	0.29	**0.93**	
9. Privacy customization	0.72	0.93	0.90	0.03	0.34	0.12	-0.06	0.07	0.21	0.54	0.06	**0.85**

Note: CR: composite reliability, CA: Cronbach's alpha.
The diagonal elements (in bold) represent the square roots of AVE.

Common Method Bias

Common Method Bias (CMB) could be an important source of measurement error (Podsakoff, MacKenzie, Lee and Podsakoff 2003). Presence of CMB may result in erroneous conclusions (Campbell and Fiske 1959). To evaluate the presence of the CMB in our measurement model we applied two different methods. First we applied Harman's single factor test suggested by Podsakoff et al. (2003). They suggest that CMB exists in the measurement model in two conditions: (1) a single factor in the factor analysis, and (2) a single factor in factor analysis which accounts for majority of the covariance among the variables.

The results of unrotated factor analysis for all 35 indicators show that 9 factors account for 80.4% of the variance and the first factor accounts for less than 50% of the total variance (21.9%). Hence, applying the Harman's single factor test for CMB, we conclude that CMB is not a serious issue in the measurement model.

The second method that we used to check for presence of CMB was an approach suggested by Podsakoff et al. (2003) following the procedure of Liang, Saraf, Hu and Xue (2007). As shown in Appendix 3, the results revealed that the theoretical constructs were loaded highly significant while the CMB construct was loaded non-significant on all items in our measurement model. Therefore, CMB is unlikely to be present in our measurement model.

Structural model assessment

This study examined the path coefficients and R-square to assess the structural model. Path coefficient indicates the strength of the relationship between constructs and R-square shows the predictive power of the model. The results of the structural model assessment revealed that most of the hypothesized relationships are significant (See Figure 2). The results also revealed that the control variables were included in this study were non-significant ($p > .05$) Table 5 represents a summary of the results.

