Social Networking Information Disclosure and Continuance Intention: A Disconnect

D. Harrison McKnight
Michigan State University
Eli Broad College of Business
Dept. of Accounting and Information Systems
East Lansing MI 48824
mcknight@bus.msu.edu
517-432-2929

Nancy Lankton
Marshall University
Lewis College of Business
Division of Accountancy and Legal Environment
Huntington, WV 25755
lankton@marshall.edu
304-696-2656

John Tripp
Michigan State University
Eli Broad College of Business
Dept. of Accounting and Information Systems
East Lansing MI 48824
tripp@bus.msu.edu
517-353-8754

November 2010

Acknowledgements:
We express appreciation to Fred Roddamer for his help in facilitating the data collection for this paper. We acknowledge the Department of Accounting and Information Systems at Michigan State University for research support during the drafting of this paper. In addition, we appreciate the comments and suggestions of several anonymous reviewers from the Hawaii International Conference on System Science.

Social Networking Information Disclosure and Continuance Intention: A Disconnect

Abstract

This paper tests a privacy calculus model for Facebook users. Privacy calculus means that individuals weigh a complex set of factors—including both costs and benefits—to decide whether to disclose personal information. Because information disclosure is closely related to use for many information technologies (IT), our privacy calculus model proposes that costs and benefits of user privacy will simultaneously influence users' information disclosure and usage continuance intention. Based on past research, our model includes as 'costs' privacy concern and information sensitivity, while it includes as 'benefits' perceived usefulness, enjoyment, and trust. In a sample of business college students' use of a social networking website, we find that the privacy calculus model is not well-supported. The benefits do not positively affect information disclosure; only the two cost factors, privacy concern and information sensitivity, predict it. Thus, our findings do not support the privacy calculus model theory that users will weigh costs against benefits in determining whether to disclose information on a social networking website. We also find two benefit factors, usefulness and enjoyment, are the sole predictors of Facebook usage continuance intention. That is, information sensitivity, trust, and privacy concern do not predict continuance. Overall, the study finds that one set of factors influence information disclosure while a separate set of factors influence continuance intention. That is, the predictors of continuance intention are completely different from the predictors of information disclosure. This means, surprisingly, that these users display a clear disconnect between their reasons to disclose information on Facebook and their reasons to continue using Facebook.

Social Networking Information Disclosure and Continuance Intention:

A Disconnect

Introduction

Privacy or the state of limited access to one's information, while considered important for many years (Culnan 1993; Smith et al. 1996), has become even more critical due to the advent of the Internet and the increasing ease of exchanging information online. When interacting online, individuals are often faced with the decision of whether to disclose their personal information. Privacy research finds that people perform a privacy calculus by weighing both the costs and benefits before making the decision to disclose information (Culnan and Armstrong 1999; Dinev and Hart 2006). On the one hand, online users have serious concerns about how their information might be used or abused. On the other hand, users know they need to disclose certain information in order to receive benefits such as procuring online goods and services. Privacy calculus takes place when both costs and benefits are considered; otherwise, the decision is too simple to be called a "calculus."

In the past, participation in a data-sharing relationship was contingent on the other party keeping one's information private. For example, one would typically share personal information like birth dates and social security numbers with an online bank when sharing this personal information provided more perceived benefits than costs. In this case, the "cost" of information sharing was the potential risk of the bank not keeping one's personal information secure and private, while the "benefit" was the ability to transact online.

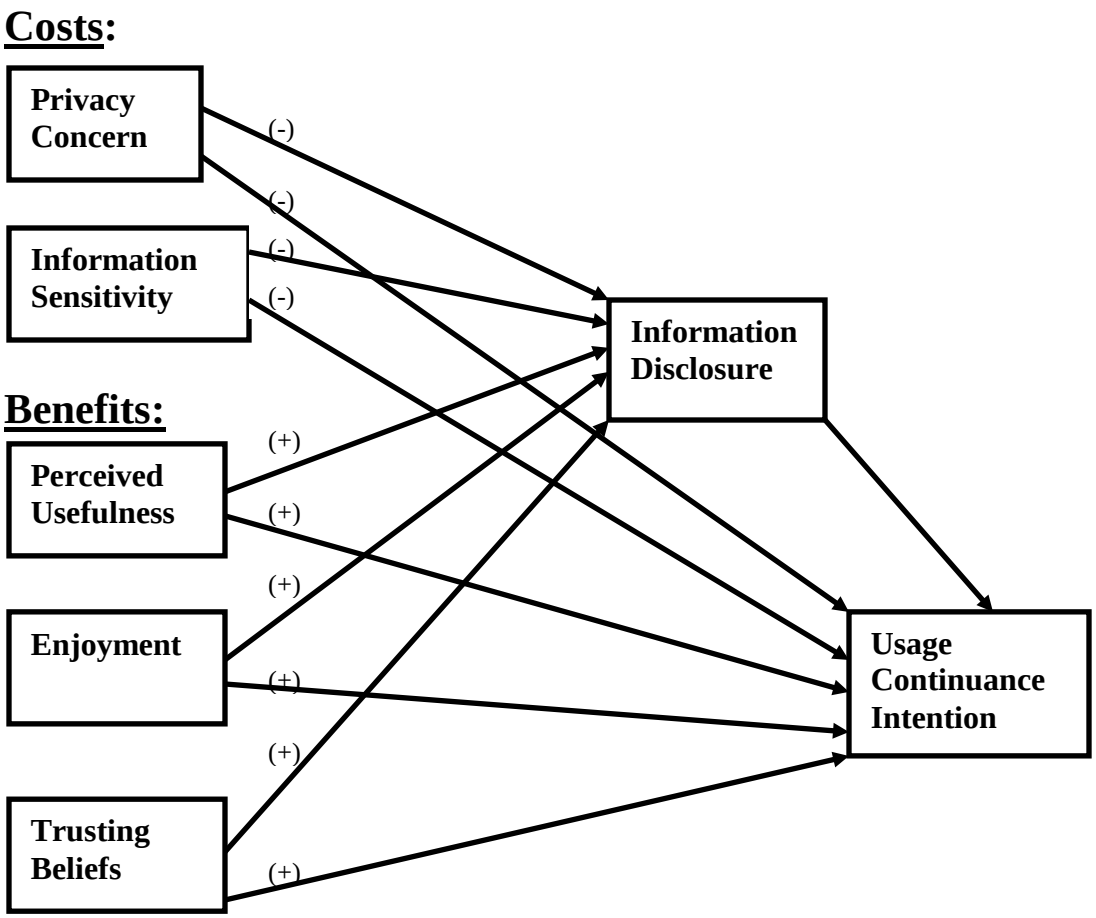
The dynamics of today's data-sharing relationships are somewhat different. For example, online social networking privacy settings let people control who has access to what information. For example, a Facebook user may decide to allow friends access to his/her birth date and to not

allow friends-of-friends access to this same information. Giving up certain aspects of privacy by not restricting access to their personal information allows one to interact more openly with friends and others online. In these online environments, individuals themselves play an active role in determining what information ends up being disclosed to third parties (i.e., the website vendor, friends, and other users). Information disclosure in this sense means the extent to which one allows access to aspects of one's personal information, rather than the more traditional meaning of whether or not one shares one's personal information. Also, unlike traditional e-commerce websites, the level of information disclosure does not necessarily prohibit social network use. It simply specifies what types and how much information are available to specific others.

