A Quantitative and Qualitative Study of Facebook Privacy using the Antecedent-Privacy Concern-Outcome Macro Model

Completed Research Paper

Nancy Lankton
Marshall University
lankton@marshall.edu

John Tripp
Baylor University
john_tripp@baylor.edu

ABSTRACT

Information privacy is a complex and important phenomenon to understand. Because of this, several recent review articles have integrated findings across various studies and contexts. In this study we investigate information privacy in the online social networking context using the Antecedent-Privacy Concern-Outcome (APCO) Macro Model as the theoretical lens. We use both quantitative and qualitative data collected in a survey of Facebook users. Online social networking provides a rich window into privacy concerns and the resulting behavioral reactions. By analyzing both types of data, we are able to show additional support and insights for our hypotheses tests. These results provide future research opportunities that include modifying the APCO model and refining its constructs to be more context and risk-specific.

Keywords

Privacy, privacy concern, social networking, qualitative

INTRODUCTION

Determining whether to disclose one's personal information or keep it private is a complex decision that people face every day. Because disclosure decisions can influence information technology use (Dinev and Hart, 2006), it is an important topic in information systems (IS) research. This study's aim is to enhance our understanding of information privacy and disclosure decisions in the online social networking context (OSN) by using the Antecedent-Privacy Concern-Outcome (APCO) Macro Model (Smith, et al., 2011). This model was developed based on a review of the information privacy literature. It focuses on privacy concerns, which are concerns that an individual has regarding opportunistic behavior related to personal information that the individual discloses (Dinev and Hart, 2006). In the APCO model antecedents to privacy concerns include privacy experiences, privacy awareness, personality differences, demographic differences, and culture/climate. Outcomes include trust, behavioral reactions, regulation, and risks/costs and benefits that result in a privacy calculus. APCO is intended not as a comprehensive, broad model of information privacy, but rather as a guide for future research (Smith et al., 2011).

This study contributes in two ways. First, we analyze several key relationships from the APCO model both qualitatively and quantitatively. We use a survey to collect quantitative data to test our hypothesized model using structural equation modeling methods. We also collect qualitative data to help explain users' reasoning for their responses and further explain our quantitative results. Using both types of analyses allows us to examine the relationships defined in the model from multiple perspectives. Second, we extend APCO to the OSN context. Information privacy related to OSN can be more complex than in e-commerce. In the e-commerce context, users perform dyadic disclosure decisions in each e-commerce transaction event. In OSN, users must decide not only what information to disclose, but also to whom to disclose it. Therefore, Facebook privacy involves more than just disclosing or not disclosing. Users can choose to manage their privacy in various ways. For example, Facebook users can control their privacy by making their profiles accessible to friends only. While prior research investigates OSN privacy issues both quantitatively and qualitatively (e.g., Debatin, et al., 2009), no research to our knowledge has used these methods to investigate and validate the relationships presented in the APCO model.

RESEARCH HYPOTHESES

In this section we develop hypotheses for many of the relationships found in the APCO macro model. Table 1 provides definitions of the constructs in this study and shows how they relate to the APCO constructs. Figure 1 presents the research model.

Variable (This Study)	APCO Model Variable	Definition
Experience	Privacy Experiences	Length and frequency of prior Facebook use
Gender	Demographic Differences	Gender
Privacy Concerns	Privacy Concerns	Concerns about opportunistic behavior related to personal information that is disclosed by the respondent in particular
Privacy Risk	Risks/Costs	Concerns about opportunistic behavior related to personal information that is disclosed by the respondent in general
Enjoyment	Benefits	The extent to which using the website is perceived to be enjoyable in its own right, apart from any performance consequences that may be incurred
Trust	Trust	Being willing to depend on the website, or a volitional preparedness to make oneself vulnerable
Change Privacy Settings	Behavioral Reactions	Whether the vendor-provided privacy settings have been changed
Limit Number Friends		Number of MySNW.com friends at [University]
Differentiate Friends		To what extent does the user restrict who is included in his or her list of friends
Continuance Intention		Intentions to continue using MySNW.com

Table 1: Variables

The APCO model includes privacy experience as an antecedent to privacy concern because individuals who have been exposed to or been the victim of personal information abuses should have stronger privacy concerns (Smith et al., 2011). Further, Tufekci (2008) finds that nonusers of a social network site had higher privacy concerns than users. We include prior experience to capture these effects, as users with more prior experience are more likely to have encountered privacy abuses.