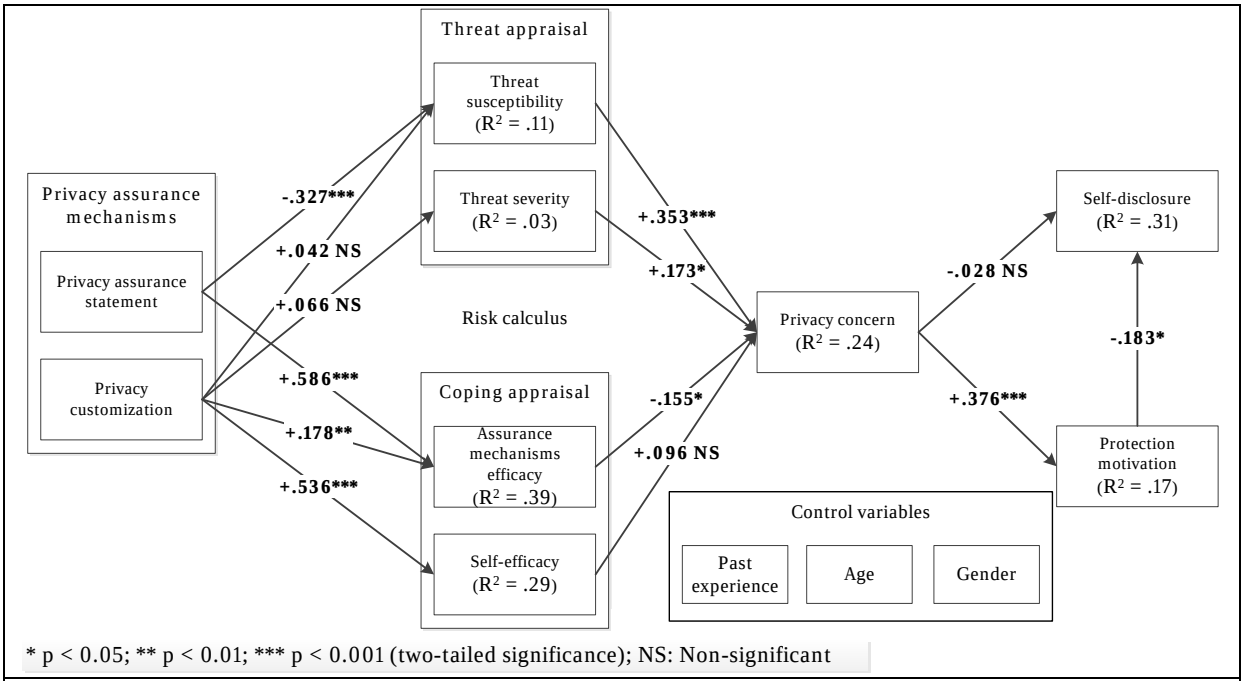

Figure 2. Structural Model Assessment Results

Discussion

The results of this study revealed that the privacy assurance statement affects privacy concern by decreasing the susceptibility of privacy threat and increasing perceived effectiveness of assurance mechanisms. Moreover, results of this study revealed that privacy customization features on SNSs do not have a significant influence on users' appraisal of the threat. One possible reason is that when SNS users use privacy customization features, they believe that there are some other threats such as threats from hackers, blackmails, and etc. that cannot be controlled by customizing privacy preferences. According to Xu et al. (2012), privacy customization is one of the technological approaches that is available on websites that enable users to protect their information. Xu et al. argue that there are several other approaches such as anonymous web surfing tools, cookie management tools, and etc. that enable website users to protect themselves about other types of threats. Therefore, these users perceive that some uncontrolled factors may still threat their privacy and privacy customization is not an appropriate mechanism to control these factors. The results of our study also support the positive influence of privacy customization features on

the perceived effectiveness of assurance mechanisms and SNS users' self-efficacy. PMT postulates that people process available information in the environment to assess existing threats and their coping strength against these threats (Milne, Sheeran and Orbell 2000). Findings of this study support that assurance mechanisms on SNSs are considered as a source of information for users. These information enable users to evaluate privacy threats and their coping strength against them.

Table 3: Summary of Structural Model Assessment Results

Hypothesis	Path coefficient	Result
H1: Protection motivation → Self-disclosure	-0.183*	Supported
H2: Privacy concern → Self-disclosure	-0.013	Not Supported
H3: Privacy concern→ Protection motivation	-0.376***	Supported
H4: Threat susceptibility → Privacy concern	+0.353***	Supported
H5: Threat severity → Privacy concern	+0.173*	Supported
H6: Assurance mechanisms efficacy → Privacy concern	-0.155*	Supported
H7: Self-efficacy → Privacy concern	+0.096	Not Supported
H8: Privacy assurance statement → Threat susceptibility	-0.327***	Supported
H9: Privacy assurance statement → Assurance mechanisms efficacy	+0.586***	Supported
H10: Privacy customization → Threat susceptibility	+0.042	Not Supported
H11: Privacy customization → Threat severity	+0.066	Not Supported
H12: Privacy customization → Assurance mechanisms efficacy	+0.178**	Supported
H13: Privacy customization → Self-efficacy	+0.536***	Supported
Note: * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$ (two-tailed significance)		

Additionally, our results posits a strong role for threat appraisal as an antecedent of privacy concern which is consistent with PMT point of view that suggests that fear results from threat appraisal (Rogers et al. 1983). Although the effectiveness of assurance mechanisms negatively affects privacy concern, there is no significant relationship between self-efficacy and privacy concern. The insignificant effect of self-efficacy is consistent with the results of previous studies in the online privacy concern literature (Youn 2009). Furthermore, this paper found that privacy concern does not have a significant effect on self-disclosure. After we tested the mediator effect of protection motivation we found that protection motivation fully mediates the effect of privacy concern on self-disclosure. Finally, the results of this study revealed that age, gender, and past experiences does not matter in studying self-disclosure behavior in the context of SNS.

Implications

This study has implications for academia and practice. From a theoretical point of view, this study successfully applied PMT to investigate self-disclosure on SNSs. The PMT provided a theoretical lens for this study to conceptualize a model that explains the antecedents of self-disclosure on a SNS based on different assurance mechanisms that exist on that SNS. Moreover, the results of this study revealed that motivation protection mediates the effect of privacy concern on self-disclosure. Although prior researches have investigated the effect of privacy concern on protection motivation (Youn 2009) and self-disclosure (e.g., Dwyer et al. 2007; Jiang, Chan, Tan and Chua 2010; Joinson, Reips, Buchanan and Schofield 2010), to the best of our knowledge this study is the first one that investigates the mediator effect of protection motivation on the effect of privacy concern on self-disclosure by applying PMT. Therefore, this paper makes novel contributions by extending PMT in the following ways. (1) This work is the first one that applied PMT to theoretically explain how privacy assurance mechanisms affect SNS users' privacy

