# Abandon Online Social Networking Services? A Trade-off Analysis

*Research-in-Progress*

**Yong Chen**
Old Dominion University
y7chen@odu.edu

## Abstract

As online social networking services (OSNS) become more and more ubiquitous, users are more likely to become targets and/or victims of cybercrimes, simply because they need to disclose personal information if they use OSNS. Should they continue using OSNS? By adopting the Utility Maximization Theory (UMT) as a theoretical lens to provide a research model, this paper identifies the benefits and costs that users need to balance in order to make their decision about whether or not to continue using OSNS. The benefits that users can get from OSNS include Perceived Usefulness and Perceived Enjoyment. The costs include Privacy Concerns and Previous Privacy Invasion Experiences. This paper proposes that users' Perceived Usefulness and Perceived Enjoyment positively influence their intention to continue using OSNS, whereas their Privacy Concerns and Previous Privacy Invasion Experiences negatively influence their intention to continue using OSNS. When they perceive that the benefits are larger than the costs, users tend to continue using OSNS, and vice versa.

### Keywords

Online social networking, privacy concern, utility maximization theory, perceived usefulness, perceived enjoyment, previous privacy invasion.

## Introduction

Online social networking services (OSNS) are popular Web 2.0 applications. They are "an integrative collection of telecommunications and computer networking technologies that allow users to build online, social, hedonic-oriented experiences by maintaining network resources within communities of individuals and sharing connections and interests with others" (Hu, Poston, & Kettinger, 2011, p. 442). To date, popular OSNS include Facebook, Twitter, and LinkedIn. Providing users with a level of unprecedentedly convenient platforms on which to keep in touch, to develop relationships, and to create social capital is a source of the OSNS' public value and their important contribution to modern society (Koroleva, Krasnova, Veltri, & Günther, 2011; Krasnova, Veltri, & Günther, 2012). OSNS serve as platforms that allow users to build and share ideas, thoughts, and experiences, even as users gain online, social, hedonic-oriented benefits (Ellision, 2007; Hu, Poston, & Kettinger, 2011). On these platforms, users build their profiles, which include their personal information, and then they present themselves publicly to meet their personal goals. For example, Facebook allows users to keep up with friends by sharing thoughts, by uploading photos and videos, and by posting links of web pages of interest (Xu, Benbasat, & Cavusoglu, 2012). OSNS are an easy and entertaining way for users not only to keep in contact with people they already know (e.g., their friends and family members), but also to meet new people who share common interests with them (Gibbs, Ellison, & Heino, 2006; Marett, McNab, & Harris, 2011; Valkenburg, Peter, & Schouten, 2006). Although many OSNS users make their personal information available to others just for the enjoyment of social acknowledgement (e.g., posting one's birth date in order to receive well-wishes from friends) (Ellison, 2007; Marett, McNab, & Harris, 2011), it is not surprising that this private information can become a prime target for online predators and troublemakers.

Scholars, privacy advocates, and the media have raised concerns about the risks associated with the disclosure of personal information in OSNS (Barnes, 2006; Govani & Pashely, 2005; Gross & Acquisti, 2005; Young & Quan-Haase, 2009). Kaspersky Lab reports that Facebook was the No. 4 most targeted

site by phishers during the first quarter of 2010 (Richmond, 2010). Consumer Reports' State of the Net survey released in May 2010 points out that 9% of OSNS users experienced some form of abuse within the past year (e.g., malware infections, scams, identity theft or harassment) (Woollacott, 2010). Twitter users have been targeted by cyber-criminals who link malware with current topics tags (Voigt, 2009).

These reports raise OSNS users', providers', and lawmakers' concerns about privacy. In reaction to growing online privacy concerns, Facebook has offered new IT features, such as "choose your audience" and "view as", to protect its users' privacy (Xu, Benbasat, & Cavusoglu, 2012). In the U.S., the Commercial Privacy Bill of Rights Act of 2011 was introduced to protect consumers' privacy, both online and offline (Zhang, Wang, & Xu, 2011). Despite the efforts of OSNS providers and lawmakers, OSNS users' privacy cannot be completely safeguarded unless users choose carefully with whom they choose to communicate and what information to post about themselves on their personal profiles (Marett, McNab, & Harris, 2011). Criddle (2006) advises OSNS users to seriously consider the risks before sharing their entire names, friends' and family members' names, home addresses, phone numbers, or the locations of where one might go to school or work.