This paper's first objective is to understand if the privacy calculus model predicts information disclosure in online social networking. Because the social networking (SN) site largely exists for connecting with and sharing information with friends (Hart et al. 2008), users may weigh the costs and benefits of information disclosure. We predict that the benefits of disclosing information on a social networking website are primarily the usefulness and enjoyment of being able to communicate with and share things with friends, family, and other acquaintances. The cost is embodied in both the concern for privacy and the sensitivity of the information that may become available to the wrong persons. Therefore, we propose that users' information disclosure will result from a privacy calculus decision influenced by a combination of privacy concern, information sensitivity, trusting beliefs, perceived usefulness, and enjoyment (see Figure 1 and Table 1 definitions). Our model treats information disclosure as a self-reported behavior. Early privacy calculus research (Dinev and Hart 2006) tended to examine privacy disclosure intention rather than information disclosure behavior, as we do. (For some recent

exceptions see Krasnova et al. 2009; and Krasnova and Veltri 2010.). In offline settings, studies find intentions to disclose information do not always result in actual disclosure behaviors, which suggests the need to study privacy behaviors (Norberg et al. 2007). This study contributes by being among the first to look at how well the privacy calculus model applies to behavioral information disclosure in social networking.

Figure 1. Research Model



The second objective of this paper is to examine whether privacy calculus is involved in social networking usage continuance intention decisions. We feel that it is likely that users weigh

both the costs related to usage (such as privacy concerns) and the benefits of usage (such as enjoyment) when deciding to continue using the website. But this is a question that needs to be answered empirically. While privacy research has shown that several of the costs/benefits used in calculus decisions significantly affect continuance intentions (e.g., Dinev and Hart 2005/6; Krasnova et al. 2009), it is not clear whether the resulting disclosure behavior makes one more likely to continue using the target technology. Therefore, our study contributes by examining simultaneously how both disclosure behavior and continued use intention are affected by privacy calculus factors, and whether disclosure behavior affects continued use intention. Prior research has examined privacy calculus for either disclosure or usage but not both. This allows us to see whether privacy calculus works and which costs/benefits are most influential to both information disclosure and continuance intentions, since both are important concepts to predict.

Our study also contributes to practice as privacy and continued usage are important issues to social networking vendors. For example, officials from Facebook, one of the most popular social networking websites, say that privacy issues are complex and somewhat confusing to users (Wortham 2010b). In fact, Facebook has implemented several software changes that the news media has reported as threatening to user privacy (Wortham 2010a). Opinions can change over time and the past and present popularity of social networking websites may or may not be permanent. It is possible that privacy issues, if users consider them serious enough, could threaten the website's continued use. Awad and Krishnan suggested that "if managers are not careful, their firms may be the victims of consumer backlash for overstepping the bounds of expected information practices" (2006: 14). If outcry over privacy issues reached a critical mass, perhaps a large exodus from social networking websites would result.

Overall, this paper contributes to the literature by examining: 1) how privacy calculus applies to reported information disclosure behavior instead of the more common intention to disclose; 2) how online social networking privacy calculus issues differ from privacy calculus issues in e-commerce or other settings; and 3) how privacy calculus predictors apply to both information disclosure and usage continuance intention simultaneously.

Table 1: Constructs and Construct Definitions

Construct Name	**Construct Definition**
Information Disclosure (ID)	The extent to which one provides access to one's personal information, using social network provider privacy control settings to allow access.
Privacy Concern	Concerns about opportunistic behavior related to one's personal information (Dinev and Hart 2006)
Information Sensitivity	Beliefs that certain information in one's profile might result in a loss of privacy if revealed (disclosed) to others who might be untrustworthy and/or have indeterminable or hostile intentions. (adapted from http://en.wikipedia.org/wiki/Information_sensitivity)
Trusting Beliefs	Beliefs that the social networking website has certain trustworthy attributes.
Trusting Beliefs: Reliability	Belief that the social networking website will continually operate properly, or will operate in a consistent, flawless manner.
Trusting Beliefs: Functionality	Belief that the social networking website will have the functions or features needed to accomplish one's task
Trusting Beliefs: Helpfulness	Belief that the social networking website will provide adequate and responsive help.
Perceived Usefulness	Belief that using the social networking website enhances one's personal or performance outcomes (Davis et al. 1989; Venkatesh et al. 2003)
Enjoyment	Affective cognition that one's social networking website use behavior is enjoyable in its own right apart from any anticipated personal gain or performance-related outcomes.
Usage Continuance Intention	Plans to utilize the social networking website in the future.

Theoretical Development

The overarching theory this study employs is the privacy calculus model. Privacy calculus has to do with the cost/benefit tradeoffs people consider when deciding whether or not to provide information (Culnan and Armstrong 1999). Researchers have found that individuals will exchange privacy for some economic or social benefit subject to a "privacy calculus" (e.g., Laufer and Wolfe 1977). The privacy calculus model examines contrary beliefs as opposed to other typical behavioral models such as the Theory of Reasoned Action that examine the relative strength of non-contrary beliefs (Dinev and Hart 2006). It assumes that individuals can have strong beliefs about the costs and benefits of information disclosure simultaneously (Dinev and Hart 2006). Culnan and Armstrong (1999) proposed that firms can offset privacy concern by telling the customer their fair information practices (which builds trust). The customer then decides to disclose transactional information based on the benefits versus risks of disclosure.

Several IS researchers have recently used the privacy calculus model to predict information disclosure, use of personalization services, e-commerce use, and privacy protection behaviors (see Table 2). Note from column three that researchers typically test privacy calculus using one dependent variable, not two or more. The most often-used dependent variables are: 1) information disclosure and 2) use/transacting. Hence, these are the two we employ. For example, Dinev and Hart (2006) extended the privacy calculus model to the Internet environment to predict one's willingness to disclose enough information to transact online. They found that users decided to disclose based on the contrasting forces of certain costs (Internet privacy concern and privacy risk) and benefits (Internet trust and personal interest). This suggests that users decide to disclose information using a privacy calculus that involves tradeoffs among costs and benefits.

