Privacy Management Strategies: An Exploratory Cluster Analysis

Full Paper

Nancy K. Lankton
Marshall University
lankton@marshall.edu

D. Harrison McKnight
Michigan State University
mcknight@broad.msu.edu

John F. Tripp
Baylor University
john_tripp@baylor.edu

Abstract

Online privacy management research related to e-commerce mainly focuses on whether or not to disclose information. Online social networking (OSN) on the other hand, offers a broader set of privacy management strategies. However, how individuals use these OSN strategies has not yet been studied. We survey college students about a popular OSN website and four privacy management strategies: privacy setting use, limiting content disclosure, friend list variety ,and firend list size. We take an exploratory approach using cluster analysis that results in four clusters with varying combinations of privacy management strategies. The findings reveal intriguing differences among the combinations of privacy control strategies. Overall, the findings support the control portfolios approach of Kirsch. Further, we show that each cluster has unique motivations for continued OSN use. Implications for future research are discussed.

Keywords: Privacy management strategies, Facebook. Cluster analysis.

Introduction

Privacy management strategies are the actions individuals take to protect their personal information (Ellison et al. 2011; Hogan 2010). In the online realm these strategies were once limited to individuals choosing to disclose or not disclose personal information to organizations (e.g., Dinev and Hart 2006). However, in online social networking (OSN) users disclose information to more than just the organization behind the website. Information posted to one's OSN profile can be seen by many individuals. Disclosing information about oneself is necessary to benefit from online social networking (e.g., finding a new job and developing new relationships) (Ellison et al. 2011). However, sometimes this involves sharing information that one may not want to disclose to wider audiences (Ellison et al. 2011).

Fortunately, OSN websites provide users with many options to manage their personal information that can help them achieve these benefits without totally forfeiting control and privacy (Ellison et al. 2011; Stutzman and Kramer-Duffield 2010). Users can employ one or more privacy management strategies including limiting disclosures, using vendor-provided privacy settings, or managing the variety and size of their networks (Ellison et al. 2011). While many researchers investigate individual privacy management strategies (e.g., Stutzman and Kramer-Duffield 2010), other researchers suggest that individuals use a combination or portfolio of strategies to protect their personal information (Hogan 2010). This research explores OSN privacy management strategy portfolios. We investigate the following research question:

What privacy management strategy portfolios do users employ on online social networking (OSN) websites, and how do these portfolios differ in terms of individuals' privacy-related and usage-related beliefs and attitudes?

Theory

Similar to other information systems researchers (Smith et al. 2011), we take the control-based view of privacy in which general privacy is associated with control over access to the self (Altman 1975; Westin

1967). Information privacy is defined as an individual's desire to control or have some influence over personal information (Bélanger and Crossler 2011). In this view control or perceived control is not privacy *per se*, but rather a factor that can enhance one's cognitions of privacy (Smith et al. 2011).

This fits with our study because privacy management strategies can afford one with a sense of control over personal information. Dinev and Hart (2004) discuss how control over information privacy is possible through limiting self-disclosure. In an online environment, limiting self-disclosure is important. However, users have other options. In this study, we examine the privacy management strategies as described by Ellison et al. (2011): Using privacy settings (using vendor-provided privacy settings), limiting disclosure (limiting the personal information one posts on the OSN website), friend list variety (closeness of friends), and friend list size (number of friends).

Privacy management strategies on OSN websites are rather complex, partly because OSN platforms serve multiple, disparate audiences. For this reason privacy management strategies may best be seen as operating in conjunction with one another (Ellison et al. 2011). For example, Ellison et al. (2011) find a positive relationship between privacy setting use and the number of Facebook friends. They discuss how this may reflect a strategy by which users with larger friend counts need to place these friends into groups. Or it could reflect the fact that those who feel comfortable creating groups also feel more comfortable accepting different types of people as friends.