Interestingly, the increasing privacy concerns from OSNS users, providers, and lawmakers have not hindered the blooming of OSNS at all. In recent years, OSNS have grown rapidly. For instance, the number of Facebook users reached one billion in October 2012 (Smith, Laurie, & Stacy, 2012). It is reasonable to expect that OSNS will remain popular around the world for the foreseeable future (Marett, McNab, & Harris, 2011). This leads to the following research question:

What motivates people to use OSNS despite news stories, warnings, and even legislation about privacy? And further, do previous privacy invasion experiences influence users to discontinue using OSNS?

The purpose of this paper is to investigate whether privacy concerns and/or previous privacy invasion experiences influence users' intentions to continue to use OSNS. Many articles focus on the consequences/impacts of privacy concerns and have treated the construct of privacy concerns as an antecedent to various behavior-related variables (Xu, Dinev, Smith, & Hart, 2011). Some scholars apply specific theories to the study of online social networking privacy issues. For example, Marett, McNab, and Harris (2011) applied Protection Motivation Theory to identify the perceptions and beliefs held by users that influence their responses to the imposed threats. Hu, Poston, and Kettinger (2011) incorporated Status Quo Bias theory into the well-established Technology Acceptance Model in order to analyze OSNS nonadopters. Xu, Dinev, Smith, and Hart (2011) developed an information privacy research model based on Communication Privacy Management theory. Unlike the explorations in previous studies, this paper explores how OSNS users' privacy concerns and previous privacy invasion experiences impact their intention to continue using OSNS. Although Jung, McKnight, Jung, and Lankton (2011) did a similar study and found that there was no direct effect or mediation effect of privacy concerns on users' intention to use OSNS, their study did not take users' previous privacy invasion experiences into consideration.

The main contributions of this paper are these: (1) it embeds users' previous privacy invasion experiences into the analysis of their decision whether or not to continue using OSNS; and (2) it applies benefits appraisal and cost appraisal in the users' decision-making process. Previous studies (e.g., Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1973; Yoo, Ahn, & Rao, 2012) either choose users' previous privacy invasion experiences as a factor for other research topics, or treat each benefit factor and cost factor separately as independent variables to find the relations between them and the dependent variables in their research. This paper aims to explore the reasons why users continue using OSNS from a new angle.

The rest of this paper is organized in this manner: first, Utility Maximization Theory is reviewed and then a research model, tailored to users' intention to continue using OSNS, balancing the perceived benefits and perceived costs, is presented. Next, a set of propositions is developed. This paper concludes with a discussion and directions for future research.

## Theoretical Foundations

OSNS require users to disclose personal information, to some extent. In other words, if users want to use OSNS, they run the risk of possible damage to their privacy. What motivates them to use OSNS? Gross and Acquisti (2005) list the following possible reasons: "(1) the perceived benefit of selectively revealing data to strangers may appear larger than the perceived costs of possible privacy invasions; (2) peer

pressures and herding behavior; (3) relaxed attitudes towards (or lack of interest in) personal privacy; (4) incomplete information (about the possible privacy implications of information revelation); (5) faith in the networking service or trust in its members; (6) myopic evaluation of privacy risks" (p73). This paper focuses on the first reason and goes deeper by analyzing to what extent the tradeoff of perceived benefits and perceived costs impacts users' decision-making about continuing the use OSNS, based on the Utility Maximization Theory (UMT). The other reasons are not discussed in this paper, not because this paper does not agree with them but because they are beyond the scope of this paper.