concern and ultimately their self-disclosure behavior. According to Bansal et al. (2015) most of previous researchers studied privacy assurance mechanisms in the context of e-commerce. Hence, a contribution of our study is that this study investigates the effect of privacy assurance mechanisms on information disclosure in SNS by applying PMT. (2) this paper Introduced protection motivation as a mediator of the effect of privacy concern on self-disclosure which was overlooked by previous researches. (3) Our study introduced use of privacy customization features available on SNSs as a new construct that influences users' perceived effectiveness of privacy assurance mechanisms and their self-efficacy. The results of this study support the findings of previous studies (e.g., Xu et al. 2012) about the influence of self-protection approaches that exist on websites to enable users to protect their information. (4) Findings of our study showed that SNS users' privacy concern is the result a risk calculus process. In this process users perceive privacy concern based on the amount of risk that they perceive from privacy threat and their perceived effectiveness of privacy assurance mechanisms. This finding is an important contribution to previous studies that only focus threat appraisal component (e.g., Mohamed and Ahmad 2012; Youn 2005) of PMT. (5) According to Bansal et al. (2015) most of previous researches studied privacy assurance mechanisms in the context of e-commerce. Hence, another contribution of our study is that this study investigates the effect of privacy assurance mechanisms on information disclosure in SNS by applying PMT. This study also provides several implications for practitioners. First, the findings of our study revealed that privacy assurance statement and privacy customization features on SNSs negatively influence users' privacy concern and consequently affect them to share more personal information. Thus, SNS website designers may apply findings of our study by empowering users to customize their privacy preferences more. Based on our findings, this empowerment motivates them to disclose their information. Moreover, SNSs can provide users with stronger privacy assurance statements as a tool to enhance users' perceived effectiveness of their assurance practices and consequently decrease their privacy concerns.

Limitations and future research

Like any other studies, this study has limitations. Although our conceptual model successfully explained the self-disclosure, there are some other factors that have not been investigated as the antecedents of self-disclosure behavior (Dinev and Hart 2006). This affected our model power (R-square) since we just investigated risks of sharing personal information on the SNS. Future researches may investigate risks and benefits of sharing personal information on SNS. Additionally, using undergraduate students as our sample frame can be another limitation of this study. We believe that student data is a good sample for the study of social networking websites because it reflects a very high proportion of SNS users which are college students (Lenhart et al. 2010). Furthermore, our study lacks cultural diversity. We collected data from students of a university in United States. Different cultures may care about privacy differently (Wu et al. 2012). Thus, future studies may look at the differences in privacy concern among different cultures. Another possible limitation of this study is that personal trait was not studied in the research model. The reason that personal traits were not studied is that threat appraisal in this study is influenced by personal traits of the users (Junglas et al. 2008). In fact, assurance mechanisms have less influence on threat appraisal for those users who perceive more general privacy concern because of their personal traits and consequently these individuals have more privacy concern. Therefore, Future studies may consider the moderating effect of personal traits on the effect of assurance mechanisms on threat appraisal. Finally, this study does not captured the actual self-disclosure behavior of SNS users. As argued by Smith, Dinev and Xu (2011), the actual disclosure behavior of SNS users is a more predict measure than the intention to disclosure. In this study we address Smith et al. argument by measuring the disclosure behavior instead of the intention to disclosure. This study borrowed almost all of the measures from Koohikamali et al. (2015). They applied these items to measure actual behavior.

Conclusion

This study undertook the examination of the collective contributions of privacy assurance mechanisms on privacy concern and self-disclosure and the moderating effect of protection motivation. The PMT was applied as a theoretical lens for the conceptualization of the research model and interpretation of results. The results of the study revealed that privacy assurance mechanisms influence users' privacy concern by affecting their appraisal of a threat and the available coping mechanisms available on a SNS. This study also found that the effect of privacy concern is mediated by SNS users' protection motivation.

References

Altman, I., and Taylor, D.A., 1973. *Social penetration: The development of interpersonal relationships* Holt, Rinehart & Winston, Oxford.

Arcand, M., Nantel, J., Arles-Dufour, M., and Vincent, A. 2007. "The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust," *Online Information Review* (31:5), pp 661-681.

Bansal, G., and Gefen, D. 2010. "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decision Support Systems* (49:2), pp 138-150.

Bansal, G., Zahedi, F., and Gefen, D. (2015). The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems*, 1-21. Retrieved from http://dx.doi.org/10.1057/ejis.2014.41

Bansal, G., Zahedi, F.M., and Gefen, D., 2008. "Efficacy of Privacy Assurance Mechanisms in the Context of Disclosing Health Information Online," AMCIS 2008 Proceedings, p. 178.

Barclay, D., Higgins, C., and Thompson, R. 1995. "The partial least squares (PLS) approach to causal modeling: personal computer adoption and use as an illustration," *Technology studies* (2), pp 285-309.

Boer, H., and Seydel, E.R., 1996 "Protection motivation theory." in: *Predicting Health Behavior*, Open University Press, Buckingham, UK.

Bowman, G.D., and Stern, M. 1995. "Adjustment to occupational stress: The relationship of perceived control to effectiveness of coping strategies," *Journal of Counseling Psychology* (42:3), pp 294-303.