We test privacy calculus in the social networking domain. In social networking, we predict users will employ a privacy calculus when deciding how much to enable others access to their personal information. Table 2 shows the cost and benefit factors used in prior IS calculus studies. In general, any set of factors that reflects both the costs and benefits of information

Table 2 Selected Recent Information Systems Privacy Calculus Model Empirical Studies

Study	**Context**	**Behavior / Cognition (dependent variable)**	**Costs (risk beliefs)**	**Benefits (confidence and enticement beliefs)**
Awad and Krishnan 2006	e-commerce	Willingness to be profiled online for personalized services/advertising	Privacy concern, Previous online privacy invasion, importance of privacy policies	Importance of information transparency
Chellappa and Sin 2005	e-commerce	Likelihood of using personalization services	Privacy concern	Value for personalization, trust building factors
Dinev and Hart 2006	e-commerce	Willingness to provide personal information to transact on the Internet	Internet privacy concerns, Perceived Internet privacy risk	Internet trust, Personal Internet interest
Dinev et al. 2006	e-commerce	e-commerce use	Privacy concern, Perceived risk	Institutional trust
Dinev et al. 2008	Internet and government surveillance	Willingness to provide personal information to transact on the Internet	Internet privacy concerns, Government intrusion concerns	Perceived need for government surveillance
Krasnova et al. 2009	Online social networking	Self-disclosure amount	Privacy concern	Perceived enjoyment
Krasnova and Veltri 2010	Online social networking	Self-disclosure amount	Privacy concern, Privacy violation likelihood, Perceived damage	Enjoyment, Self-preservation, Relationship Maintenance
Son and Kim 2008	Internet	Privacy protective responses (e.g., refusal, removal, negative word-of-mouth, complaints)	Privacy concern	Perceived justice, Societal benefits from complaining
Yang and Wang, 2009	Online purchasing and job hunting	Willingness to reveal the requested information	Privacy concern, information sensitivity	Compensation
Zeng et al. 2009	Virtual communities	Intention to share personal information	Privacy concern	Attitude toward the social exchange, Trust

disclosure would provide a privacy calculus. The privacy calculus concept would be supported if one finds that both cost and benefit factors serve as significant predictors of information disclosure. Based on prior research on privacy and social networking (see hypothesis justification), we employ privacy concern and information sensitivity as costs of information disclosure, and technology usefulness, enjoyment, and trusting beliefs as benefits. Taken together, we propose a privacy calculus for social networking technology, as described below.

Costs: Privacy Concern and Information Sensitivity

Privacy concern can decrease one's information disclosure activity (Dinev and Hart 2006; Krasnova et al. 2009; Yang and Wang 2009). Therefore, the higher an individual's privacy concern, the less likely the individual will engage in information disclosure. For example, a person who thinks information will be misused on Facebook will be less likely to provide access to this information. In an experimental e-commerce study, greater privacy concern was found to increase intent to protect information (Yang and Wang 2009) and thus disclose less information.

H1: Privacy concern will negatively influence Information Disclosure.

Sensitive information is information in one's profile that might result in negative consequences if revealed to untrustworthy or hostile individuals. In prior research one's beliefs that information is sensitive (i.e., their information sensitivity) has been found to negatively affect information disclosure (Yang and Wang 2009). We predict that users will be less likely to provide access to information they believe is sensitive because the adverse consequences of misuse will be greater. Thus, disclosure will be lower for higher information sensitivity beliefs.

H2: Information sensitivity will negatively influence Information Disclosure.

Benefits: Trusting Beliefs, Usefulness and Enjoyment

Interpersonal trust or trust between two people is considered a prerequisite to sharing information with others (Zand 1972). Today many transactions requiring information disclosure are performed online, making trust in the website an important consideration for disclosure. If one believes a website to be reliable, functional, and helpful, one will be more likely to disclose information on the site. Previous research finds that trust in the Internet is an important predictor of disclosure intentions for e-commerce (Dinev and Hart 2006). Likewise we predict that the more one trusts the Facebook website, the more one will feel open to providing access to personal information on that website.

H3: Trusting beliefs will positively influence Information Disclosure.

Sharing information with other users makes a website such as Facebook more productive and effective in social networking activities. While researchers have not yet examined usefulness in terms of this privacy calculus decision, it can be an important factor for exchanging information with friends online. Restricting access to personal information could actually hamper this usefulness. The more useful a social networking site is, the more it will offset risks and thus encouraging disclosure. Hence, we predict that usefulness will increase information disclosure.

H4: Perceived usefulness will positively influence Information Disclosure.

Enjoyment means the positive, hedonic feeling one has when doing something, apart from any anticipated performance outcomes (van der Heijden 2004). Enjoyment is a major reason people use social networking websites (Hart et al. 2008). Enjoyment has been found to increase self-disclosure in social networking (Krasnova et al. 2009). Therefore, enjoyment may

be thought of as a benefit associated with disclosing information. For example, users may find it pleasurable to know that others can see their activities and interests. The more the Facebook user experiences enjoyment, the more the user will participate in information disclosure activity.

H5: Enjoyment will positively influence Information Disclosure.

We will consider privacy calculus supported to the extent that a combination of both positive and negative predictors of the dependent variables are significant. Next, based on prior research, we justify Hypotheses 6-10 to reflect how these same factors represent a privacy calculus for usage continuance intentions.

Usage Continuance Intention Predictors

Dinev and Hart (2005/2006) find that privacy concerns directly influence the intention to transact online. Privacy concern can weigh against the usefulness or enjoyment of a website because it causes one to worry about the results of using the site. For example, worry that co-workers or future employers might see things one posts online might offset perceptions of the site's usefulness. We propose that the higher the privacy concern, the less one will intend to continue using the website due to fears about information misuse.

H6: Privacy concern will negatively influence continuance intention.

Individuals who believe their information is more sensitive are less likely to continue using a website where the main purpose is to share information. That is, they may even feel so uncomfortable sharing any information that they discontinue use of the website. Information sensitivity will also likely cause some users to limit the extent to which they use a website.

H7: Information sensitivity will negatively influence continuance intention.

Trust in a website has been found to encourage website use (Gefen et al. 2003). One who trusts the website will feel the site will be more desirable and less risky to use. The more one trusts the website, the more one is likely to continue using it, as found in numerous e-commerce studies (e.g., Pavlou and Gefen 2004).

H8: Trusting beliefs will positively influence continuance intention.

Usefulness has a long history of influencing one's intentions to use a technology (Davis et al. 1989; Venkatesh et al. 2003). Social networking users may want to continue using the website because it provides "social usefulness" (Stafford et al. 2004). One study (Sledgianowski and Kulviwat 2009) finds that usefulness influences Facebook, Friendster, and MySpace user intentions to continue using the websites.

H9: Perceived usefulness will positively influence continuance intention.

Because individuals will want to continue behaviors that are pleasant or fun, enjoyment will increase continuance intention. Enjoyment has been found to influence intentions in other online contexts including instant messaging (Li et al. 2005), shopping (Koufaris 2002), and gaming (Wu and Liu 2007).

H10: Enjoyment will positively influence continuance intention.

While we test the relationship between information disclosure and continuance intention below, we hypothesize no relationship because of the approximately equal draw of two opposing

arguments. On the one hand, the more one discloses personal information, the more likely one will have a positive experience and thus the more likely one is to continue using the site. On the other hand, users that restrict access to their information may feel less worried about adverse outcomes, and therefore may be more likely to continue using the site.

Methodology

This study used a questionnaire approach. We selected a course required for all business students in a large Midwestern U.S. university. To encourage honesty of response, we told the students we would keep individual responses confidential. To avoid hypothesis guessing, subjects were not told the theory base of the study or its objectives. We told them we were interested in knowing their opinions as social network users. 481 responses were received out of 540 enrollees (89%). We removed the cases of those who did not use Facebook and those who did not complete the questionnaire, resulting in a sample size of 391. To test for non-response bias, we did a means difference t-test between cases included versus cases not included for age, gender, and the three disposition to trust technology items. We found no significant mean differences between included and not-included groups.