UMT is a concept from the field of economics which notes that, when making a purchase decision, consumers try to get the maximum attainable benefit from what they spend (Krishnamurthi & Raj, 1988). UMT indicates that driven by the intent to advance their self-interests (McFadden, 2002), consumers make purchase decisions to maximize their utility subject to their budget constraints, and consumers' demands for different goods or services depend upon their prices (Handy, 2005). UMT is built based on the following assumptions: (1) consumers are economically rational; (2) their budgets are limited; (3) their preferences for certain goods or services are clear; (4) goods or services have prices. Although it is an economics concept, UMT has been applied in the information technology domain in recent studies (e.g., Awad & Krishnan, 2006; Jorgenson & Stiroh, 1999; Samadi, Mohsenian-Rad, Schober, Wong, & Jatskevich, 2010). As Awad and Krishnan (2006) point out, although UMT has weaknesses when it is applied to information exchange analysis, it can be used to study the tradeoff between the use of personal information against the potential negative consequences of disseminating personal information. Awad and Krishnan (2006) also argue that the equation Function U(X) = Benefit - Cost can be used to examine this tradeoff, based on UMT.

In the context of OSNS, users' benefits are derived through the degree of their personal goals realized, and their costs are a function of their privacy concerns, previous privacy invasion experiences, and user-rated importance of information transparency and privacy policies (Awad & Krishnan, 2006). More specifically, their benefits consist of their perceived usefulness (Hu, Poston, & Kettinger, 2011; Qin, Kim, Hsu, & Tan, 2011) and their perceived enjoyment (Hu, Poston, & Kettinger, 2011) regarding using OSNS, while their costs include their privacy concerns (Zhang, Wang, & Xu, 2011), previous privacy invasion experiences (Awad & Krishnan, 2006; Yoo, Ahn, & Rao, 2012), and user-rated importance of information transparency and privacy policies (Awad & Krishnan, 2006). According to UMT, OSNS users tend to get maximal benefits with minimal costs when they choose to continue or to stop using OSNS. In other words, users will appraise their benefits and costs first, and then compare these two.

## *Benefit Appraisal*

This section examines the benefits that users get from OSNS. From the users' perspective, benefits are appraised by perceived usefulness and perceived enjoyment.

### Perceived Usefulness

Perceived usefulness is "the extent to which the focal technology is useful in enhancing individuals' social sharing needs" (Hu, Poston, & Kettinger, 2011). According to Davis, Bagozzi, and Warshaw (1989), the usefulness of information technology is an important antecedent for people considering IT use. Qin, Kim, Hsu, & Tan (2011) prove that users' perceived usefulness, which is indicated by subjective norm and critical mass, has a significant positive influence on their intent to use OSNS. This paper argues that, other than subjective norm and critical mass, if users perceive that OSNS would be useful and productive in improving their online social networks with people and their performance in social sharing, they will continue to use OSNS. This leads to the following proposition:

Proposition 1: Perceived usefulness will positively influence users' intention to continue to use OSNS.

### Perceived Enjoyment

Perceived enjoyment refers to "individuals' perception of pleasure and enjoyment when using OSNS" (Hu, Poston, & Kettinger, 2011). The main functions of OSNS are supporting, capturing, and sharing individuals' experiences when using online social activities (Csikszentmihalyi, Kolo, & Baur, 2004; Hu, Poston, & Kettinger, 2011; Thambusamy, Church, Nemati, & Barrick, J., 2010). Online interactions

offered by OSNS can be novel, exciting, interesting, and intriguing (Ellison, 2007; Hu, Poston, & Kettinger, 2011). Users choose OSNS for enjoyable, social, hedonic-oriented benefits (Hu, Poston, & Kettinger, 2011). Therefore, this paper proposes:

Proposition 2: Perceived enjoyment will positively influence users' intention to continue to use OSNS.

## *Cost Appraisal*

This section examines the costs that users have to pay for their use of OSNS. Prior studies (Awad & Krishnan, 2006; Yoo, Ahn, & Rao, 2012; Zhang, Wang, & Xu, 2011) have indicated that the costs include privacy concerns, previous privacy invasion experiences, user-rated importance of information transparency, and privacy policies. Since user-rated importance of information transparency and privacy policies have been studied intensively in Awad and Krishnan (2006), this paper will not cover them. Instead, this paper will concern itself with the privacy concerns and previous privacy invasion experiences of users of OSNS.