H1: Experience will positively influence privacy concern.

To incorporate demographic differences as proposed by APCO we include gender in our model. Researchers find that women are generally more concerned about privacy than men. For example, Sheehan (1999) finds that women are more likely than men to be concerned when a web site says that personal information will be used by other divisions of the company. They suggest that this shows women are more uncomfortable with unfamiliar entities than are men, which could make them more concerned about others acting opportunistically with their personal information in OSN. Further, Fogul and Nehmad (2009) find that women have significantly greater OSN privacy concerns than men, suggesting that women are less influenced by implied social contracts relating to privacy safeguards than men.

H2: Women will have greater privacy concerns than men.

APCO depicts privacy risk, trust, and behavioral reactions as outcomes of privacy concern. Both privacy concern and privacy risk represent the "costs" of disclosing information (Dinev and Hart, 2006). The two variables are highly related because perceptions that one's personal information might be used opportunistically can influence one's perceptions that personal information in general might be used opportunistically.

H3: Privacy concern will positively influence privacy risk.

Privacy concern negatively influences trust because greater concerns may make one less likely to feel they can rely or depend on the technology. While privacy concern relates to the likelihood of not having desirable results, trust refers to the likelihood that one can depend and rely on the trustee to perform desirable actions. This suggests a negative relation between the variables. Empirical research shows that privacy concern negatively influences trust (Eastlick et al., 2006).

H4: Privacy concern will negatively influence trust.

APCO also predicts that privacy concern will influence behavioral reactions. The more OSN privacy concern the more one is likely to exercise privacy behaviors to control their personal information and prevent bad things from happening. Privacy concern can make OSN users more likely to take action to protect their privacy. In OSN, privacy behaviors can include changing vendor privacy settings (change privacy settings) (Lankton et al., 2012), limiting the number of friends in one's friends list (limit number friends) and allowing only friends one has interacted with a lot in one's friends list (differentiate friends) (Debatin et al., 2009; Stutzman and Kramer-Duffield, 2010). These responses to high concerns are consistent with expectancy theory's explanation that individuals are motivated to minimize negative outcomes (Dinev and Hart, 2006).

H5a: Privacy concern will positively influence privacy behaviors (change privacy settings, limit number friends, differentiate friends).

We also include usage continuance intention in our model as a behavioral reaction to privacy concerns because some OSN users might discontinue use if their concerns are too high.

H5b: Privacy concern will negatively influence usage continuance intention.

APCO also predicts that trust, and the privacy risks and benefits involved in the privacy calculus decision will influence behavioral reactions. Trust plays an important role in predicting privacy behaviors (Dinev and Hart, 2006). Trust reduces the perceived concerns about revealing information making one feel that disclosure is a safe activity (Metzger, 2004). If one decides a website is dependable and reliable one will be less likely to take steps to keep information private.

H6a: Trust will negatively influence privacy behaviors (change privacy settings, limit number friends, differentiate friends).

Trust also predicts usage continuance intentions because when one is willing to depend, one makes a conscious choice to put aside doubts and move forward with the relationship (Holmes, 1991). Benamati et al., (2010) find that trust influences intention to use a bookseller website.

H6b: Trust will positively influence usage continuance intention.