Boyd, D.M., and Ellison, N.B. 2010. "Social network sites: Definition, history, and scholarship," *Engineering Management Review, IEEE* (38:3), pp 16-31.

Brown, M., and Muchira, R. 2004. "Investigating the relationship between Internet privacy concerns and online purchase behavior," *Journal of Electronic Commerce Research* (5:1), pp 62-70.

Buchanan, T., Paine, C., Joinson, A.N., and 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), pp 157-165.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS quarterly* (34:3), pp 523-548.

Campbell, D.T., and Fiske, D.W. 1959. "Convergent and discriminant validation by the multitrait-multimethod matrix," *Psychological bulletin* (56:2), pp 81-105.

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H.R., and Upadhyaya, S.J. 2009. "Internet and online information privacy: An exploratory study of preteens and early teens," *Professional Communication, IEEE Transactions on* (52:2), pp 167-182.

Chen, R. 2013. "Living a private life in public social networks: An exploration of member self-disclosure," *Decision Support Systems* (55:3), pp 661-668.

Chen, R., and Sharma, S.K. 2015. "Learning and self-disclosure behavior on social networking sites: the case of Facebook users," *European Journal of Information Systems* (24:1), pp 93-106.

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

Crossler, R.E., Long, J.H., Loraas, T.M., and Trinkle, B.S. 2014. "Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap," *Journal of Information Systems* (28:1), pp 209-226.

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

Dinev, T., and Hart, P. 2004. "Internet privacy concerns and their antecedents-measurement validity and a regression model," *Behaviour & Information Technology* (23:6), pp 413-422.

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

Dwyer, C., Hiltz, S., and Passerini, K., 2007. "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," AMCIS 2007 Proceedings, p. 339.

Fishbein, M., and Ajzen, I., 1975. *Belief, attitude, intention and behavior: An introduction to theory and research* Addison-Wesley.

Floyd, D.L., Prentice-Dunn, S., and Rogers, R.W. 2000. "A meta-analysis of research on protection motivation theory," *Journal of applied social psychology* (30:2), pp 407-429.

Folkman, S. 1984. "Personal control and stress and coping processes: a theoretical analysis," *Journal of personality and social psychology* (46:4), p 839.

Fornell, C., and Larcker, D.F. 1981. "Evaluating structural equation models with unobservable variables and measurement error," *Journal of marketing research* (18:1), pp 39-50.

Greenberg, M.A., and Stone, A.A. 1992. "Emotional disclosure about traumas and its relation to health: effects of previous disclosure and trauma severity," *Journal of personality and social psychology* (63:1), p 75.

Hann, I.-H., Hui, K.-L., Lee, S.-Y.T., and Png, I.P. 2007. "Overcoming online information privacy concerns: An information-processing theory approach," *Journal of Management Information Systems* (24:2), pp 13-42.

Herath, T., and Rao, H.R. 2009. "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems* (18:2), pp 106-125.

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

Ioinson, A.N., and Paine, C.B., 2007 "Self-disclosure, privacy and the Internet." in: *The Oxford handbook of Internet psychology*, pp. 235-250.

Jiang, Z., Chan, J., Tan, B.C., and Chua, W.S. 2010. "Effects of interactivity on website involvement and purchase intention," *Journal of the Association for Information Systems* (11:1), pp 34-59.

Jiang, Z., Heng, C.S., and Choi, B.C.F. 2013. "Research Note-Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions," *Information Systems Research* (24:3), pp 579-595.

Johnston, A.C., and Warkentin, M. 2010. "Fear appeals and information security behaviors: an empirical study," *MIS quarterly* (34:3), pp 549-566.

Joinson, A.N., Reips, U.-D., Buchanan, T., and Schofield, C.B.P. 2010. "Privacy, trust, and self-disclosure online," *Human–Computer Interaction* (25:1), pp 1-24.

Junglas, I.A., Johnson, N.A., and Spitzmüller, C. 2008. "Personality traits and concern for privacy: an empirical study in the context of location-based services," *European Journal of Information Systems* (17), pp 387-402.

Kim, D.J., Ferrin, D.L., and Rao, H.R. 2008. "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents," *Decision Support Systems* (44:2), pp 544-564.

Kim, D.J., Steinfield, C., and Lai, Y.-J. 2008. "Revisiting the role of web assurance seals in business-to-consumer electronic commerce," *Decision Support Systems* (44:4), pp 1000-1015.

Ko, D.-G., Kirsch, L.J., and King, W.R. 2005. "Antecedents of knowledge transfer from consultants to clients in enterprise system implementations," *MIS quarterly* (29:1), pp 59-85.