### Privacy Concerns

OSNS users expose themselves to security risks, reputation and credibility risks, and profiling risks (Aimeur, Gambs, & Ho, 2010). Because they are making a large amount of their personal information public, they are very likely to encounter cybercrimes, such as identity theft, phishing, scams, and predators. In addition, third party applications (e.g. games on Facebook) pose a great security risk to users. Among the age group of OSNS users, young teenagers are online predators' main targets and are the main victims of online attack and cyber bulling. Aimeur, Gambs, and Ho (2010) also point out that, with the blooming of OSNS, a user's online reputation is extended beyond the Internet. If a user's reputation is damaged in OSNS, this will affect his/her credibility in real life. As more and more employers choose OSNS to screen potential employees, OSNS users may lose job opportunities because of the inappropriate information posted on their profiles. What's more, companies collect information from customers to build comprehensive profiles on individuals. OSNS are their main resources to get customer information; based on what they learn, they can improve their customer relations management systems and sell products more easily to their target markets (Aimeur, Gambs, & Ho, 2010).

Privacy concerns refer to "an individual's subjective views of fairness in losing the ability to control his/her virtual territorial, factual, interactional, and psychological privacy" (Zhang, Wang, & Xu, 2011). Many scholars argue that privacy concerns are general concerns that reflect individuals' inherent worries about possible loss of information privacy (Malhotra, Kim, & Agarwal, 2004; Smith, Milberg, & Burke, 1996; Xu, Dinev, Smith, & Hart, 2011). From an emphasis on conceptualization, Xu, Dinev, Smith, and Hart (2011) define privacy concerns as "consumers' concerns about possible loss of privacy as a result of information disclosure to a specific external agent."

Yoo, Ahn, and Rao (2012) argue that privacy concerns by themselves do not fully explain behavioral intention. They conclude that "privacy concerns themselves do not show a direct influence on the discontinuance of service use even in privacy invasion situations." The relationship between users' privacy concerns and users' intention to continue using OSNS is proposed as following: Users need to balance benefits and cost, and then decide whether they will continue to use OSNS. However, this paper does not treat privacy concerns as an independent factor in users' decision-making processes.

Proposition 3: Privacy concerns will negatively influence users' intention to continue to use OSNS.

### Previous Privacy Invasion Experiences

Individuals' previous experiences will shape their concerns about information sharing (Awad & Krishnan, 2006). Privacy invasion is a critical factor in provoking actual behavior related to information privacy (Yoo, Ahn, & Rao, 2012). Fishbein and Ajzen (1973) argue that knowledge gained from past behavior helps to shape behavioral intention. The reasons are: (1) experience makes knowledge more accessible in memory; and (2) past experience may make low probability events more salient, ensuring that they are accounted for in the formation of intentions (Ajzen & Fishbein, 1980). Repeated privacy invasion increases users' privacy concerns (Awad & Krishnan, 2006; Yoo, Ahn, & Rao, 2012). When a privacy

invasion incident happens, victims perceive and evaluate the risk caused by the incident. Yoo, Ahn, and Rao (2012) conclude that repeated privacy invasion experiences make individuals extremely sensitive to information privacy threats and that, as a result, users show more information privacy concerns, but users still have a willingness to use certain services. This leads to the following proposition:

Proposition 4: Previous privacy invasion experiences will negatively influence users' intention to continue to use OSNS.