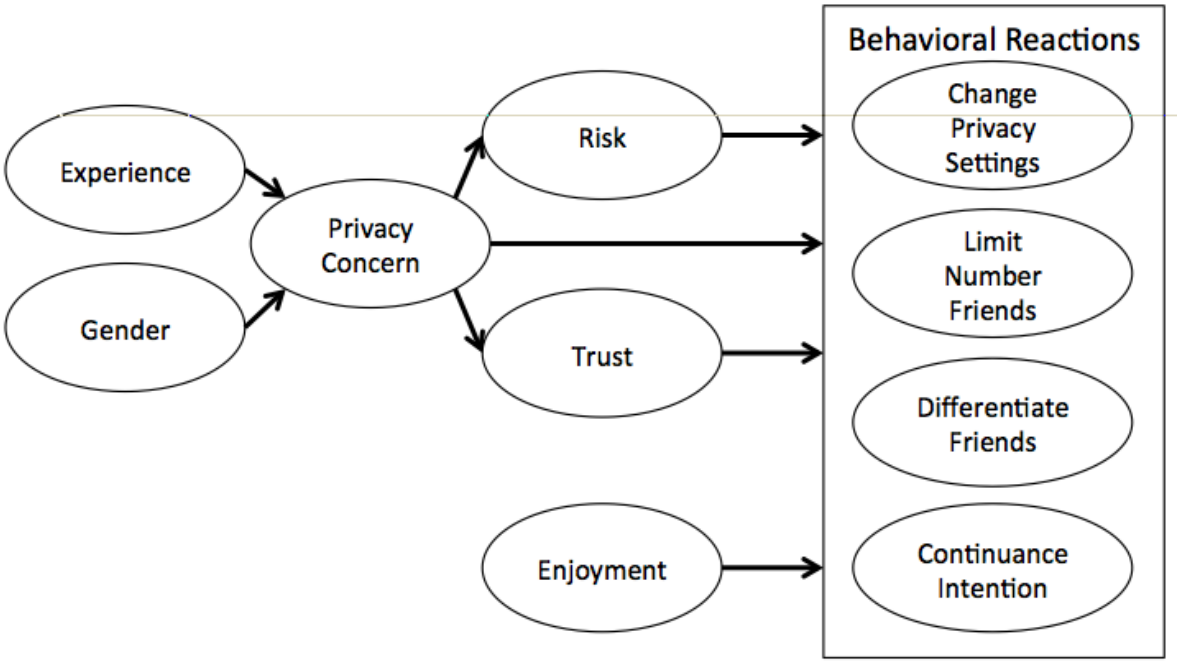

Figure 1: Research Model

The final relationships in APCO that deal with OSN are the effects of privacy risks and benefits on behavioral reactions. Similar to privacy concerns, privacy risks should increase the likelihood of engaging in privacy behaviors to protect opportunistic use of personal information. These risks should also make one less likely to want to continue using the OSN website.

H7a: Privacy concern will positively influence privacy behaviors (change privacy settings, limit number friends, differentiate friends).

H7b: Privacy concern will negatively influence usage continuance intention.

According to previous research that motivates the APCO model, benefits from using a technology should decrease one's privacy behaviors and increase continued use. We consider enjoyment as a benefit of OSN use, because enjoyment is a major reason people use social networking websites (Hart et al., 2008). The more enjoyable using the OSN is, the less likely one will engage in privacy behaviors because this might stifle one's ability to make social connections.

H8a: Enjoyment will negatively influence privacy behaviors (change privacy settings, limit number friends, differentiate friends).

Enjoyment is part of the extended unified theory of acceptance and use of technology for consumers as a predictor of continuance intention (Venkatesh et al., 2012). People will want to continue using a technology they find enjoyable. Prior research finds that enjoyment significantly influences intention to continue using OSN websites (Sledgianowski and Kulviwat, 2009).

H8b: Enjoyment will positively influence usage continuance intention.

METHODOLOGY

This study used a questionnaire that we administered to students in a course required for all business students in a large Midwestern U.S. university. We asked respondents to indicate an OSN site of which they were either currently a member or might become a member. The survey then instructed then to answer all remaining questions referring to that OSN site. 481 responses were received out of 540 enrollees (89%). We removed cases in which the respondent did not use Facebook and those who did not complete the questionnaire (including the qualitative question), resulting in a sample size of 322. Although people of many age groups now use Facebook, young adults are just as concerned about privacy issues as older groups (Hoofnagle et al., 2010).

We adapted most scales from previous research: privacy concern and privacy risk (Dinev and Hart, 2006), trust (McKnight et al., 2002), enjoyment (Venkatesh, 2000), and usage continuance intention (Venkatesh et al., 2003) (Appendix A). Items for behavioral reactions including change privacy settings, limit number friends, and differentiate friends were created by the authors. We measured experience using two items representing length and frequency of prior use. These items were multiplied to form a total site experience score.

	Mean	CA	AVE	1	2	3	4	5	6	7	8	9	10
1. Experience	23.89	na	na	**na**									
2. Gender	na	na	na	.12	**na**								
3. Privacy Concern	4.74	.91	.80	-.01	.13	**.89**							
4. Privacy Risk	4.67	.79	.61	-.02	.11	.46	**.78**						
5. Trust	5.33	.95	.90	.31	.13	-.10	-.05	**.95**					
6. Enjoyment	5.71	.94	.89	.41	.19	-.02	-.07	.50	**.94**				
7. Continuance Intention	5.97	.97	.94	.42	.14	-.08	-.18	.49	.57	**.97**			
8. Change Privacy Settings	1.92	na	na	.20	.15	.17	.05	.07	.10	.14	**na**		
9. Limit Number Friends	3.15	na	na	.34	.11	.09	.06	.17	.22	.17	.18	**na**	
10. Differentiate Friends	4.35	na	na	.07	-.06	-.05	-.08	.01	.06	.04	-.05	.26	**na**