Related to the idea that privacy management strategies might work together is Kirsch's (1997) work on organizational control strategies. She examines how control modes are implemented during system development projects, and why IS and user stakeholders implement particular control mode combinations. Kirsch (1997) finds stakeholders in organizational settings implement different portfolios or combinations of control strategies that use overlapping and complementary mechanisms. For example, one IS department used formal behavioral and outcome mechanisms with informal self-control mechanisms, while another IS department used formal behavioral and outcome mechanisms with informal clan controls. This conceptualization of control is relevant to our study, because online privacy management strategies are a form of control that users exert to protect their personal information. We propose that OSN users may choose different privacy management strategies (i.e., portfolios of control) to protect their personal information on OSN websites.

In another study, Hogan (2010) identifies two possible online privacy management strategies. One is where individuals do not use privacy settings, and also do not disclose much personal information. They do not want to make decisions about who sees what information, and because of this, they do not post information that will harm their reputations. Hogan (2010) explains that in another strategy, individuals disclose a great deal of personal information, but use privacy settings to control who has access to this information. Individuals using this approach want the freedom to disclose more information. It allows them to take control of their site, place friends into groups, and be more aware of what is happening on the site. We next describe a study in which we seek to identify different privacy management strategy portfolios used on the popular OSN platform, Facebook.

Methodology

To explore OSN privacy management strategies, we collected survey data of Facebook users in Spring 2011. Participants were juniors and seniors in an information systems course required for all business majors in a large United States public university. This is an appropriate sample because Facebook originally targeted college students, and a large percent of online 18-29 year-olds are Facebook users (Duggan et al. 2015).

The survey instructions asked subjects to indicate an OSN site of which they were either currently a member or might become a member. The survey then instructed subjects to answer all remaining questions referring to that OSN site, which was labeled MySNW.com. This approach was taken because the survey was administered during class time and we wanted to be inclusive. Of the 476 respondents, we used the 396 that provided complete responses and indicated they currently use Facebook. Non-response was limited to those who did not attend class that day. Our response rate was 94% (476/505 in the course).

The questionnaire is shown in Appendix A. We examine four privacy management strategies: privacy setting use, limiting content disclosure, friend list variety, and friend list size. For privacy setting use, we presented a list of information and asked respondents who they allow to see those types of information, from everyone on Facebook to no one. These items were created based on the Facebook settings at the time of the study. We followed Hsieh et al. (2008) and used item averages for the analysis because of this construct's formative nature (an individual might use privacy settings to control who can see their contact information, but not their work information), yet the high correlations among some items. This makes theoretical sense because a higher (lower) average indicates using privacy settings to obtain more (less) privacy. The three limiting disclosure items refer to limiting content and not placing personal information on the website. We created items for the friend list variety construct with questions about who users allow to be on their friends list, from close friends and those they have interacted with a lot, to people they do not know personally or have never interacted with. This variable also includes an item that asked how exclusive their friends list is. Finally, for friend list size, we asked the respondents how many total MySNW.com (Facebook) friends they have.

To help explain individuals' privacy management strategies in terms of beliefs and attitudes toward privacy and OSN use, we also measured other privacy- and technology usage-related constructs (Table 1). We adapted most scales from previous research: privacy risk and privacy concern (Dinev and Hart 2006), trust beliefs (McKnight et al. 2002), usefulness (Venkatesh and Morris 2000), enjoyment (Venkatesh 2000), habit (Limayem and Hirt 2003), and usage continuance intentions (Venkatesh et al. 2003). All items were adapted to relate to the OSN setting. We also included gender and experience as possible privacy management strategy differentiators. We adapted most scales from previous research to relate to the OSN setting. We pilot tested most items (excluding limiting disclosure) in the same course during a previous semester and made minor adjustments to reflect additional Facebook functionality between surveys. The experience variable was created by multiplying the scores of the length and frequency items.

Construct	**Definition**
Privacy-Related Perceptions *(Privacy Calculus Model: Dinev and Hart 2006)*	
Privacy Risk	Perceptions of opportunistic behaviors that result from general others disclosing personal information on the OSN website.
Privacy Concern	Perceptions of opportunistic behaviors that result from oneself disclosing personal information on the OSN website.
Trust Beliefs	Beliefs that the website has integrity, competence, and benevolence.
Technology Usage-Related Perceptions *(Unified Theory of Acceptance and Use of Technology: Venkatesh et al. 2012)*	
Usefulness	Belief about the utility of using the website
Enjoyment	Belief that using the website is enjoyable in its own right, apart from any performance consequences that are incurred
Habit	Belief that one's tendency to use the website is automatic because of learning
Continuance Intention	Intention to continue using the website beyond initial acceptance