### *The Trade-off*

The above propositions argue that OSNS users' intentions to continue to use OSNS are impacted by their Perceived Usefulness, Perceived Enjoyment, Privacy Concerns, and Previous Privacy Invasion Experiences. These positive and negative impacts influence users simultaneously. If OSNS users perceive that the overall benefit of their privacy disclosure is greater than the assessed risk of disclosure, OSNS users will disclose personal information as the cost for using OSNS (Culnan & Bies, 2003; Jung, McKnight, Jung, & Lankton, 2011). In addition, Gross and Acquisti (2005) point out that OSNS users choose OSNS because their perceived benefit of selectively revealing data to strangers may appear larger than their perception of the costs of possible privacy invasions. This paper agrees with this argument. In particular, this paper argues that OSNS users' perceived benefits include their Perceived Usefulness and Perceived Enjoyment while their perceived costs include their Privacy Concerns and Previous Privacy Invasion Experiences. According to UMT theory, after OSNS users conduct the benefit and cost appraisal, if their perceived benefits are bigger than their perceived costs, those users are likely to continue using OSNS, and vice versa. In other words, their intention is dependent upon the result of the trade-off. Therefore, this paper proposes the following propositions:

Proposition 5a: When users perceive the benefits to be larger than the costs, they tend to continue to use OSNS.

Proposition 5b: When users perceive the costs to be larger than the benefits, they tend to stop using OSNS.

### *Research Model*

In summary, this paper expects that the adoption of UMT via benefit and cost appraisal will yield a better perspective on the determinants of users' intention to continue using OSNS. The relationships among constructs include perceived usefulness, perceived enjoyment, privacy concerns, and previous privacy invasion experiences. Figure 1 shows the research model.