Table 2. Correlation Matrix
Means, Cronbach Alphas (CA) and Average Variance Extracted (AVE) (square root of AVE on diagonal)

QUANTITATIVE RESULTS

We used XL-Stat to analyze the measurement and structural models. For the measurement model, the items displayed adequate convergent validity with Cronbach alphas ranging from .79-.97, average variances extracted (AVE) from .61-.94, and item loadings from .79-.99 (Table 2). The items also had adequate discriminate validity with no PLS cross-loadings greater than the loadings (the highest cross-loading is .57). Also, the square root of the AVE for each variable is greater than the correlations among it and the other variables (Table 2).

The structural model results are presented in Table 3. Experience does not influence privacy concern but gender does, supporting H1 but not H2. Privacy concern has positive significant effects on privacy risk and change privacy settings, but has no significant effects on trust, limit number friends, differentiate friends, and continuance intention. This shows support for H3, partial support for H5a, and no support for H4 and H5b. The results also show that neither trust nor privacy risk have significant influences on the privacy behaviors but do significantly influence continuance intention, supporting H6b and H7b, but not supporting H6a and H7a. H8a is partially supported as enjoyment negatively influences limit friends. Also as predicted in H8b enjoyment influences continuance intention. The variance explained in continuance intention is 39%.

Structural Model Path	Standardized Coefficient (* p<05, ** p<.01, ***p<.001)	Hypothesis Supported
H1: Experience → Privacy Concern (+)	-.03ns	No
H2: Gender → Privacy Concern (+)	.13*	Yes
H3: Privacy Concern → Privacy Risk (+)	.46***	Yes
H4: Privacy Concern → Trust (-)	-.10ns (p=.07)	No
H5a: Privacy Concern → Limit Number Friends (+)	-.08ns	Partial
H5a: Privacy Concern → Differentiate Friends (+)	.02ns	
H5a: Privacy Concern → Change Privacy Settings (+)	.20**	
H5b: Privacy Concern → Continuance Intention (-)	.02ns	No
H6a: Trust → Limit Number Friends (-)	-.09ns	No
H6a: Trust → Differentiate Friends (-)	.04ns	
H6a: Trust → Change Privacy Settings (-)	.06ns	
H6b: Trust → Continuance Intention (+)	.27***	Yes
H7a: Privacy Risk → Limit Number Friends (+)	-.03ns	No
H7a: Privacy Risk → Differentiate Friends (+)	.07ns	
H7a: Privacy Risk → Change Privacy Settings (+)	-.04ns	
H7b: Privacy Risk → Continuance Intention (-)	-.15**	Yes
H8a: Enjoyment → Limit Number Friends (-)	-.18**	Partial
H8a: Enjoyment → Differentiate Friends (-)	-.08ns	
H8a: Enjoyment → Change Privacy Settings (-)	.07ns	
H8b: Enjoyment → Continuance Intention (+)	.42***	Yes

Table 3. Structural Model Results

QUALITATIVE RESULTS

To investigate these relationships more deeply, we also performed a qualitative analysis. For the qualitative analysis, immediately following the quantitative privacy concern questions we asked: "How crucial to your MySNW.com use are these privacy concerns? Then we asked, "Please briefly explain why:" and provided a box for a free-form answer. Two individuals coded the responses to the qualitative question. One was a researcher who is not a co-author and the other was an honors student. By analyzing each response, the researcher made up a coding sheet that grouped similar reasons as to why the privacy concerns influence Facebook use. Then the student reviewed the categories, combining four categories that were not distinguishable, leaving 32 distinct categories. Upon agreement about the coding sheet, these two independently coded the first 100 responses to one or more category. They subsequently met and reconciled codes that did not initially agree. They repeated the dual-coding process for the next 100 responses, and then for the remaining 122 responses to produce the final codes. Out of the 322 total responses, 51.6% of the responses were coded exactly the same (Cohen's Kappa =.50), and 81.7% in the same groups (Cohen's Kappa = .77).