Table 1. Privacy- and Technology Usage-Related Constructs

Data Analysis

Before analyzing the clusters, we used PLS (XLStat PLSPM) to test construct convergent and discriminant validity. Dillon-Goldstein's rho, Cronbach's alpha, average variance extracted (AVE), PLS loadings and cross-loadings, and inter-correlations compared to square roots of the AVEs are all in the recommended ranges (Fornell and Larcker 1981; Gefen and Straub 2005; Nunnally and Bernstein 1994; Vinzi et al. 2010), with the exception of the Cronbach's alpha for friend list variety (at .68—close to the .70 standard). We did not drop this construct from this study because it had an adequate Dillon-Goldstein rho (.82) that also measures reliability.

Multicollinearity is also not a problem because the highest variance inflation factor is 2.33, which is well below the suggested cutoff of 5.00 (Menard, 1995). Also, no variable has a condition index above 30 and has two variance decomposition proportions greater than .50 (Belsley et al. 1980). Common method variance was also not a major problem because the Harman's single-factor test (Podsakoff et al. 2003) revealed that the first of the fifteen factors did not explain a majority of the variance explained (only 25% of the 83% explained).

We used a two-stage cluster analysis using both hierarchical and non-hierarchical methods to explore the privacy management strategies (Balijepally et al. 2011; Miranda and Kim 2006). Experts recommend using hierarchical and non-hierarchical methods in tandem to counter the inherent limitations of each method—hierarchical algorithms help identify the number of clusters and cluster centroids, which are then used as starting points for non-hierarchical procedures (Balijepally et al. 2011). We first performed a hierarchical cluster analysis in SPSS using Ward's method with the standardized values of the four privacy management strategy constructs. Using standardized values can correct for differences in construct scales (Blijepally et al. 2011). To determine the number of clusters we examined the resulting agglomeration schedule stage for which there was a large distance between clusters. We also calculated the variance ratio criterion (Calinski and Harabasz 1974). Both methods indicated that a four-cluster solution was the most appropriate. We then obtained the cluster centers for the four-cluster solution, following Mooi and Sarstedt (2011, pages 274-276), and used them as the initial cluster centers in a non-hierarchical k-means cluster analysis. Table 2 depicts the sample sizes and privacy management strategy means for each cluster. After determining the clusters, we calculated the means of the other variables by cluster (Table 3). We ran Tukey post-hoc multiple comparison tests to determine what means significantly differ by cluster (Tables 2 and 3).

Privacy Management Strategy	**Total All Clusters**	**Cluster Number**				**Tukey Post-Hoc Multiple Comparison Test p-values**					
		1	**2**	**3**	**4**						
Sample Size	396	81	122	127	66	1&2	1&3	1&4	2&3	2&4	3&4
Privacy Setting Use	2.77	2.69 Med	2.95 Med-High	3.12 High	1.89 Low	**.004**	**.000**	**.000**	.080	**.000**	**.000**
Limiting Disclosures	5.33	4.91 Med	4.41 Low	6.29 High	5.69 Med-High	**.000**	**.000**	**.000**	**.000**	**.000**	**.000**
Friend List Variety	2.87	2.70 Low	3.04 High	2.61 Low	3.25 High	**.001**	.751	**.000**	**.000**	.133	**.000**
Friend List Size	6.01	3.67 Low	6.77 High	6.41 Med	6.71 Med-High	**.000**	**.000**	**.000**	**.007**	.971	.104

Table 2. Privacy Management Strategy Means by Cluster

Discussion

The clusters are such that within groups, respondents answered the privacy management strategy questions in much the same way. Cluster 1 has the lowest number of friends of all the clusters as indicated by a significantly lower friend list size (Table 2). It is also one of the two clusters with lower friend list variety meaning they have more close friends on their friend list than the other clusters. The individuals in this cluster thus have smaller, more tight-knit networks. They are also at a medium level for limiting content and using privacy settings. They probably do not limit disclosures more or use privacy settings more because with a smaller friend list size that is more apt to be close friends they are not concerned about who sees what information.

