Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2013 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

6-18-2013

Privacy in Online Social Networking: Applying a Privacy Calculus Model

Janice C. Sipior
Villanova University, Janice.Sipior@villanova.edu

Burke T. Ward
Villanova University, burke.ward@villanova.edu

Regina Connolly
Dublin City University, Regina.connolly@dcu.ie

Labhras MacGabhann
Villanova University, lrozan01@villanova.edu

PRIVACY IN ONLINE SOCIAL NETWORKING: APPLYING A PRIVACY CALCULUS MODEL

Janice C. Sipior, Villanova School of Business, Villanova University, PA, USA, janice.sipior@villanova.edu

Burke T. Ward, Villanova School of Business, Villanova University, PA, USA, burke.ward@villanova.edu

Regina Connolly, DCU Business School, Dublin City University, Dublin 9, Ireland, regina.connolly@dcu.ie

Labhras MacGabhann, Villanova School of Business, Villanova University, PA, USA, lrozan01@villanova.edu

Abstract

The penetration rate continues to grow for social networking sites where individuals join a virtual community to socialize, make connections, and share opinions with those who have similar interests, while revealing personal information. However, online social networking presents a unique context with distinct privacy challenges. To understand information disclosure behavior in this context, we apply the extended privacy calculus model, developed by Dinev and Hart (2006a), which addresses the trade-off between the expected costs of privacy risk beliefs and the benefits of confidence and placement beliefs on the willingness to provide personal information. We further extend this model to include specific types of personal information, based on our proposed taxonomy of information integral to social networking. To test our research model, a questionnaire will be administered to undergraduate students, drawn from the mid-Atlantic U.S. For hypothesis testing, structural equations modeling will be used. The completion of this research-in-progress study is expected to contribute to our understanding of the types of information revealed in online social networking.

Keywords: social networking, privacy calculus, trust, risk, taxonomy of personal information.

1 INTRODUCTION

The penetration rate continues to grow for social networking sites where individuals join a virtual community to socialize, make connections, and share opinions with those who have similar interests, while revealing personal information. The global audience for Facebook, for example, has grown to 964,368,120 as of 02 February 2013.[1] However, this vast growth of online social networking (OSN) has brought increasing privacy concerns (Rizk et al. 2009). While OSN creates value for society in supporting connections among people, criticism abounds about privacy risks in disclosing personal information which is used for commercial purposes (Krasnova et al. 2009a). Since OSN is fee-free to users, user information is used for marketing purposes, an important source of revenues (Krasnova et al. 2009a; Krasnova et al. 2012).

The privacy controversy over collecting information on the Internet arises from the far-reaching unprecedented capability to collect more detailed information and disseminate greater quantities of information (Sipior et al. 2009). OSN presents a unique context with distinct privacy challenges (Bulgurcu et al. 2010; Krasnova et al. 2010; Xu et al. 2008). For users of OSN, information sharing has become even easier as users can simultaneously update personal information across multiple social networks, such as Facebook, Twitter, and LinkedIn. Rosenblum (2007) observed that OSN users seem to be comfortable sharing personal information, seemingly oblivious to the privacy risks. However, privacy concerns of Facebook users, for example, have been found to be prevalent (O'Brien & Torres 2012). The contradiction between disclosing personal information while holding concerns about privacy is called the privacy paradox (Jensen et al. 2005). When confronted with the privacy paradox, the decision to disclose personal information may entail a cost-benefit calculation, termed the privacy calculus (Culnan & Armstrong 1999). Information may be exchanged for some economic or social benefit, weighed against the risks of disclosure. The decision to disclose personal information results from the rational choice when the economic or social benefit outweighs the risks of disclosure.