Table 3 shows the demographics of the sample. Although Facebook is now used by many age groups, young adults still comprise a core group of intensive Facebook users (Hart et al. 2008). Young adults are also just as concerned about privacy issues as older groups (Hoofnagle et al. 2010). Our respondents had used Facebook for an average of 3.5 years and reported using it 3-4 times per day on average, both of which mean they are very familiar with Facebook.

The questionnaire is shown in Appendix A. We adapted most scales from previous research: privacy concern (Dinev and Hart 2006), trust (Thatcher et al. 2007), usefulness

(Venkatesh and Morris 2000), and enjoyment (Venkatesh 2000), and usage continuance intentions (Venkatesh et al. 2003). Items for information disclosure were created by the authors and reflect one's exercising control over different types of personal information. Controlling one's information is the opposite of disclosing it, making these reverse-scored items. Items for information sensitivity followed the categories of information users could control using their Facebook privacy tools at the time of the questionnaire (December, 2009). We depicted trusting beliefs as a second-order concept with three first-order factors: reliability belief, functionality belief, and helpfulness belief. These beliefs are geared toward trust in a technology rather than in a person. Facebook is not a person. It is a website system. Thus it seemed more natural to ask respondents questions that relate to the website nature of Facebook rather than assuming respondents think of Facebook as a person or organization (Thatcher et al. 2007). We depict these beliefs as first-order factors making up an overall technology trusting beliefs second-order construct based on prior trust research (McKinney et al. 2002; Wang and Benbasat 2005). We expect the dimensions to reflect jointly the overall technology trust concept and may be influenced by it. We also expect the dimensions to co-vary with and even influence each other (Jarvis et al. 2003; McKnight et al. 2002). Therefore, we model the first-order dimensions as reflective (not formative) constructs of the second-order factor.

For all items, a pilot study using the same course in a prior semester was used to refine the scales. We found acceptable reliability (e.g., Cronbach's alpha > 0.70) and construct validity in the pilot (using the methods described below) and therefore used the same items in this study. Next we used item culling on the main test sample to eliminate items that did not load properly (Churchill 1979). To do this, we performed an SPSS exploratory factor analysis in which we entered items for all ten multi-item constructs. We specified ten factors and a direct oblimin

rotation, since we expected many of the variables to be correlated. It was decided a priori to drop items that did not load at 0.50 or higher on their intended variable or that cross-loaded on another variable at more than 0.30 (Yoo and Alavi 2001). Using these criteria, only one item was

Table 3: Descriptive Statistics

Variable	Mean	Std. Dev.	Cronbach's α	AVE
Information Sensitivity	4.15	1.31	0.89	.64
Information disclosure	3.13	1.33	0.86	.64
Privacy Concern	4.71	1.32	0.91	.79
Trusting Belief-Reliability	4.94	1.25	0.88	.81
Trusting Belief-Functionality	5.68	1.09	0.89	.83
Trusting Belief-Helpfulness	4.35	1.12	0.92	.86
Use Continuance Intention	5.89	1.19	0.97	.95
Perceived Usefulness	5.30	1.06	0.96	.88
Enjoyment	5.64	1.10	0.95	.90
Control: Disposition to Trust	4.68	1.31	0.91	.85
Control: Number of Facebook Friends at U.	4.35	1.63	n/a	n/a
Control: Facebook Experience (duration X frequency)	23.3	8.63	n/a	n/a
Control: Gender (0=M; 1=F)	0.41	0.49	n/a	n/a
Control: Age	21.0	1.23	n/a	n/a
Education (1=Soph; 2=Junr.; 3=Senr.; 4=Grad.)	2.46	0.52	n/a	n/a

Table 4: Construct Intercorrelations

Construct	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1. Info. Sens	***.80***													
2. Info. Disclos.	-.28	***.80***			*Note: The square root of the AVE is on the diagonal*									
3. Privacy Con.	.18	-.22	***.89***											
4. Tr. Bel-Rel.	.00	-.07	-.06	***.90***										
5. Tr. Bel-Fun.	-.06	-.15	.02	.58	**.91**									
6. Tr. Bel-Hlp.	.07	-.06	.01	.36	.27	***.93***								
7. Use Intentn.	-.09	-.08	-.06	.30	.42	.07	***.97***							
8. Percd. Usefls.	-.02	-.06	-.03	.34	.36	.19	.47	***.94***						
9. Enjoyment	-.04	-.11	.00	.38	.49	.24	.55	.53	***.95***					
10. Dsp to Trust	-.14	.14	-.10	.19	.16	.14	.22	.15	.15	***.92***				
11. # of Frds.	-.03	-.21	.10	.14	.18	.03	.18	.19	.22	.08	***n/a***			
12. Experience	-.02	-.27	.04	.22	.32	.07	.41	.24	.39	.10	.36	***n/a***		
13. Gender	.13	-.20	.07	-.04	.01	.03	.06	.11	.11	-.05	.10	.07	***n/a***	
14. Age	-.03	.08	.05	-.04	-.10	.03	-.15	-.07	-.09	.02	-.23	-.15	***-.07***	***n/a***

dropped, information sensitivity item 7, which loaded at 0.43 and cross- loaded with trusting

belief—functionality at 0.31. All other items passed the test, with the lowest loading at 0.66 and the highest cross-loading 0.20 (both for information sensitivity item 2). We also examined the Cronbach's alphas, finding the lowest one to be 0.86, which is satisfactory.

Convergent validity was next examined further using Fornell and Larcker's (1981) standard of 0.70 or above for the average variance extracted (AVE). Table 3 shows that each variable exceeded this hurdle. Finding acceptable convergent validity, we examined discriminant validity by comparing the variable inter-correlations with the square roots of the AVEs (Table 4). Each correlation should be lower than the square roots of the AVEs of the two variables correlated (Fornell and Larcker 1981). Table 4 shows this standard is met, supporting discriminant validity.

We also assessed common method variance by using nested measurement models in EQS as outlined by Widaman (1985). We found that adding a method factor only minimally improved model fit (non-normed fit index increased .009) (Bentler and Bonnet 1980). In addition, the original factor loadings are significant even with the method effects taken out. Thus we conclude common method variance was not a major problem. While there are some criticisms to using the method factor approach to test for common method variance, a method without problems has not yet been identified (Sharma et al. 2009). Also, we took several steps to prevent common method variance in the survey. The first preventive step was to mix several open-ended questions (e.g., one about risk to college students of using Facebook) among the quantitative questions to give respondents an occasional mental break. The second step was to use different scale headers for different types of questions, changing between the Strongly Agree-Strongly Disagree scale, the Not True at All-Absolutely True scale, and Not at All-A Great Deal scale (see Appendix). The

third step we took was to group items together by construct so as not disrupt the logical flow of the instrument (Podsakoff et al. 2003).

To test the validity of the second-order trusting belief factor we examined the correlations among the first-order constructs (reliability, functionality, and helpfulness) and the first-order construct loadings on the second-order construct. We find that the first-order factors are significantly correlated ($p<.01$) and of medium to high magnitude ($r = .27$ to $.58$). We find their loadings on the second-order factor range from .63 to .86 and are significant at $p<.01$. Thus the second-order construct appears valid. These findings also support treating the first-order constructs as reflective rather than formative. The factors would not be significantly and strongly correlated if they were formative.