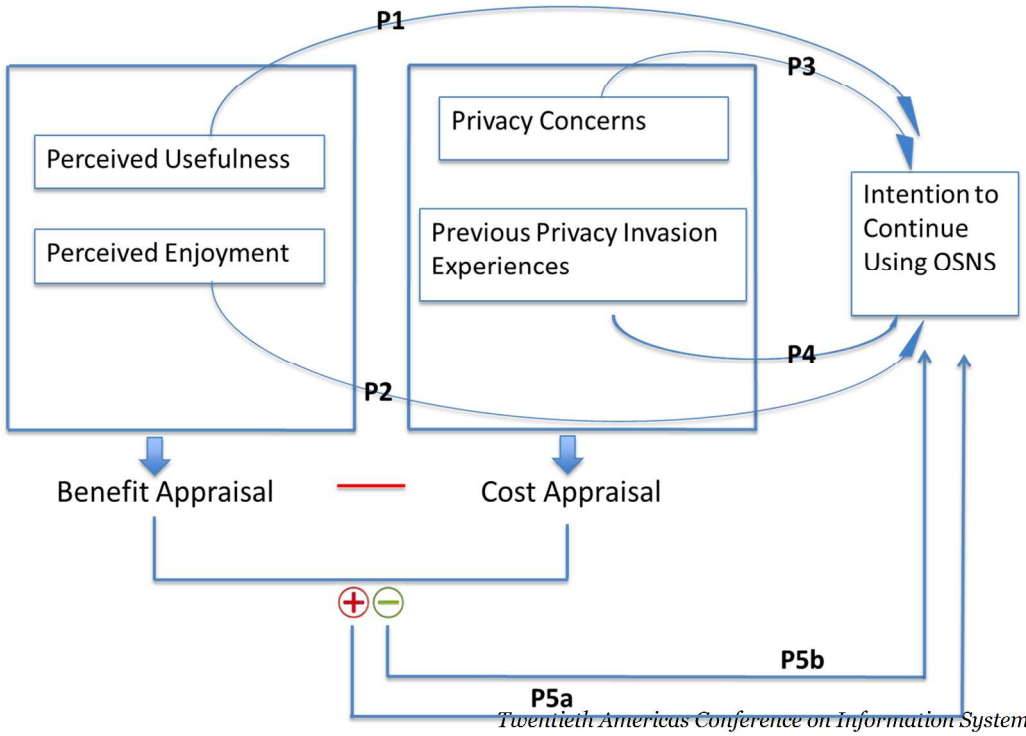

**Figure 1 Factors impacting users' intention to continue using OSNS**

## Discussion and Conclusion

OSNS contribute to modern society by providing unprecedentedly convenient platforms for users to keep in touch, to develop relationships, and to create social capital. Many users are attracted by the huge benefits offered by OSNS. However, these benefits require their private information. While they enjoy the social acknowledgements of using OSNS, users run the risk of leaking their private information. The disclosure of personal information in OSNS raises users' concerns about their privacy. Should they continue using OSNS? This paper proposes that users' Perceived Usefulness and Perceived Enjoyment positively influence their intention to continue using OSNS, whereas their Privacy Concerns and Previous Privacy Invasion Experiences negatively influence their intention to continue using OSNS. Furthermore, this paper applies the UMT theory and argues that users need to deal with the trade-off. In other words, when they perceive the benefits are bigger than costs, users tend to continue using OSNS, and vice versa.

Although the analysis indicates that users have to pay the cost of leaking their private information to use OSNS, this does not mean that the cost should have to be paid. OSNS providers should take effective measures to protect their users' privacy and to minimize privacy invasions. If they neglect users' costs, users will abandon their services once the costs are bigger than the benefits.

Future studies need to explore what other factors (besides Perceived Usefulness and Perceived Enjoyment) users consider as benefits of OSNS, and what other factors (besides Privacy Concerns and Previous Privacy Invasion Experiences) users consider as costs of OSNS. In addition, during the process of the users' trade-off, what factors moderate their decision? Future studies are needed to clarify these questions.

## REFERENCES

Aimeur, E., Gambs, S., and Ho, A. 2010. "Towards a Privacy-enhanced Social Networking Site," In *Proceedings of IEEE ARES'10 International Conference on Availability, Reliability, and Security*, pp. 172-179.

Ajzen, I., and Fishbein, M. 1980. *Understanding Attitudes and Predicting Social Behavior*, Prentice-Hall: Englewood Cliffs, NJ.

Awad, N. F., and Krishnan, M. S. 2006. "The Personalization Privacy Paradox: an Empirical Evaluation of Information Transparency and The Willingness to be Profiled Online for Personalization," *MIS Quarterly*, pp.13-28.

Barnes, S. B. 2006. "A Privacy Paradox: Social Networking in the United States," *First Monday*, (11:9).

Criddle, L. 2006. *Look Both Ways: Help Protect Your Family on the Internet. Redmond*, WA: Microsoft Press.

Csikszentmihalyi, M., Kolo, C., & Baur, T. (2004). Flow: The psychology of optimal experience. Australian Occupational Therapy Journal, 51(1), 3-12.

Culnan, M. J., and Bies, R. J. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues*, (59:2), pp. 323-342.

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

Ellison, N. B. 2007. "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication*, (13:1), pp. 210-230.

Fishbein, M., and Ajzen, I. 1973. "Attribution of Responsibility: A Theoretical Note," *Journal of Experimental Social Psychology*, (9:2), pp. 148-153.

Gibbs, J. L., Ellison, N. B., and Heino, R. D. 2006. "Self-presentation in Online Personals the Role of Anticipated Future Interaction, Self-disclosure, and Perceived Success in Internet Dating," *Communication Research*, (33:2), pp. 152-177.

Govani, T., and Pashley, H. 2005. "Student Awareness of the Privacy Implications when Using Facebook," *unpublished paper presented at the "Privacy Poster Fair" at the Carnegie Mellon University School of Library and Information Science*, 9.

Gross, R., and Acquisti, A. 2005. "Information Revelation and Privacy in Online Social Networks," In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society,* pp. 71-80.

Handy, S. 2005. "Critical Assessment of the Literature on the Relationships among Transportation, Land Use, and Physical Activity," *Transportation Research Board and the Institute of Medicine Committee on Physical Activity, Health, Transportation, and Land Use*. Resource paper for TRB Special Report, 282.

Hu, T., Poston, R. S., and Kettinger, W. J. 2011. "Nonadopters of Online Social Network Services: Is It Easy to Have Fun Yet?" *Communications of the Association for Information Systems*, (29:1), pp. 25.

Jorgenson, D. W., & Stiroh, K. J. 1999. "Information Technology and Growth," *American Economic Review*, 89, 109-115.