Because responses could be coded into more than one category, there were a total of 542 coded responses (Appendix B). The group representing high privacy risk/importance (group D) had 247 responses. These individuals were mostly worried that personal information is available to others and can be misused/used by others as evidenced by the large number of responses

(147) coded to category D1. There are also quite a few responses coded to D3 and D6 that deal with privacy being an important issue. The group representing privacy behaviors (group B) had 138 responses. A majority of these relate to controlling content (74), while 25 discuss using privacy settings. Group C relating to job/financial risks had 83 responses, group A relating to low privacy risk/importance had 62, and group E relating to trust had 12.

Construct	Qualitative Category				
	Group A: *Low privacy risk/ importance*	Group B: *Privacy behaviors*	Group C: *Job/ financial risks*	Group D: *High privacy risk/importance*	Group E: *Trust*
How crucial to your Facebook use are these privacy concerns?	.27	.20	-.17	-.26	.13
Experience					.15
Gender			.11		
Privacy Concern	-.16	-.33	.30	.26	-.12
Privacy Risk	-.15		.13	.13	
Trust					.11
Enjoyment					
Continuance Intention		.16			
Change Privacy Settings	-.19		.13		
Limit Number Friends	-.14	.15			
Differentiate Friends			-.14		

Table 4. Significant ($p < .05$) Correlations among Qualitative Groups and Research Variables

We ran bivariate correlations (Table 4) of the group responses with the initial question, "How crucial to your Facebook use are these privacy concerns?" (measured from (1) absolutely vital to (7) not at all vital). Code groups A, B, and E that relate to low privacy risk/importance, privacy behaviors, and trust, respectively, are positively correlated with this question. This indicates these individuals were less likely to allow privacy concerns to impact their OSN use. Code groups C and D (that relate to job/financial risks and low privacy risk/importance) are negatively correlated, meaning these individuals' privacy concerns impacted their use.

We also ran bivariate correlations of the group responses with the research variables (Table 4). Similar to the above results, groups A, B, and E are negatively correlated with privacy concern meaning these individuals had lower privacy concerns, and groups C and D are positively correlated meaning these individuals had higher privacy concerns. As expected because they deal with risk levels, group A (low privacy risk/importance) correlates negatively with privacy risk, and groups C and D (job/financial risks and high privacy risk/importance) correlate positively with privacy risk. We discuss these results further in the next section.

DISCUSSION

We tested the APCO Macro Model within the OSN context. Regarding the antecedents to privacy concern, we find that while experience has no significant effect on privacy concern (H1), gender does (H2). The former result could be because our measure does not account for previous experience with privacy invasions. However, in the qualitative data, group E's significant correlation with experience indicates that experience may have a direct effect on trust (Gefen et al., 2003). Also, group C correlates significantly with gender suggesting that female's privacy concern may be related to lost job opportunities. Future research could incorporate experience's influence on other factors in the model, and examine more specific privacy concerns.

We also find that while privacy concern influences privacy risk (H3) it does not significantly influence trust (H4)— even though the relation is significant at p=.07. However, the qualitative group E (trust) correlates negatively with privacy

concern. The lack of greater significance between privacy concern and trust in the structural model could be because we used items that capture the OSN website's reliability and dependability. Privacy concern may have greater influence on other trust dimensions such as competence or benevolence. This can be explored in future research.

There were mixed results for the hypotheses related to the behavioral reactions. Privacy risk and trust do not significantly influence any of the privacy behaviors. However, we do find that the low privacy risk/importance group (A) was less likely to engage in privacy behaviors, probably because they do not perceive using the OSN website to be risky. This provides some support for H7a, even though it was not supported in the structural model. The high privacy risk/importance group D on the other hand, does not have any association with privacy behaviors, which is more consistent with our finding for H7a. It could be that the risk measures do not capture what makes OSN users take action to protect their privacy. We do find that those responding about job/financial risks were more likely to change privacy settings and *less* likely to differentiate friends. This latter finding supports the idea of using more specific risks and also reveals an important privacy management strategy. Because these individuals allow people they have not interacted with to become friends, they use privacy settings to control what these so-called "friends" can see. This may offset any job-related risks. Research can further investigate the relation between job risks and OSN privacy. Group E (trust) significantly correlates with the trust variable and does not correlate with the privacy behaviors, consistent with the structural results.