In addition to the Figure 1 model, we used five control variables in predicting both information disclosure and continuance intention. We controlled for age, gender, and experience, since these have been found to cause variation in Facebook and other system usage (Ajzen 2002; Culnan and Armstrong 1999; Hoofnagle et al. 2010). Experience was measured as usage duration and frequency. We multiplied duration and frequency to form a total experience-over-time variable. We also controlled for the number of Facebook friends at the University and disposition to trust technology. The former may affect information disclosure because one's privacy exposure increases as the number of Facebook friends grows. Disposition to trust could influence one to be more likely to disclose information and more likely to use social networking.

Results

Partial Least Squares (PLS) was used to test the hypotheses. PLS is often used when the model is complex and not previously tested. Our model is new and complex, especially with twelve variables (including the five control variables). In addition, PLS is robust to departures to

normality. As an indicator of normality, we examined variable skewness and kurtosis using SPSS's descriptive statistics function. We divided the skewness stat by the standard error of skewness to obtain a Z-score. The absolute values of the skewness Z-scores varied from 0.93 for information disclosure item five to 10.80 for use continuance item one. Twenty-eight of the thirty-six variables' Z scores exceed the skewness standard of <3.0 (Kline, 1998). The highest kurtosis Z score value was 8.05, which is within Kline's standard of 10.0. PLS is one acceptable method to use when data is non-normal. PLS also easily enables one to use second order factors, which we used to depict trusting beliefs.

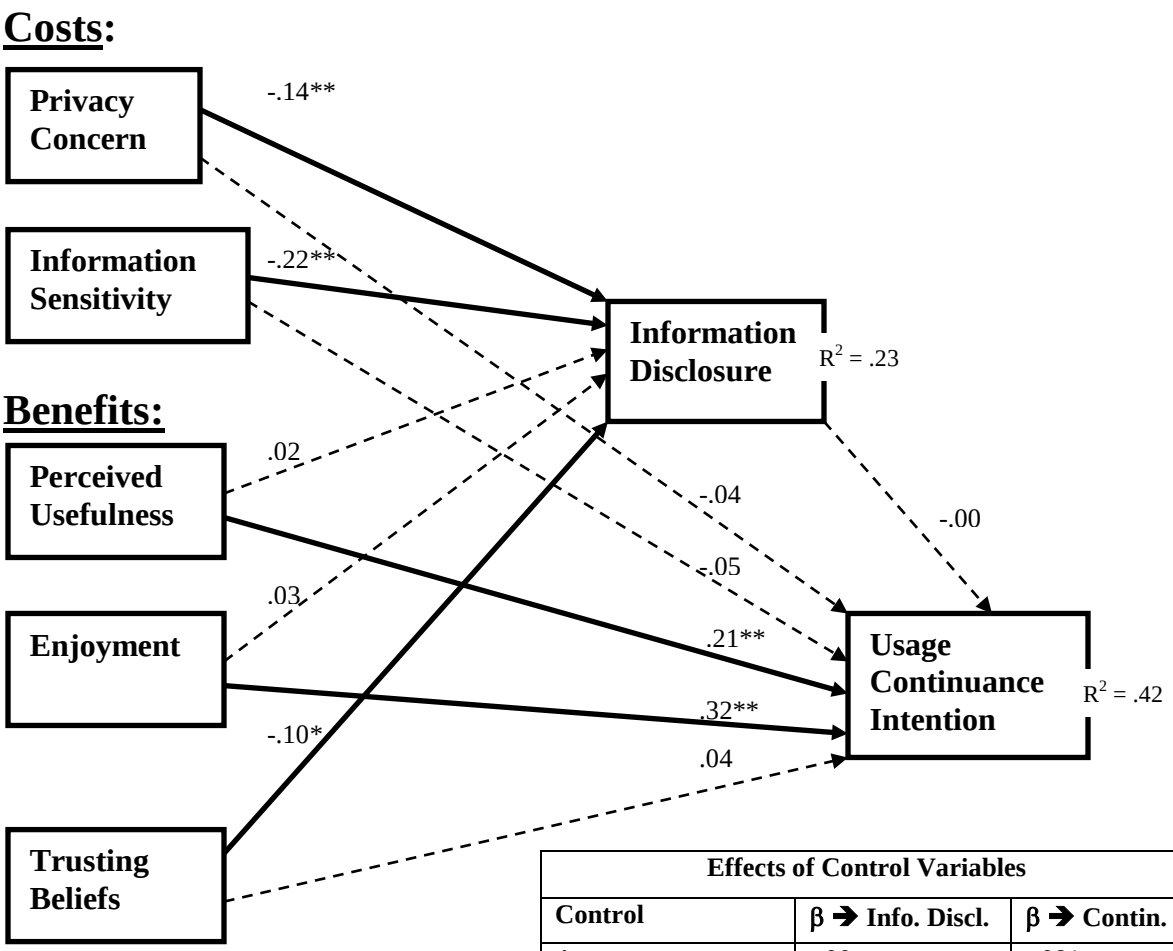
Figure 2 shows the results of the structural model test. Both privacy concern (β = -.14*) and information sensitivity (β = -.22**) significantly influence information disclosure, supporting H1 and H2. Trusting beliefs also significantly predict information disclosure (β = -.10*), but in the direction opposite of that predicted by H3 (i.e., as a cost). Neither perceived usefulness (β = .02) nor enjoyment (β = .03) influenced information disclosure; thus H4 and H5 were not supported. H6 through H8 were also not supported, since privacy concern, information sensitivity, and trusting beliefs did not influence usage continuance intentions. However, usefulness (β = .21**) and enjoyment (β = .32**) did influence continuance intention, supporting H9 and H10. Finally, information disclosure did not affect continuance intentions.

Discussion

This study is one of the first to examine how a privacy calculus model that incorporates information disclosure behavior affects social networking website continuance intentions. The model explains 23% of the variance in information disclosure, which is more than the 13.6% reported by Krasnova et al. (2009). This could be because we operationalized information disclosure as the users' ability to restrict access to their personal information using vendor

provided privacy settings, rather than a more general type of disclosure behavior. However, more work will need to be done to pinpoint what users feel is the most important privacy behavior related to social networking websites. For example, Facebook users can restrict access to certain groups (i.e., "friends only" or "friends of friends"). Future research should study privacy calculus decisions regarding specific types of privacy behavior.

Figure 2. Empirical Test Results



Effects of Control Variables		
Control	**β → Info. Discl.**	**β → Contin. Int.**
Age	-.00	-.09*
Gender	-.14**	-.01
Experience	-.22**	.22**
Number Friends	-.12**	-.04
Disp. to Trust	.13**	.10**

This study found mixed results regarding privacy calculus for Facebook disclosure behavior as only three of the five cost/benefit factors were significant. Privacy concern and information sensitivity, which we predicted would decrease one's information disclosure and thus be perceived as a cost to allowing access to one's information, were indeed significant. However, neither enjoyment nor perceived usefulness influenced information disclosure, meaning that users did not employ usefulness or enjoyment of the website to decide their information disclosure behavior. As a whole, this result does not support privacy calculus because only the two negative (cost) factors of information disclosure were significant. Users did not utilize any benefits in making their privacy-disclosure decision.