Koohikamali, M., Gerhart, N., and Mousavizadeh, M. 2015. "Location Disclosure on LB-SNAs: The Role of Incentives on Sharing Behavior," *Decision Support Systems* (71), pp 78-87.

Korzaan, M.L., and Boswell, K.T. 2008. "The influence of personality traits and information privacy concerns on behavioral intentions," *Journal of Computer Information Systems* (48:4), pp 15-24.

Laufer, R.S., and Wolfe, M. 1977. "Privacy as a concept and a social issue: A multidimensional developmental theory," *Journal of social Issues* (33:3), pp 22-42.

Lee, L.T., 2000 "Privacy, security, and intellectual property." in: *Understanding the Web: Social, political, and economic dimensions of the Internet*, Ames: Iowa State University Press., pp. 135-164.

Lenhart, A., Purcell, K., Smith, A., and Zickuhr, K. 2010."Social Media & Mobile Internet Use among Teens and Young Adults. Millennials." Pew Internet & American Life Project.

Li, Y. 2012. "Theories in online information privacy research: A critical review and an integrated framework," *Decision Support Systems* (54:1), pp 471-481.

Liang, H., Saraf, N., Hu, Q., and Xue, Y. 2007. "Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management," *MIS quarterly* (31:1), pp 59-87.

Liu, C., Marchewka, J.T., and Ku, C. 2004. "American and Taiwanese perceptions concerning privacy, trust, and behavioral intentions in electronic commerce," *Journal of Global Information Management (JGIM)* (12:1), pp 18-40.

Madden, M., Fox, S., Smith, A., and Vitak, J. 2007."Digital footprints: Online identity management and search in the age of transparency." Pew Internet & American Life Project.

Maddux, J.E., and Rogers, R.W. 1983. "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of experimental social psychology* (19:5), pp 469-479.

McKnight, D.H., Choudhury, V., and Kacmar, C. 2002. "Developing and validating trust measures for e-commerce: An integrative typology," *Information systems research* (13:3), pp 334-359.

Meinert, D.B., Peterson, D.K., Criswell, J.R., and Crossland, M.D. 2006. "Privacy policy statements and consumer willingness to provide personal information," *Journal of Electronic Commerce in Organizations (JECO)* (4:1), pp 1-17.

Milne, G.R., and Culnan, M.J. 2004. "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices," *Journal of Interactive Marketing* (18:3), pp 15-29.

Milne, S., Sheeran, P., and Orbell, S. 2000. "Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory," *Journal of Applied Social Psychology* (30:1), pp 106-143.

Miyazaki, A.D., and Fernandez, A. 2000. "Internet privacy and security: An examination of online retailer disclosures," *Journal of Public Policy & Marketing* (19:1), pp 54-61.

Miyazaki, A.D., and Fernandez, A. 2001. "Consumer perceptions of privacy and security risks for online shopping," *Journal of Consumer Affairs* (35:1), pp 27-44.

Mohamed, N., and Ahmad, I.H. 2012. "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia," *Computers in Human Behavior* (28:6), pp 2366-2375.

Norman, P., Boer, H., and Seydel, E.R., 2005 "Protection motivation theory." in: *Predicting Health Behavior*, Open University Press, London.

Nunnally, C., and Bernstein, H., 1978 "Psychometric theory," New York: McGraw-Hill.

Nunnally, J.C., Bernstein, I.H., and Berge, J.M.t., 1967. *Psychometric theory* McGraw-Hill New York.

Ofcom 2014."Ofcom Technology Tracker."

Pavlou, P.A. 2003. "Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model," *International journal of electronic commerce* (7), pp 101-134.

Peterson, D., Meinert, D., Criswell, J., and Crossland, M. 2007. "Consumer trust: privacy policies and third-party seals," *Journal of Small Business and Enterprise Development* (14:4), pp 654-669.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y., and Podsakoff, N.P. 2003. "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *Journal of Applied Psychology* (88:5), pp 879-903.

Posey, C., Lowry, P.B., Roberts, T.L., and Ellis, T.S. 2010. "Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities," *European Journal of Information Systems* (19:2), pp 181-195.

Rainie, L., Kiesler, S., Kang, R., and Madden, M. 2013."Anonymity, Privacy, and Security Online." Pew Internet & American Life Project.

Raman, P., and Pashupati, T.K., 2004. "Online privacy: the impact of self perceived technological competence," American Marketing Association Educators.

Rogers, R.W. 1975. "A protection motivation theory of fear appeals and attitude change," *The journal of psychology* (91:1), pp 93-114.

Rogers, R.W., Cacioppo, J.T., and Petty, R., 1983 "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation." in: *Social psychophysiology: A sourcebook*, pp. 153-177.