Cluster 1 is also lower on many of the other variable means (Table 3). Their lower experience and habit mean could mean they are newer to Facebook than those in the other clusters. Combined with the above results, they could have recently started using the OSN website to communicate with close friends. In turn, they may perceive lower privacy concerns because of their choice of friends. However, because they have more close friends on their friend list they may not have access to the bridging social capital benefits associated with having a more diverse friend list with weaker acquaintances (Ellison et al. 2011). This

Variables	Total All Clusters	Cluster Number				Tukey Post-Hoc Multiple Comparison Test p-values					
		1	2	3	4						
Sample Size	396	81	122	127	66	1&2	1&3	1&4	2&3	2&4	3&4
Privacy Concern	4.92	4.71 Low	4.90 Low-Med	5.24 Med-High	4.56 Low	.831	**.041**	.837	.182	.322	**.004**
Privacy Risk	5.01	4.79	4.85	5.21	5.17	.985	.056	.207	.071	.281	.995
Trust Beliefs: Integrity	4.64	4.56	3.52	4.68	4.87	.996	.902	.400	.740	.229	,711
Trust Beliefs: Competence	6.04	5.79 Low	5.84 Low	6.22 High	6.36 High	.982	**.010**	**.003**	**.012**	**.003**	.790
Trust Beliefs: Benevolence	4.19	4.09	4.26	4.08	4.39	.798	1.00	.520	.681	.923	.401
Usefulness	5.46	5.14 Low	5.36 Low-Med	5.63 Med-High	5.69 Med-High	.348	**.001**	**.002**	.085	.075	.967
Enjoyment	5.77	5.46 Med	5.33 Low-Med	5.69 Med-High	5.97 High	**.028**	**.000**	**.000**	.075	**.020**	.806
Habit	5.49	4.77 Low	5.56 High	5.77 High	5.70 High	**.000**	**.000**	**.000**	.497	.860	.981
Continuance Intention	5.92	5.48 Low-Med	5.85 Med-High	6.07 Med-High	6.29 High	.082	**.001**	**.000**	.389	**.041**	.531
Experience	27.20	20.40 Low	29.13 High	29.27 High	27.98 High	**.000**	**.000**	**.000**	.999	.809	.746
Gender	37% F 63% M	28% F 73% M	32% F 68% M	52% F 48% M	33% F 67% M	Using a chi-square crosstabs analysis, clusters 1, 2, and 4 do not differ significantly from each other at the p < .05 level					

Table 3. Other Variable Means by Cluster

could explain their lower enjoyment and usefulness of the site, which could also make them less likely to want to continue using it. Given these results we label this cluster the "secure, but less committed" cluster.

Table 2 shows that Cluster 2 is one of the two clusters with the highest mean friend list size and friend list variety. Cluster 2 also discloses the most, but uses privacy settings at a medium to high level. This represents the group discussed by Hogan (2010) that discloses a great deal of personal information, but uses privacy settings to control who has access to this information.

Similar to Cluster 1, Cluster 2 is lower on many of the other variables including privacy concern, competence, usefulness, and enjoyment (Table 3). It appears that despite the higher number of friends, individuals in this cluster may have lower privacy concerns because they use privacy settings more. They could be using the privacy settings more at least partly because their trust in the website's competence is low. Das and Teng (1998) argue that control is an alternative mechanism to trust. For Cluster 2 respondents, the control offered by using privacy settings could be taking the place of trust in the OSN website. Enjoyment and usefulness are also lower, which could be the result of using privacy settings more, which may be cognitively unmanageable for some individuals (Hogan 2010). Previous research findings support that users have misunderstandings or confusion relating to privacy setting use (O'Brien and Torres 2012). This could decrease perceived usefulness and enjoyment, especially if privacy setting use is critical to keeping their comparatively higher amount of disclosures private.

Unlike Cluster 1, Cluster 2 is more like the other clusters because it has higher habit and experience (Table 3). For these individuals, site use has become more of a habit, possibly through repeated experiences. However, this higher experience and habit coupled with lower usefulness and enjoyment, and only medium continuance intention might indicate that perhaps the "novelty" of Facebook has worn off over time. We call Cluster 2, the "bored but confident in privacy setting use" cluster.