Trusting beliefs influenced information disclosure, but was perceived as a cost rather than a benefit. In other words, while we thought users with higher levels of trust in the website would have higher information disclosure (H3), results show that higher trust levels actually decreased information disclosure. Trusting beliefs may have had a negative effect on information disclosure because the privacy settings provided by the vendor promote feelings of trust. Individuals who use the settings are more aware that the website is trying to act in their best interests by giving them control over their privacy. Trust in the website may actually encourage users to take more precautionary privacy behaviors.

Only perceived usefulness and enjoyment predicted usage continuance intention. In fact, none of the factors that predicted information disclosure predicted continuance intention. What the above results imply overall is that people disclose information on Facebook for different reasons than their reasons for continuing to use Facebook.

Perhaps one reason for our results is that online social interactions and the Facebook privacy setting options change the way we think about privacy from "do I share or not?" to "how much do I share and with whom?" The former is a simple binary decision, while the latter is a more complex decision. This complexity may change the effects of the privacy calculus.

Results Robustness Test

In order to try to understand the results better and to test them for robustness, we added three additional control variables (all at once) to the model predicting information disclosure and continuance intention. This enables us to test plausible alternatives to our model. First, we asked respondents how close they are to being on the job market: now, next semester, next year, in two-plus years, or not at all. We did this to see if nearness to time for the job market might decrease their tendency to disclose information or decrease their Facebook usage intention. Although the beta coefficients were negative, neither were significant. Second, we wanted to see if perceived risk would matter. We asked, "Considering what you do on MySNW.com, how would you rate the overall risk of doing your social networking using MySNW.com?" (Scale: 1=Extremely Low; 7=Extremely High) We reasoned that perceived risk would decrease both information disclosure and continuance intention. Neither beta coefficient was significant. Third, we decided to control for structural assurance, which means perceptions that the Facebook website employs adequate technological structures and safeguards to protect one while using the site, thus providing a successful online experience (Gefen et al. 2003). We adapted four items from McKnight (2002) to measure structural assurance (validity statistics: Cronbach's Alpha = .95; AVE = .86; highest correlation with another construct = .46 with trusting beliefs). We projected that structural assurance would offset risk and thus increase both information disclosure and continuance intention. The beta for predicting continuance intention was 0.18

($p<.01$), while the beta for predicting information disclosure was not significant. Adding these three variables only increased the R^2 for information disclosure from .23. to .24 and only increased the R^2 for continuance intention from .42 to .44. The other significant relationships in the model were unchanged, except that the trusting beliefs beta in predicting information disclosure dropped from -.10 ($p < .05$) to -.09 ($p < .10$). These results indicate our findings are relatively robust to the effects of these plausible alternatives.

To understand our results qualitatively, we also asked an open-ended question regarding Facebook risks: "What do you see as risks to a college student using MySNW.com?" One of the authors went through the answers and made up a coding key. Next, two co-authors coded each of the first 91 cases and then met to reconcile their disagreeing answers, with the coding key author as arbitrator. Each item received a final agreed-upon set of codes. They then coded the next 109 cases and met again. Next they coded the other 191 cases and met. Overall coding agreement was 0.81. Next a research assistant student coder went through the same three cycles while her agreement with the reconciled codes was measured. Her coding agreement was 0.89.

Eighty-four subjects did not answer this open-ended question (a limitation), but of the 307 who did, a wide variety of risks were mentioned, and many students listed not only one risk, but several. Their answers were often quite insightful. 52% of the comments were about job- or financial risk, which were primarily about losing a job or an interview because of something seen on Facebook. 15% of the comments were about privacy risks, 9% mentioned risk of mental or bodily harm (e.g., stalking), 5% mentioned risk of legal action, such as underage alcohol detection, and 16% mentioned other risks, such as reputation loss or spammers/hackers. Only 2% (10) of the comments indicated there was little or no risk. Only 5 comments (1%) mentioned time wasted on the website. Females mentioned mental/bodily harm more than did males, on

average. Males disproportionately mentioned legal action risk. We created a dummy variable reflecting respondent mention of these risk categories and then correlated the risk category dummy variables with the main model dependent variables. None of the categories correlated with the information disclosure dependent variable. Only the job-financial risk dummy correlated with continuance intention ($r = .130$, $p = .010$). This suggests most students were aware of one or more risks but that understanding these risks had no impact on their information disclosure. Only the job-financial risk affected continuance intention, and the impact was positive. Job-financial risk awareness may be a function of how much Facebook experience subjects have; experience reveals such risks but also often incites a desire to continue using Facebook.

Habit

One reason respondents separated their decision to disclose information from their decision to continue using the website is that use for many is an engrained daily habit. 64.7% reported using Facebook either several times or many times a day. An additional 18.4% use it about once a day. 71.4% had used Facebook for more than three years, which means most have had plenty of time to form a habit. 34.0% strongly agreed that "The use of MySNW.com has become a habit for me." 27.4% moderately agreed and 22.5% slightly agreed, making 83.9% in total. Perhaps because Facebook is a habit for many, they accept the privacy risks and move forward. Note that 68.8% of respondents said they "intend to continue using" Facebook at the 6 or 7 level on a 7-point scale from 1=Not True at All to 7=Absolutely true. Habit theory suggests that once a habit is formed, actions are not reasoned through but occur automatically (Limayem et al. 2007). This kind of automatic response would therefore obviate the need to reason through the decision, which makes habit a solid explanation for the lack of a privacy calculus.

Compartmentalization

We searched additional literature to explain the separation of predictors between information disclosure and continuance intention. We speculate that perhaps one issue affecting how privacy calculus works is that people sometimes "compartmentalize" different beliefs about others. Principles 1 and 2 provide background for how beliefs compartmentalize.

Principle 1: At first, beliefs about someone (e.g., about their competence and integrity) will stay consistent with each other; for example, an increase in competence belief may elevate integrity belief, and a decrease in integrity belief may drag down competence belief. Beliefs stay consistent at first because people don't know each other in detail and yet would like to maintain a simple, unified positive or negative view of the other person (Abelson et al. 1968). This is especially true when people first meet and continues true as long as one lacks verifiable information about a person. For example, newly-revealed information that a CEO lacks benevolence toward workers will probably drag down worker beliefs about that CEO's integrity and competence. Negative beliefs can "taint" other beliefs because they are a unified set.

Principle 2: People seek evidence to confirm their initial beliefs. Over time people develop a multi-dimensional view of the other. Then, as credible evidence arises contrary to one belief, that belief can be modified without affecting other beliefs (compartmentalization). Over time, we differentiate beliefs about others as we get to know them well (Fiske 1993; Lewicki et al. 1998). While beliefs like integrity and competence may be consistent with each other at first, experience enables one to acquire a combination of high integrity belief and low competence belief in the other (Lewicki et al. 1998). A just-married couple may trust each other in almost everything. But interaction over time teaches them specific areas in which they can and cannot trust each other. One may fully trust one's spouse to be faithful but not trust her to remember to

pick up groceries on the way home from work. This is the "compartmentalization of beliefs" effect.