The two predictors of privacy behaviors in the structural model are privacy concern and enjoyment. The more privacy concern the more one is likely to use privacy settings (H5a). Also, the more enjoyment the less likely one is to limit friends (H8a). There may be other predictors of these privacy behaviors that future research can explore. We find in the qualitative data that those who engage in privacy behaviors (group B) limit the number of friends. It is a little surprising that this group does not significantly correlate with the other two privacy behaviors. However, because the responses relate to specific behaviors (B2 and B4 for example), it again suggests that reactions to privacy concerns, and possibly enjoyment may involve multiple privacy behaviors in certain subsets of OSN users.

Finally, we found that three out of four hypotheses related to continuance intention are significant. Enjoyment has the strongest effect (.42***). This makes sense because OSN website use is a hedonic activity. We also find that group B significantly correlates with continuance intention. This suggests that there may be an indirect effect of enjoyment through privacy behaviors, or vice versa. Future research can explore such extended APCO models.

LIMITATIONS AND CONCLUSIONS

This study has several limitations. First, we did not include all the variables from APCO. Some are not relevant to the OSN environment, for example privacy seals, and but some like culture, may be relevant. Second, we used student subjects, which are only one (albeit large) segment of OSN users. Third, we did not explore all possible OSN privacy behaviors. Future research can address these limitations.

Our study's aim was to use the APCO model as a lens to test privacy concern and privacy behaviors in the OSN context using both quantitative and qualitative data. We find that the qualitative data supports our structural model findings in many cases. It also provides insight into some hypotheses that were not supported. One key finding is that OSN users may engage in some privacy behaviors, and not others, resulting in some cancelling out of effects. Further, concerns and risks that produce these behaviors may be very specific (e.g., job related). We find that the APCO model is a useful guide for exploring privacy behaviors, and provide avenues for future research.

References

Benamati, M. A. Fuller, M. A. Serva and Baroudi, J. (2010) Clarifying the integration of trust and TAM in e-commerce environments: Implications for systems design and management, *IEEE Transactions on Engineering Management*, 57, 3, 380-393.

Debatin, B., Lovejoy, J. P., Horn, A-K. Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. Journal of Computer-Mediation Communication, 15, 83-108.

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

Eastlick, M. A., Lotz, S. L. and Warrington, P. (2006) Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment, *Journal of Business Research*, 59, 877–886.

Fogel, J. and Nehmad, E. (2009) Internet social network communities: Risk taking, trust, and privacy concerns, *Computers in Human Behavior*, 25, 153-160.

Gefen, D., Karahanna, E. and Straub, D. W. (2003) Inexperience and experience with online stores: The importance of TAM and trust, *IEEE Transactions on Engineering Management,* 50, 3, 307-321.

Hart, J., Ridley, C., Taher, F. Sas, C. and Dix, A. (2008) Exploring the facebook experience: A new approach to usability, *Proceedings of NordiCHI 2008*, October 8-22, Lund, Sweden, 471-474.

Holmes, J. G. (1991). Trust and the appraisal process in close relationships, in W. H. Jones, D. Perlman, (Eds) *Advances in Personal Relationships,* London, Jessica Kingsley, 57-104.

Hoofnagle, C. J., King, J., Li, S. and Turow, J. (2010) How different are young adults from older adults when it comes to information privacy attitudes and policies? Available at SSRN: http://ssrn.com/abstract=1589864 or http://dx.doi.org/10.2139/ssrn.1589864

Lankton, N., McKnight, H. and Thatcher, J. (2012) The moderating effects of privacy restrictiveness and experience on trusting beliefs and habit: An empirical test of intention to continue using a social networking website, *IEEE Transactions on Engineering Management,* 59, 4, 654-665.

McKnight, D. H. Choudhury, V. and Kacmar, C. Developing and validating trust measures for e-commerce: An integrative typology, *Information Systems Research,* 13, 3, 2002, 334-359.

Metzger, M. J. (2004) Privacy, trust, and disclosure: Exploring barriers to electronic commerce, *Journal of Computer-Mediated Communication*, 9, 4.

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.

Sheehan, K. B. (1999) An investigation of gender differences in on-line privacy concerns and resultant behavior, *Journal of Interactive Marketing*, 13, 4, 24-38.

Smith, H. J., Dinev, T. and Xu H. (2011) Information privacy research: An interdisciplinary review, *MIS Quarterly*, 35, 4, 989-1015.

Stutzman, F. and Kramer-Duffield, J. (2010) Friends only: Examining a privacy-enhancing behavior in Facebook, *CHI 2010, Privacy*, April 10–15, 2010, Atlanta, GA, USA.