We extend the privacy calculus to OSN, by building on the research of Dinev and Hart (2006a) who examined the balance between privacy risk beliefs and confidence and enticement beliefs which influence the intention to provide personal information required to conduct transactions on the Internet. Dinev and Hart (2006a) developed a theoretical model comprised of contrary factors representing elements of a privacy calculus for e-commerce transactions. We apply their extended privacy calculus model to assess the impact of privacy risk beliefs, and confidence and placement beliefs, on the willingness to provide personal information within the context of OSN. We further extend this model to include specific types of personal information, based on our proposed taxonomy of information integral to social networking.

[1] www.checkfacebook.com 2013

This research-in-progress paper first summarizes previous privacy calculus research in the context of OSN. We then propose a taxonomy of information integral to social networking. Based on the review of previous research, we present our research model, followed by our hypotheses, and our research methodology. Finally, we discuss expected implications of our study for research and for practice.

2 BACKGROUND

2.1 Previous Privacy Calculus Research in the Context of Online Social Networking

Xu (2009) argues that privacy beliefs are influenced by situational and environmental cues which are indicative of the level of privacy protections in a specific context environment. Further, Xu et al. (2008) confirm that privacy related relationships vary across types of websites, including e-commerce, OSN, financial, and healthcare sites, indicative of information sensitivity in various contexts. The unique context of OSN in this regard has prompted an emergent stream of research within the information systems (IS) literature addressing the disclosure of personal information. To understand the privacy paradox, we take a privacy calculus research perspective. We reviewed the privacy calculus research within the context of OSN and present a summary of this research in Table 1.

Research Study	**Objective**	**Conclusion**
Hugl 2011	Analysis of scholarly work on information privacy in the OSN context.	Adults are more concerned about privacy; the majority underestimate privacy risks; privacy approaches fall short. Call for research on privacy calculus and fair information practices.
Dinev et al. 2009	Investigate users' privacy perceptions by integrating privacy values, beliefs, and attitudes into a theoretical framework.	Perceived control and vulnerability influence perception of privacy. Anonymity and secrecy control information. Information sensitivity and expectation of privacy impact perceived vulnerability.
Krasnova et al. 2009b	Examine the factors behind individual self-disclosure decisions.	Perceived enjoyment and privacy concerns impact information revelation. Users' concerns are determined by perceived likelihood of a privacy violation, less than expected damage.
Krasnova et al. 2010	Develop a self-disclosure model.	Convenience of relationships and enjoyment motivates information disclosure. Privacy risks are a barrier to disclosure. Users' perception of risk can be mitigated by trust in the provider and availability of controls.
Krasnova and Veltri 2010	Explore the differences in perceptions of disclosure-relevant determinants between German and US users.	German users expect more damage and attribute higher probability to privacy violations. US users show higher level of privacy concern, with more benefits, more trust in the provider and legal assurances, and perceive more control.
Krasnova et al. 2012	Explore the role of the two cultural dimensions of individualism and uncertainty avoidance in self-disclosure decisions.	Trusting beliefs are key in self-disclosure decisions of users from individualistic cultures, while uncertainty avoidance determines the impact of privacy concerns.

Li et al. 2011	Examine online information disclosure decision as a result of affective and cognitive reactions of consumers over several stages.	Initial emotions from impression of a site are initial hurdles to information disclosure. Once in the information exchange stage, fairness-based levers adjust users' privacy beliefs.
Li 2012	Develop a dual-calculus framework of trade-offs that influence information disclosure behavior: privacy calculus and risk calculus.	A decision table based on the dual-calculus model to predict an individual's intention to disclose personal information online.
Wilson and Valacich 2012 (research-in-progress)	Develop a theoretical model of actual disclosure behavior and potential for irrational behavior induced by situational factors.	Expected outcome is to capture and study actual information disclosure behaviour.

Table 1. Previous privacy calculus research in the context of online social networking.