Our findings suggest our respondents (who have high Facebook experience) tend to compartmentalize social networking privacy issues from use issues. By contrast, in e-commerce research, privacy and security issues have often affected use. For example, Dinev and Hart (2005/2006) find that privacy concern influences intention to transact online. Liu et al. (2004) find that privacy indirectly affects behavioral intention to use two e-commerce websites. Wang et al. (2006) find privacy and security are important to intention to use a mobile phone service. By contrast, we find that for use of a very familiar social networking website, privacy concerns did not significantly affect use intention. Showing a further compartmentalization effect, we also find that information disclosure was not a factor predicting use intention (Figure 2). That is, people hold entirely separate views of continuance intention and information disclosure. These variables correlate at only -0.08ns and have different antecedents. Therefore, it appears our subjects did not link their privacy concerns and information disclosure choices with the issue of whether or not to continue using Facebook.

Limitations and Future Research

This study's results may not generalize due to sample limitations (US-based university business students). Different reactions may result from sampling different age groups or nationalities (Krasnova and Veltri 2010). Our measures of information disclosure are limited to self-reports, which will likely differ somewhat from actual information disclosure. The study also does not consider other possible factors, such as social pressure, trust in other users, and past privacy violations. Future studies should also address what users believe they are disclosing

online and how aware they are of how organizations use their undisclosed information, such as Internet surfing patterns.

Conclusion

This study addresses the issue of privacy calculus in a social networking context. We find that the privacy calculus model is not well-supported, in that only costs-of-disclosing variables predict information disclosure and only benefits-of-disclosing variables predict continuance intention. We also find that information disclosure is not related to intentions to continue using the social networking website. This finding may be due to the strong pull of habit on Facebook users or due to the added complexity of Facebook privacy options. Or, it could be because users know Facebook well enough to compartmentalize their privacy perceptions from their continued use intentions. This research should prompt further investigations about privacy and social networking and how privacy issues affect use.

References

R.P. Abelson, E. Aronson, W. J. McGuire, T. M. Newcomb, M. J. Rosenberg, and P. H. Tannenbaum, eds. *Theories of Cognitive Consistency: A Sourcebook*. Chicago 1968: Rand-McNally.

I. Ajzen, "Residual effects of past on later behavior: habituation and reasoned action perspectives," *Personality and Social Psychology Review* (6:2), 2002, pp. 107-122.

N. F. Awad, and M. S. Krishnan. "The Personalization Productivity Paradox: An Empirical Examination of Information Transparency and the Willingness to be Profiled Online for Personalization," *MIS Quarterly* (30:1), 2006, pp. 13-28.

P.M. Bentler, and Bonett, D. G., "Significance Tests and Goodness of Fit in the Analysis of Covariance Structures," *Psychological Bulletin* (88:3), 1980, pp. 588-606.

R. K. Chellappa and R. G. Sin, "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma." *Information Technology and Management* (6), 2005, pp. 181-202.

G. A. Churchill, Jr., "A Paradigm for Developing Better Measures of Marketing Constructs," *Journal of Marketing Research* (16:1), 1979, pp. 64-73.

M. J. Culnan, "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," *MIS Quarterly* (17:3), 1993, pp. 341-363.

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

F. Davis, R. Bagozzi, and P Warsaw, "User Acceptance of Information Technology: A Comparison of Two Theoretical Models," *Management Science* (35:8), 1989, pp. 982-1003.

T. Dinev, and P. Hart, "Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact," *International Journal of Electronic Commerce* (10:2), 2005-2006, pp 7-29.

T. Dinev, and P. Hart, "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), 2006, pp. 61-80.

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

T. Dinev, P. Hart and M. R. Mullen, "Internet Privacy Concerns and Beliefs About Government Surveillance – An Empirical Investigation," *Journal of Strategic Information Systems* (17). 2008, pp. 214-233.

S. Fiske, "Social Cognition and Social Perception," *Annual Review of Psychology* (44), 1993, pp. 155-194.

C. Fornell, and D. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:3), 1981, pp. 39-50.

D. Gefen, E. Karahanna, and D. Straub, "Trust And Tam In Online Shopping: An Integrated Model." *MIS Quarterly* (27:1), 2003, pp. 51-90.

J. Hart, C. Ridley, F. Taher, C. Sas and A. Dix, "Exploring the Facebook Experience: A New Approach to Usability", *Proceedings of NordiCHI 2008*, 18-22 October 2008, Lund, Sweden, 471-474.

C. Hoofnagle, J. King, S. Li, Su and J. Turow, "How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?" (April 14, 2010). Available at SSRN: http://ssrn.com/abstract=1589864

C. B. Jarvis, S. B. MacKenzie and P. M. Podsakoff, "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research," *The Journal of Consumer Research* (30:2), 2003, pp. 199-218.

Kline, R.B. *Principles and Practices of Structural Equation Modeling*, The Guilford Press, New York, NY 1998.

M. Koufaris, "Applying the technology acceptance model and flow theory to online consumer behavior." *Information Systems Research* (13:20), 2002, pp. 205-223.

H. Krasnova, E. Kolesnikova and O. Guenther, "'It won't happen to me!': Self-disclosure in online social networks," *AMCIS 2009 Proceedings*, 2009.

H. Krasnova and N. Veltri, "Privacy calculus on social networking sites: Explorative evidence from Germany and USA". *Proceedings of the 43rd Hawaii International Conference on System Sciences*, 2010.

R. S. Laufer, and M. Wolfe. "Privacy as a Concept and a Social issue: A Multidimensional Development Theory," *Journal of Social Issues* (33:3), 1977, pp. 22-42.

R. Lewicki, D. McAllister and R. Bies, "Trust and distrust: New relationships and realities." *Academy of Management Review*, 23(3), 1998, pp. 438-458.

D. Li, P. Y .K. Chau and H. Lou, "Understanding individual adoption of instant messaging; An empirical investigation," *Journal of the Association for Information Systems* (6:4), 2005, pp. 102-129.

M. Limayem, S. G. Hirt and C. M. K. Cheung, "How Habit Limits the Predictive Power of Intention: The Case of Information Systems Continuance," *MIS Quarterly* (31:4), 2007, pp. 705-737.

C. Liu, J. Marchewkaa and J. Lub, "Beyond Concern: a privacy-trust-behavioral intention model of electronic commerce," *Information & Management* (42:2), 2004, pp. 127-142

V. McKinney, K. Yoon, and F. M. Zahedi, "The Measurement of Web-Customer Satisfaction: An Expectation and Disconfirmation Approach," *Information Systems Research*, (13:3), 2002, pp. 296-315.

D. H. McKnight, V. Choudhury, and C. Kacmar, "Developing and Validating Trust Measures for e-Commerce: An Integrative Typology," *Information Systems Research* (13:3), 2002, pp. 334-359.

P. Norberg, D. R. Horne and D. A. Horne, "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors." *Journal of Consumer Affairs* (41:1), 2007, pp. 100-126.

P. A. Pavlou and D. Gefen, "Building effective online marketplaces with institution-based trust," *Information Systems Research* (15:1), pp. 37-59.

P. M. Podsakoff, J. Y. Lee and N. P. Podsakoff, "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies, *Journal of Applied Psychology* (88:5), 2003, pp. 879-903.

R. Sharma, P. Yetton, and J. Crawford, "Estimating the Effect of Common Method Variance: The Method-Method Pair Technique with an Illustration from TAM Research," *MIS Quarterly* (33:3), 2009, 473-490.