Rogers, R.W., and Thistlethwaite, D.L. 1970. "Effects of fear arousal and reassurance on attitude change.," *Journal of Personality and Social Psychology* (15:3), p 227.

Scherer, K.R., 1988 "Criteria for emotion-antecedent appraisal: A review," in: *Cognitive perspectives on emotion and motivation*, Springer, pp. 89-126.

Smith, H.J., Dinev, T., and Xu, H. 2011. "Information privacy research: an interdisciplinary review," *MIS quarterly* (35), pp 989-1016.

Solomon, Z., Mikulincer, M., and Benbenishty, R. 1989. "Locus of control and combat-related post-traumatic stress disorder: The intervening role of battle intensity, threat appraisal and coping," *British Journal of Clinical Psychology* (28:2), pp 131-144.

Squicciarini, A., Paci, F., and Sundareswaran, S., 2010. "PriMa: an effective privacy protection mechanism for social networks," ACM Symposium on Information, Computer and Communications Security, pp. 320-323.

Stutzman, F., Capra, R., and Thompson, J. 2011. "Factors mediating disclosure in social network sites," *Computers in Human Behavior* (27:1), pp 590-598.

Tanner Jr, J.F., Hunt, J.B., and Eppright, D.R. 1991. "The protection motivation model: A normative model of fear appeals," *The Journal of Marketing* (55:3), pp 36-45.

Wakefield, R. 2013. "The influence of user affect in online information disclosure," *The Journal of Strategic Information Systems* (22:2), pp 157-174.

Wang, S., Beatty, S.E., and Foxx, W. 2004. "Signaling the trustworthiness of small online retailers," *Journal of interactive marketing* (18:1), pp 53-69.

Weinstein, N.D. 1993. "Testing four competing theories of health-protective behavior.," *Health psychology* (12:4), pp 324-333.

Westin, A.F. 1967. "Special report: legal safeguards to insure privacy in a computer society," *Communications of the ACM* (10:9), pp 533-537.

Witte, K. 1992. "Putting the fear back into fear appeals: The extended parallel process model," *Communications Monographs* (59:4), pp 329-349.

Wu, K.-W., Huang, S.Y., Yen, D.C., and Popova, I. 2012. "The effect of online privacy policy on consumer privacy concern and trust," *Computers in human behavior* (28:3), pp 889-897.

Wurtele, S.K., and Maddux, J.E. 1987. "Relative contributions of protection motivation theory components in predicting exercise intentions and behavior," *Health Psychology* (6:5), p 453.

Xu, H., Dinev, T., Smith, J., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances.," *Journal of the Association for Information Systems* (12:12), pp 798-824.

Xu, H., Teo, H.-H., Tan, B.C., and Agarwal, R. 2012. "Research Note-Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services," *Information Systems Research* (23:4), pp 1342-1363.

Xu, H., Teo, H.-H., Tan, B.C.Y., and Agarwal, R. 2009. "The role of push-pull technology in privacy calculus: the case of location-based services," *Journal of Management Information Systems* (26:3), pp 135-174.

Youn, S. 2005. "Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach," *Journal of Broadcasting & Electronic Media* (49:1), pp 86-110.

Youn, S. 2009. "Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents," *Journal of Consumer Affairs* (43:3), pp 389-418.

Appendix 1. Measurement Items

Construct	Item	Source
Self-disclosure	SD1: How many times do you share information on Social Networking Site (SNS) each week?	Koohikamali et al. (2015)
	SD2: I share my information every time I use this SNS.	
	SD3: I rarely disclose my information when I use this SNS.	
	SD4: I am very likely to disclose my information on SNS.	New item
Protection motivation	PM1: I plan to protect my information against possible threats.	Johnston and Warkentin (2010)
	PM2: I predict I will protect my information on this SNS.	
	PM3: I intend to protect my information when I use this SNS.	
	PM4: I am sure that I will protect my information on this SNS.	Herath and Rao (2009)
	PM5: It is possible that I do something to protect my information.	
Privacy concern	PC1: I am concerned that this SNS is collecting too much information from me.	Kim, Ferrin and Rao (2008)
	PC2: I am concerned that this SNS will use my information for other purposes.	
	PC3: I am concerned that this SNS will share my information with other parties.	
	PC4: I am concerned that this SNS does not protect privacy of my information.	
Threat susceptibility	TSUS1: My information is at risk for being released to unauthorized people.	Johnston and Warkentin (2010)
	TSUS2: It is likely that my information will become available to unauthorized people.	
	TSUS3: It is possible that my Information will become available to unauthorized people.	
	TSUS4: It is likely that others get access to my information without my permission.	New items
	TSUS5: It is probable that others get access to my information without my permission.	
Threat severity	TSEV1: If my information released to unauthorized people, it would be very bad for me.	Johnston and Warkentin (2010)
	TSEV2: If my information released to unauthorized people, it would be a serious danger.	
	TSEV3: If my information released to unauthorized people, it would be significant danger.	
	TSEV4: If my information be available to unauthorized users, it would be risky.	New item
Assurance mechanisms efficacy	AME1: When this SNS uses privacy assurance mechanisms, my information are more likely to be protected.	Johnston and Warkentin (2010)
	AME2: I believe that the privacy assurance mechanisms that this SNS uses help me to keep my information private.	New items
	AME3: I think the privacy assurance mechanisms that this SNS uses are effective.	