Jung, E. J., McKnight, D. H., Jung, E., and Lankton, N. K. 2011. "The Surprising Lack of Effect of Privacy Concerns on Intention to Use Online Social Networks," in *Proceedings of the Seventeenth Americas Conference on Information Systems, Detroit, Michigan*.

Koroleva, K., Krasnova, H., Veltri, N., and Günther, O. 2011. "It's All about Networking! Empirical Investigation of Social Capital Formation on Social Network Sites," in *Proceedings of 2011 ICIS*.

Krasnova, H., Veltri, N. F., and Günther, O. 2012. "Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture," *Business & Information Systems Engineering*, (4:3), pp. 127-135.

Krishnamurthi, L., & Raj, S. P. 1988. "A Model of Brand Choice and Purchase Quantity Price Sensitivities," *Marketing Science*, 7(1), 1-20.

Malhotra, N.K., Kim, S.S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research*, (15:4), pp. 336-355.

Marett, K., McNab, A. L., and Harris, R. B. 2011. "Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory," *AIS Transactions on Human-Computer Interaction*, (3:3), pp. 170-188.

McFadden, D. L. 2002. "The Path to Discrete-Choice Models," In Access, Vol. 20, pp. 2–7.

Qin, L., Kim, Y., Hsu, J., and Tan, X. 2011. "The Effects of Social Influence on User Acceptance of Online Social Networks," *International Journal of Human-Computer Interaction*, 27(9), 885-899.

Richmond, R. 2010. "Facebook Moves to Thwart Cybercrooks," May 13 (http://gadgetwise.blogs.nytimes.com/2010/05/13/facebook-moves-to-thwart-cybercrooks/).

Samadi, P., Mohsenian-Rad, A. H., Schober, R., Wong, V. W., & Jatskevich, J. 2010. "Optimal Real-time Pricing Algorithm Based on Utility Maximization for Smart Grid. In *Smart Grid Communications (SmartGridComm),* 2010 First IEEE International Conference on (pp. 415-420). IEEE.

Smith, A., Laurie, S., and Stacy, C. 2012. "Facebook Reaches One Billion Users," October 04 (http://money.cnn.com/2012/10/04/technology/facebook-billion-users/index.html).

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

Thambusamy, R., Church, M., Nemati, H., and Barrick, J. 2010. "Socially Exchanging Privacy for Pleasure: Hedonic Use of Computer-mediated Social Networks," in *Proceedings of ICIS 2010, St. Louis, Missouri*, paper 253.

Valkenburg, P. M., Peter, J., and Schouten, A. P. 2006. "Friend Networking Sites and Their Relationship to Adolescents' Well-being and Social Self-esteem," *CyberPsychology & Behavior,* (9:5), pp. 584-590.

Voigt, K. 2009. "Dangerous Internet Search terms Grow with Cybercrime," June 10 (http://edition.cnn.com/2009/BUSINESS/06/21/Internet.cyber.crime/index.html?iref=mpstoryview).

Woollacott, E. 2010. "Most Social Network Users Court Cybercrime, Says Report," May 04 (http://www.tgdaily.com/security- features/49619-most-social-network- users-court-cybercrime-says-report)

Xu, H., Dinev, T., Smith, J., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems*, (12:12), pp. 1.

Xu, C. M., Benbasat, I., and Cavusoglu, H. 2012. "Trusting those Who Trust You: A Study on Trust and Privacy on Facebook," in *Proceedings of ICIS 2012*.

Yoo, C. W., Ahn, H. J., and Rao, H. R. 2012). An Exploration of the Impact of Information Privacy Invasion. Thirty Third International Conference on Information Systems, Orlando 2012.

Young, A. L., & Quan-Haase, A. 2009. "Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook," in *Proceedings of ACM the Fourth International Conference on Communities and Technologies*, pp. 265-274.

Zhang, N., Wang, C., and Xu, Y. 2011. "Privacy in Online Social Networks," in *Proceedings of ICIS 2011*, paper 3.