D. Sledgianowski and S. Kulviwat, "Using Social Network Sites: The Effects of Playfulness, Critical Mass and Trust in an Hedonic Context." *The Journal of Computer Information Systems*, (48:4), 2009, pp. 74-83.

H. J. Smith, S. J. Milberg and S. J. Burke, "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20:2), 1996, pp. 167-196.

J. Son and S. S. Kim, "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), 2008, pp. 503-529.

T. F. Stafford, M. R. Stafford and L.L. Schkade, "Determining Uses and Gratifications for the Internet," *Decision Sciences* (35:2), 2004, pp. 259-288.

J. Thatcher, M. Loughry, J. Lim, and H. McKnight, "Internet Anxiety: An Empirical Study of the Effects of Personality, Beliefs, and Social Support," *Information & Management* (44:4), 2007, pp. 353-363.

H. van der Heijden, "User Acceptance of Hedonic Information Systems," *MIS Quarterly* (28:4), 2004, pp. 695-704.

V. Venkatesh, "Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model." *Information Systems Research* (11:4), 2000, p. 342

V. Venkatesh and M. Morris, "Why Don't Men Ever Stop to Ask for Directions? Gender, Social Influence, and Their Role in Technology Acceptance and Usage Behavior," *MIS Quarterly* (24:1), 2000, pp. 115-139

V. Venkatesh, M. Morris, G. B. Davis and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), 2003, pp. 425-478.

Y. Wang, H. Lin and P. Luarn, "Predicting Consumer Intention to Use Mobile Service," *Information Systems Journal* (16), 2006, pp. 157-179.

W. Wang and I. Benbasat, 'Trust in and Adoption of Online Recommendation Agents," *Journal of the Association for Information Systems* (6:3), 2005, pp. 72-101.

K. Widaman, "Hierarchically Nested Covariance Structure Models for Multitrait-Multimethod Data." *Applied Psychological Measurement* (9:1), 1985, 1-23.

J. Wortham, "Facebook Glitch Brings New Privacy Worries," *New York Times*, 2010a http://www.nytimes.com/2010/05/06/technology/internet/ 06facebook.html?hpw, accessed 5/06/2010.

J. Wortham, "Ask Facebook Your Privacy Questions," *New York Times*, 2010b, http://bits.blogs.nytimes.com/2010/05/06/ask-facebook-your-privacy-questions/?scp=1&sq=ask%20 facebook%20your%20privacy%20questions&st=cse, accessed 5/7/2010.

J. Wu and D. Liu, "The Effects of Trust and Enjoyment on Intention to Play Online Games," *Journal of Electronic Commerce Research* (8:2), 2007, pp. 128-140.

S. Yang and K. Wang, "The Influence of Information Sensitivity Compensation on Privacy Concern and Behavioral Intention," *The Database for Advances in Information Systems* (40:1), 2009, pp. 38-51.

Y. Yoo and M. Alavi, "Media and group cohesion: Relative influences on social presence, task participation, and group consensus," *MIS Quarterly* (25:3), 2001, 371-390.

D. E. Zand, "Trust and managerial problem solving." *Administrative Science Quarterly* (17), 1972, pp. 229-239.

S. Zeng, L. Wu, and H. Chen, "Sharing private information online: The mediator effect of social exchange," ICEC '09 *Proceedings of the 11th International Conference on Electronic Commerce*, 2009, pp. 231-239.

APPENDIX A
Measurement Items

Usage Continuance Intention *(7-point Likert scale from (1) Not true at all to (7) Very true)*

1. In the near future, I intend to continue using MySNW.com.
2. I intend to continue using MySNW.com.
3. I predict that I would continue using MySNW.com.

Information disclosure *(7-point scale from (1) Not at All to (4) Some to (7) A Great Deal) [new-all reverse-scored]]*

1. Using your privacy settings, how much do you control who can see your profile and personal information?
2. Using your privacy settings, how much do you control who can search for you and how you can be contacted?
3. Using your privacy settings, how much do you control what stories about you get published to your profile and your friends' News Feeds?
4. Using your privacy settings, how much do you control what information is available to applications you use on MySNW.com?
5. Using your privacy settings, how much do you block people?

Privacy Concern *(7-point scale from (1) Not at All Concerned to (7) Very Concerned)*

1. I am concerned that the information I submit on MySNW.com could be misused.
2. I am concerned that a person can find private information about me on MySNW.com.
3. I am concerned about submitting information on MySNW.com, because of what others might do with it.
4. I am concerned about submitting information on MySNW.com, because it could be used in a way I did not foresee.

Information Sensitivity *(7-point scale from (1) Not Sensitive at All to (7) Extremely Sensitive) [new]*

Rate how privacy sensitive you think the following MySNW.com information about you is:

1. Basic information (sex, birthday, hometown, political and religious views)
2. Contact information (emails, IM screen name, home/school addresses and phone numbers, website URL)
3. Relationship information (status, interested in, looking for)
4. Personal information (activities, interests, about me, favorite movies, TV shows, books, and quotes)
5. Educational information (university, concentration, class year, high school)
6. Work information (employer, position, description, city/town, time period)
7. Tagged photos

Perceived Usefulness *(7-point Likert scale from (1) Strongly disagree to (7) Strongly agree)*

1. Using MySNW.com improves my performance in online social networking.
2. Using MySNW.com increases my productivity in online social networking.
3. Using MySNW.com enhances my effectiveness in online social networking.
4. I find MySNW.com to be useful for online social networking.

Enjoyment *(7-point Likert scale from (1) Strongly disagree to (7) Strongly agree*

1. I find using MySNW.com to be enjoyable.
2. The actual process of using MySNW.com is pleasant.
3. I have fun using MySNW.com.

Technology Trusting Belief–Reliability *(7-point Likert scale: (1) Strongly disagree to (7) Strongly agree)*

1. MySNW.com is a very reliable website.
2. MySNW.com does not fail me.
3. MySNW.com is extremely dependable.
4.

Technology Trusting Belief –Functionality *(7-pt. Likert scale: (1) Strongly disagree to (7) Strongly agree)*

1. MySNW.com has the functionality I need.
2. MySNW.com has the features required for my online social activities.
3. MySNW.com has the ability to do what I want it to do.

Technology Trusting Belief –Helpfulness *(7-pt. Likert scale: (1) Strongly disagree to (7) Strongly agree)*

1. MySNW.com supplies my need for help through a help function.
2. MySNW.com provides competent guidance (as needed) through a help function.
3. MySNW.com provides whatever help I need.

Control variable: Disposition to Trust Technology *(7-pt. Likert scale: (1) Strongly disagree to (7) Strongly agree) [new]*

1. My typical approach is to trust new information technologies until they prove to me that I shouldn't trust them.
2. I usually trust in information technology until it gives me a reason not to.

3. I generally give an information technology the benefit of the doubt when I first use it.

Control variable: Experience (formed by multiplying items 1. and 2.)

1. How long have you been using MySNW.com? (7-point scale from (1) Have not used at all to (7) More than 5 years)
2. How frequently do you use MySNW.com? (7-point scale from (1) Not at all to (7) Many times a day)

Control variable: Number of MySNW.com Friends at this University

1. Approximately how many MySNW.com friends do you have from [university name]? (6-point scale from (1) 1-50 to (6) Greater than 350)