Cluster 3, while having a medium friend list size as compared to the other clusters, is otherwise the most private. Individuals in this cluster have more close friends (i.e., lower friend list variety, similar to Cluster 1), limit disclosures the most, and use privacy settings the most. They have comparatively high means for all the other variables. They have the highest privacy concerns, which corresponds to their privacy management— limit disclosure and use privacy settings—strategies. They also differ from the other clusters in that there are an equal number of males and females. The other clusters all have more males than females. This is consistent with prior research that finds women are generally more concerned about

privacy than men (Sheehan 1999), are significantly less likely than men to take risks, and are more concerned with the consequences of sharing identity information (Fogul and Nehmad 2009). We label Cluster 3 the "privacy concerned and dual-controlling" cluster.

Cluster 4 has a higher friend list size, in addition to having the highest friend list variety. Thus, they have a lot of friends and many of these friends are acquaintances or people they do not know. Our findings show that they take almost an opposite approach to managing a large friend list to that of Cluster 2. Instead of disclosing a lot and using privacy settings to keep their personal information private, they limit their disclosures and use privacy settings less (Table 2). In fact, Cluster 4 is the least restrictive of all the clusters in terms of using privacy settings. This group takes more of the "lowest common denominator" approach discussed by Hogan (2010) where they do not want to use privacy settings as much, and instead limit content to what they feel is appropriate for all audiences. Similar to Cluster 2, Cluster 4 has lower privacy concerns. Unlike Cluster 2, but similar to Cluster 3, they have higher trusting beliefs in the website's competence, which could account for their being less likely to use privacy settings. Also similar to Cluster 3, they have high usefulness, enjoyment, habit, and continuance intention. This indicates they perceive many more benefits from using the OSN website. This is what we call the "limiting disclosures has benefits" cluster.

Research Implications, Limitations, and Conclusion

This study is one of the first to examine the portfolios of users' privacy management strategies, and the perceptions and characteristics of users employing each portfolio. We find four privacy management strategy clusters, ranging from a very private strategy employed by active users (Cluster 3—"privacy concerned and dual-controlling") to a medium privacy management strategy employed by newer, less active users (Cluster 1—"secure, but less committed"). Other users with a higher number, and medium to high variety of friends use privacy settings more without limiting disclosures (Cluster 2—"bored but confident in privacy setting use"), or limited disclosures more, while not using privacy settings as much (Cluster 4—"limiting disclosures has benefits"). These last two strategies mirror the tradeoffs of privacy setting use and information disclosure discussed by Hogan (2010).

This study has several implications for future research. First, future research can further investigate why users in the different clusters choose those privacy management strategies. For example, Kirsch (1997) discusses how different controls may be used for different purposes, e.g., task outcomes or relationship building. Future research could correlate these clusters with users' motivations for using OSN. It may be that users in Cluster 3 who are the most private, yet have a lot of friends, use the OSN website for not only staying in touch with close friends, but also for monitoring what other acquaintances are doing.

Future research can also continue to explore other privacy management strategies. Some strategies we did not investigate are interpersonal privacy behaviors like wall management, or asking a friend to untag a photo (Stutzman and Kramer-Duffield 2010). Combining these strategies with those we examined may lead to new clusters with different characteristics, and different usage-related perceptions and continuance intention. Further, as OSN websites expand and alter privacy settings this research should be updated. For example, in 2014, Facebook announced new privacy control tools for mobile app users, including the ability to log in anonymously for the first time (http://www.pcmag.com/article2/0,2817,2457389,00.asp).

Finally, this exploratory research can be extended to confirmatory work that develops theory and hypotheses for the various privacy management strategies. While our study finds some consistency with strategies discussed in prior research (Ellison et al. 2011; Hogan 2010) work can be done to extend this to other data sets and other theoretical bases. Further, a theoretical model can be analyzed that includes the privacy management strategies as model constructs. Predictions can be made about how the model results may differ among clusters.