Self-efficacy	SE1: It is easy for me to use privacy assurance mechanisms on this SNS.	Johnston and Warkentin (2010)
	SE2: It is convenient for me to use privacy assurance mechanisms.	
	SE3: I am able to use privacy assurance mechanisms without much effort.	Compeau and Higgins (1995)
Privacy assurance statement	PAS1: I feel confident that this SNS's privacy assurance statement reflects their commitments to protect my information.	Xu, Dinev, Smith and Hart (2011)
	PAS2: With this SNS's privacy assurance statement, I believe that my information will be safe.	
	PAS3: I believe that this SNS's privacy assurance statement is an effective way to demonstrate their commitments to privacy.	
Privacy customization	PCUST1: I customize my SNS privacy settings when I share my information.	New items
	PCUST2: I prefer to customize privacy settings before I share my information.	
	PCUST3: I usually use privacy customization feature.	
	PCUST4: I use privacy customization on this SNS to protect my information.	

Appendix 2. Factor Loadings

Item	Mean	S.D.	SD	PM	PC	TSUS	TSEV	AME	SE	PAS	PCUS
SD1	2.46	1.34	**0.737**	-0.002	0.031	-0.124	-0.021	0.057	-0.043	-0.002	0.010
SD2	2.72	1.72	**0.728**	-0.092	0.005	-0.053	-0.045	-0.048	0.140	0.339	0.031
SD3	3.55	1.79	**0.740**	0.090	0.027	0.016	0.048	-0.004	-0.036	0.048	-0.008
SD4	3.35	1.61	**0.744**	-0.139	-0.030	0.077	-0.036	0.094	0.158	-0.011	0.016
PM1	5.60	1.21	-0.136	**0.787**	0.222	0.085	0.142	-0.029	0.070	-0.137	0.046
PM2	5.44	1.27	-0.038	**0.813**	0.211	-0.026	0.185	0.026	0.079	-0.038	0.090
PM3	5.73	1.16	-0.097	**0.857**	0.155	0.075	0.068	0.016	0.036	-0.016	0.225
PM4	5.31	1.38	-0.090	**0.827**	0.021	-0.084	0.049	0.083	-0.009	0.053	0.071
PM5	5.61	1.18	-0.022	**0.829**	0.091	0.087	-0.057	0.078	0.047	-0.043	0.184
PC1	4.73	1.56	0.041	0.147	**0.861**	0.176	0.043	-0.022	-0.003	-0.066	0.042
PC2	4.82	1.60	-0.024	0.167	**0.916**	0.186	0.124	-0.084	-0.002	-0.033	0.038
PC3	4.94	1.52	-0.075	0.187	**0.884**	0.224	0.115	-0.084	0.016	-0.040	0.072
PC4	4.64	1.55	0.030	0.185	**0.808**	0.271	0.154	-0.116	-0.030	-0.109	0.021
TSUS1	4.67	1.61	-0.039	0.045	0.225	**0.762**	0.157	-0.002	-0.025	-0.172	-0.005
TSUS2	4.44	1.64	-0.021	-0.001	0.169	**0.843**	0.171	-0.133	-0.030	-0.142	-0.052
TSUS3	4.88	1.49	-0.060	0.063	0.164	**0.893**	0.043	-0.027	-0.050	-0.124	-0.030
TSUS4	4.58	1.63	-0.025	0.024	0.142	**0.897**	0.087	-0.154	-0.041	-0.072	-0.075
TSUS5	4.66	1.61	-0.010	-0.016	0.134	**0.918**	0.052	-0.100	-0.031	-0.023	-0.001
TSEV1	4.64	1.71	-0.037	0.179	0.129	0.172	**0.833**	-0.105	0.032	-0.041	-0.032
TSEV2	4.32	1.80	-0.042	0.069	0.083	0.054	**0.956**	-0.007	-0.022	0.012	0.002
TSEV3	4.24	1.81	-0.070	0.039	0.088	0.071	**0.947**	0.005	0.017	-0.002	0.027
TSEV4	4.75	1.69	-0.018	0.057	0.085	0.163	**0.876**	0.086	-0.005	0.012	0.079
AME1	4.81	1.32	-0.007	0.064	-0.041	-0.087	-0.056	**0.847**	0.225	0.242	0.083
AME2	4.74	1.42	0.069	0.029	-0.149	-0.176	0.022	**0.839**	0.136	0.321	0.081
AME3	4.60	1.44	0.113	0.136	-0.137	-0.181	0.029	**0.795**	0.172	0.333	0.087
SE1	5.01	1.38	0.111	0.109	-0.005	-0.030	-0.013	0.139	**0.865**	0.091	0.291
SE2	4.96	1.45	0.081	0.058	-0.016	-0.056	0.007	0.148	**0.847**	0.137	0.366
SE3	4.93	1.40	0.138	0.052	0.006	-0.096	0.035	0.251	**0.819**	0.138	0.271
PAS1	3.87	1.70	0.040	-0.018	-0.086	-0.175	-0.041	0.243	0.058	**0.890**	0.031
PAS2	3.64	1.72	0.056	-0.131	-0.115	-0.139	-0.002	0.298	0.121	**0.847**	-0.014
PAS3	4.11	1.71	0.054	-0.022	-0.030	-0.171	0.030	0.235	0.134	**0.819**	0.012
PCUS1	5.39	1.53	0.008	0.101	0.018	-0.005	-0.050	0.053	0.227	0.091	**0.798**
PCUS2	5.70	1.41	-0.083	0.190	0.119	-0.043	0.010	0.095	0.162	-0.057	**0.816**
PCUS3	5.61	1.53	0.120	0.115	-0.020	-0.044	0.108	-0.006	0.144	-0.018	**0.857**
PCUS4	5.74	1.39	0.011	0.170	0.051	-0.051	0.014	0.071	0.211	0.015	**0.872**