Tufekci, Z. (2008) Can you see me now? Audience and disclosure regulation in online social network sites, *Bulletin of Science, Technology & Society*, 28, 1, 20-30.

Venkatesh, V., Thong, J. Y. L. and Xu, X. 2012 Consumer acceptance and use of Information technology: extending the Unified Theory of Acceptance and Use of Technology, MIS Quarterly, 36, 1, 157-178.

Venkatesh, V., Morris, M., Davis, G. B. and Davis, f. D. (2003) User acceptance of information technology: Toward a unified view, *MIS Quarterly,* 27,3, 425-478.

Venkatesh, V. (2000) Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model, *Information Systems Research,* 11, 4, 342-365.

APPENDIX A – Questionnaire Items

Experience
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 Likert scale from (1) not at all to (7) Many times a day.

Privacy Concern (7-point Likert 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.

Privacy Risk (7-point Likert from (1) Very Low Risk to (7) Very High Risk)
What do you believe is the risk for MySNW.com users due to the possibility that:
1. MySNW.com entries and posts could be sold to third parties?
2. Personal information submitted could be misused?
3. Personal information could be made available to unknown individuals or companies without your knowledge?
4. Personal information could be made available to government agencies?

Trust (7-point Likert from (1) Not True at All to (7) Absolutely True)
1. When I network socially online, I can depend on MySNW.com.
2. I can always rely on MySNW.com for online social networking.
3. I feel I can count on MySNW.com when networking online.

Enjoyment (7-point Likert 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.

Usage Continuance Intention (7-point Likert from (1) Not True at All to (7) Absolutely 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.

Change Privacy Settings
1. I have not changed any privacy settings since becoming a member of MySNW.com. (I have NOT made privacy setting changes/I have made privacy setting changes)

Differentiate Friends
MySNW.com Friend List consists of the following (pick one):
a. Those I have interacted with a lot only
b. Those I have interacted with a lot and SOME I have interacted with a little
c. Those I have interacted with a lot and MANY I have interacted with a little
d. Those I have interacted with a lot, many I have interacted with a little, and SOME I have never interacted with.
e. Those I have interacted with a lot, many I have interacted with a little, and MANY I have never interacted with.

Limit Number Friends (8-point scale from (1) 1-50 to (6) Greater than 350)
Approximately how many MySNW.com friends do you have at [name of University]?

APPENDIX B – Qualitative Coding Summary

Category/Code	Description	# of Responses
A1	There is likely little risk of harm from what others can do with this information	11
A2	I don't think much about privacy issues on Facebook, I'm not worried, I don't care	32
A3	This issue is not crucial or important	4
A4	Social networking is supposed to be in the public domain	3
A5	Privacy risks are low	1
A6	I worry but this doesn't affect my use	4
A7	The benefits of Facebook outweigh the privacy risks	6
A8	This website is like other websites in terms of privacy	1
Total A	*Low privacy risk/importance*	*62*
B1	Facebook's privacy settings help me keep private things private, they work	12
B2	I control my privacy on Facebook using privacy settings	25
B3	I control my privacy on FB by selecting the friends who can see the info	16
B4	I control content, no risky personal information is on my page	74
B5	I only use it to keep in touch with those I don't see often	2
B6	Facebook protects my information	9
Total B	*Privacy behaviors*	*138*
C!	(Potential) employer or colleague sees something bad	19
C2	(Potential) employer or colleague sees something	20
C3	Lose job or not be hired for job, lost job opportunities	32
C4	Potential for extortion	1
C5	Identity theft risk	11
Total C	*Job/financial risks*	*83*
D1	I worry that personal information is available to others, information is misused/used by others	108
D2	Facebook keeps changing privacy settings	1
D3	Information is used for marketing, advertising, or in other unauthorized ways, a concern	12
D4	Because privacy is important lack of it may be harmful	36
D5	My reputation could be harmed, others could judge me	19
D6	This issue is crucial/important, I worry about my privacy, I value my privacy	49
D7	My privacy concerns could lead to nonuse	11
D8	Facebook does not protect my information, there are ways to find it out	10
D9	I have had my privacy breached	1

Total D	*High privacy risk/importance*	*247*
E1	I trust Facebook	4
E2	I trust my friends	3
E3	I tend to trust someone/something until it gives me a reason not to	2
E4	I have never had my privacy breached/identity stolen	3
Total E	*Trust*	*12*
Total Coded Responses		542