Our study has limitations. The sample is limited to college students. While many OSN users are college-aged, the study should be performed with older adults and/or those with full-time employment who may have different perceptions and privacy management strategies. There were also more males than females in our study, whereas more women than men are members of social networking websites

(http://www.pewresearch.org/fact-tank/2015/08/28/men-catch-up-with-women-on-overall-social-media-use/). While this could make our results less generalizable, Cluster 3 did tease out privacy management strategies relating to a group with more women than men. Another limitation is there might be many ways to measure privacy behaviors. While we measured limiting disclosures by asking respondents how much they limit content, it could be also measured by asking what specific content they limit. Finally, we used a subjective measure of privacy management strategies, and not actual privacy behaviors, which could differ. Future research can explore these issues.

In conclusion, this study, while exploratory in nature, provides insight into how users manage their personal information on OSN websites. It uses a sound methodology and finds clusters that are somewhat consistent with prior research (Ellison et al. 2011; Hogan 2010). However, it expands these discussions by showing additional strategies and by explaining them using both privacy- and technology usage-related perceptions. This research is important for expanding our understanding of privacy management strategies. It also provides many future research opportunities.

References

Altman, I. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*, Monterey, CA: Brooks/Cole Publishing.

Balijepally, V., Mangalaraj, G., and Iyengar, K. 2011. 'Are We Wielding this Hammer Correctly? A Reflective Review of the Application of Cluster Analysis in Information Systems Research," *Journal of the Association for Information Systems* (12:5), pp. 375-413.

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp. 1017-1041.

Belsley, D.A., Kuh, E., Welsch, R.E., 1980. *Regression Diagnostics: Identifying Influential Data and Sources of Collinearity,* New York: John Wiley & Sons.

Brooks, L., and Anene, V. 2012. "Informational Disclosure and Generational Differences in Social Network Sites," in *Proceedings of the Americas Conference on Information Systems (AMCIS)*.

Calinski, T., and Harabasz, J. 1974. "A Dendrite Method for Cluster Analysis," *Communications in Statistics – Theory and Methods* (3:1), pp. 1-27.

Das, T. K., and Teng, B. 2004. "The Risk-Based View of Trust: A Conceptual Framework," Journal of Business and Psychology (19:1), pp. 85-116.

Dinev, T., and Hart, P. 2004. "Internet Privacy Concerns and their Antecedents: Measurement Validity and a Regression Model," *Behaviour & Information Technology* (23:6), pp. 413-422.

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

Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A., Madden, M. 2015. "Social Media Update 2014," Pew Research Center, available at: http://www.pewinternet.org/2015/01/09/social-media-update-2014/

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., and Lampe, C. 2011. "Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment," in *Privacy Online*, S. Trepte, and L. Reinecke (eds.), Berlin Heidelberg: Springer-Verlag, pp. 19-32.

Fogel, J., and Nehmad, E. 2009. "Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns. Computers in Human Behavior, (25:1), pp. 153-160.

Fornell, C., and Larcker, D.F., 1981. "Evaluating Structural Equations with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (18:1), pp. 39-50.

Gefen, D., and Straub, D., 2005. "A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example," *Communications of the Association for Information Systems* (16:5), pp. 91-109.

Hogan, B. 2010. "The Presentation of Self in the Age of Social Media: Distinguishing Performances and Exhibitions Online," *Bulletin of Science, Technology & Society* (30:6), pp. 377-386.

Hsieh, J. P.-A., Rai, A., and Keil, M. 2008. "Understanding Digital Inequality: Comparing Continued Use Behavioral Models of the Socio-Economically Advantaged and Disadvantaged," *MIS Quarterly* (32:1), pp. 97–126

Kirsch, L. J. 1997. "Portfolios of Control Modes and IS Project Management," *Information Systems Research* (8:3), pp. 215-239.

Limayem, M., and Hirt, S. G. 2003. "Force of Habit and Information Systems Usage: Theory and Initial Validation," *Journal of the Association for Information Systems* (4:1), pp. 65-97.

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

Menard, S., 1995. *Applied Logistic Regression Analysis,* Sage University Series on Quantitative Applications in the Social Science, Thousand Oaks, CA: Sage.