Appendix 3. Common Method Bias Analysis

Construct	Indicator	Substantive Factor Loading (R_1)	R_1^2	Method Factor Loading (R_2)	R_2^2
Self-disclosure	SD1	0.709***	0.503	-0.013 NS	0.000
	SD2	0.754***	0.569	-0.099 NS	0.010
	SD3	0.756***	0.572	-0.052 NS	0.003
	SD4	0.790***	0.624	0.039 NS	0.002
Protection motivation	PM1	0.785***	0.616	0.172 NS	0.030
	PM2	0.851***	0.724	0.024 NS	0.001
	PM3	0.904***	0.817	0.018 NS	0.000
	PM4	0.868***	0.753	-0.166 NS	0.028
	PM5	0.867***	0.752	-0.058 NS	0.003
Privacy concern	PC1	0.954***	0.910	-0.096 NS	0.009
	PC2	0.992***	0.984	-0.043 NS	0.002
	PC3	0.942***	0.887	0.006 NS	0.000
	PC4	0.806***	0.650	0.134 NS	0.018
Threat susceptibility	TSUS1	0.735***	0.540	0.112 NS	0.013
	TSUS2	0.844***	0.712	0.075 NS	0.006
	TSUS3	0.928***	0.861	-0.018 NS	0.000
	TSUS4	0.944***	0.891	-0.017 NS	0.000
	TSUS5	1.029***	1.059	-0.138 NS	0.019
Threat severity	TSEV1	0.810***	0.656	0.144 NS	0.021
	TSEV2	0.985***	0.970	-0.054 NS	0.003
	TSEV3	0.979***	0.958	-0.053 NS	0.003
	TSEV4	0.908***	0.824	-0.025 NS	0.001
Assurance mechanisms efficacy	AME1	0.955***	0.912	0.079 NS	0.006
	AME2	0.916***	0.839	-0.051 NS	0.003
	AME3	0.917***	0.841	-0.025 NS	0.001
Self-efficacy	SE1	0.951***	0.904	0.045 NS	0.002
	SE2	0.952***	0.906	0.003 NS	0.000
	SE3	0.911***	0.830	-0.048 NS	0.002
Privacy assurance statement	PAS1	0.942***	0.887	-0.002 NS	0.000
	PAS2	0.909***	0.826	-0.045 NS	0.002
	PAS3	0.924***	0.854	0.049 NS	0.002
Privacy customization	PCUS1	0.832***	0.692	-0.063 NS	0.004
	PCUS2	0.870***	0.757	0.071 NS	0.005
	PCUS3	0.872***	0.760	0.003 NS	0.000
	PCUS4	0.917***	0.841	-0.011 NS	0.000
Note: *** $p < 0.001$ (two-tailed significance)					