Miranda, S. M., and Kim, Y. M. 2006. "Professional versus Political Contexts: Institutional Mitigation and the Transaction Cost Heuristic in Information Systems Outsourcing," *MIS Quarterly 30*(3), pp. 725-753.

Mooi, E., and Sarstedt, M. 2011. *A Concise Guide to Market Research,* Heidelberg: Springer.

Nunnally, J.C., and Bernstein, I.H., 1994. *Psychometric Theory*, 3rd ed. New York: McGraw-Hill.

O'Brien, D., and Torres, A. M. 2012. "Social Networking and Online Privacy: Facebook Users' Perceptions," *Irish Journal of Management* (31L2), pp. 63-97.

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

Sheehan, K. B. 1999. "An Investigation of Gender Differences in On-Line Privacy Concerns and Resultant Behavior," *Journal of Interactive Marketing* (13:4), pp. 24-38.

Smith, H. J., Dinev, T., and Xu H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly*, (35:4), pp. 989-1015.

Stutzman, F., and Kramer-Duffield, J. 2010. "Friends Only: Examining a Privacy-Enhancing Behavior in Facebook," in *Proceedings of CHI Privacy*, Atlanta, GA.

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), pp. 342-365.

Venkatesh, V., and Morris, M. 2000. "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), pp. 115-139.

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), pp. 425-478.

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), pp. 157-178.

Vinzi, V.E., Trinchera, L., and Amato, S., 2010. "PLS Path Modeling: From Foundations to Recent Developments and Open Issues for Model Assessment and Improvement," in *Handbook of Partial Least Squares: Concepts, Methods, and Applications*, Vinzi, V. E., Chin, W.W., Henseler, J., Wang, H. (eds.), Springer, Heidelberg, pp. 47-82.

Westin, A. F. 1967. *Privacy and Freedom*, New York: Atheneum.

APPENDIX A - MEASUREMENT ITEMS

Privacy Setting Use (5-point Likert (1) Everyone on SNW.com, (2) Friends of Friends, (3) Only Friends, (4) Customize (specific people), (5) No One)

Who do you allow to see the following types of information?

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
8. Your status, photos, and posts
9. Places you check into

Limitung Disclosures (7-point Likert from (1) Strongly Disagree to (7) Strongly Agree)

1. I limit the content I place on MySNW.com.
2. I don't place things on MySNW.com that I don't want others to see.
3. I do not have very personal information on my MySNW.com account.

Friend List Variety

1. MySNW.com Friend List consists of the following (pick one):
   a. Very close friends only
   b. Very close friends and those I know personally
   c. Very close friends, those I know personally, and SOME I do not know personally.
   d. Very close friends, those I know personally, and MANY I do not know personally.
2. How exclusive (i.e., limited selective) is your list of MySNW.com friends? (5-point Likert from (1) Very Exclusive to (5) Not at All Exclusive)
3. 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.

Friend List Size (8-point scale from (1) 1-50 to (8) Greater than 1,000)

1. Approximately how many total MySNW.com friends do you have?

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 Beliefs: Integrity (7-point Likert from (1) Strongly Disagree to (7) Strongly Agree)
1. MySNW.com is truthful in its dealings with me.
2. MySNW.com is honest.
3. MySNW.com keeps its commitments.

Trust Beliefs: Competence (7-point Likert from (1) Strongly Disagree to (7) Strongly Agree)
1. MYSNW.com is competent and effective in providing online social networking.
2. MySNW.com performs the role of facilitating online social networking very well.
3. MySNW.com is a capable and proficient online social networking provider.

Trust Beliefs: Benevolence (7-point Likert from (1) Strongly Disagree to (7) Strongly Agree)
1. MySNW.com acts in my best interest.
2. MySNW.com does its best to help me if I need help.
3. MySNW.com is interested in my well-being, not just its own.

Usefulness (7-point Likert 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 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.

Habit (7-point Likert from (1) Strongly Disagree to (7) Strongly Agree)
1. The use of MySNW.com has become a habit for me.
2. Using MySNW.com is natural for me.
3. I don't even think twice before using MySNW.com.
4. Using MySNW.com has become automatic to me.
5. When faced with a particular task, using MySNW.com is an obvious choice for me. *Dropped*

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.

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.