2.2 Proposed Taxonomy of User Information Integral to Social Networking

User information disclosed on OSN begin with a profile, which is a list of identifying information such as the user's name or pseudonym, birthday, relationship status, religion, hometown, personal interests, and more. Users connect with other users by sending messages, updating activities and location, sharing photos, archiving events, posting public testimonials, and more. Schneier (2009) proposed that all social networking information falls into one of six categories: service information, disclosed information, entrusted information, incidental information, behavioral information, or derived information. Based on Schneier (2009), we propose a taxonomy of information integral to social networking which more thoroughly catalogs the sources of each information type, the user-in-question's degree of control, the parties that have access to each type, and whether each is explicitly or implicitly disclosed by the users-in-question, as presented in Table 2.

Information Type	**Data Source**	**User-in-Question's Degree of Control**	**Parties that Can Access**	**Implicit or Explicit**
Service	User-in-Question	Low	User-in-Question, Service Provider	Explicit
Disclosed	User-in-Question	High	User-in-Question, Other Authorized Users Indicated by User-in-Question, Service Provider	Explicit
Entrusted	User-in-Question	Medium	User-in-Question, Entrusted User, Other Authorized Users Indicated by Entrusted User, Service Provider	Explicit
Incidental	All Other Users	Low	Incidental User, User-in-Question, Other Authorized Users Indicated by Incidental User, Service Provider	Implicit
Behavioral	User-in-Question	Low	Service Provider, Third Parties Authorized by Service Provider to Access Data	Implicit
Derived	User-in-Question, Other Users, Various Online Databases (in the case of cross-referenced or concatenated data)	Low	Party Responsible for Deriving Data, Other Authorized Users Designated by Party Responsible for Deriving Data	Implicit

Table 2. Proposed Taxonomy of User Information Integral to Social Networking.

Service information refers to the data that users must share in order to access a social network. It includes basic information such as a person's name, date of birth, e-mail address, and – if the service is subscription based – a person's debit or credit card number. *Disclosed information* refers to whatever data individuals make available to others through their online profiles, blogs, twitter feeds, and so forth. *Entrusted information* refers to what individual users post on other users' profiles. It is similar to disclosed information in that it is generated by the user in question, but different in that once this data is turned over to an "entrusted" user it is no longer under the user-in-question's direct control. *Incidental information* refers to data other users disclose about a user-in-question, either on their own or on the user-in-question's profile. It differs from disclosed and entrusted information in that the user-in-question neither authored the data, nor has any control over it. *Behavioral information* refers to data a social networking site collects about users' habits by recording what they do online. It includes things like the amount of time a user spends on a particular site, the sorts of online games a user plays, the frequency with which data regarding user is disclosed, the kinds of music a user listens to online, the sorts of articles a user reads via links embedded in a social networking site, and so forth. Finally, *derived information* refers to data that is derived from one or more of the above kinds of data. The "derivation" involved in this case can run the gamut from simple cognitive deduction – if, for example, 90% a user's friends identify as Republicans, odds that user themselves is a Republican – to conclusions reached with the assistance of computers, algorithms or other kinds of assisted analytics.

Derived information is unlike the other five types of information in this taxonomy. It can include data derived from the activities of many users. For example, social analytic firm ListenLogic analyzes vast swaths of disclosed, entrusted, incidental, and behavioral data.

3 RESEARCH MODEL AND HYPOTHESES

In seeking to understand the willingness to provide personal information to social networking websites, the proposed research model presented in Figure 1 was developed based upon previous research on privacy concerns in the IS literature. Hugl (2011) has called for consideration of privacy calculus in research addressing information privacy in the OSN context. Specifically, we extend Dinev and Hart's (2006a) extended privacy calculus model to the context of OSN. In investigating the privacy calculus, we seek to understand the disclosure of personal information weighed against the risks of disclosure. Important to the privacy calculus is the type of information under consideration for disclosure. We therefore further extend Dinev and Hart's (2006a) extended privacy calculus model to include a taxonomy of information integral to social networking, based upon Schneier (2009). The constructs of our research are defined in Table 3.

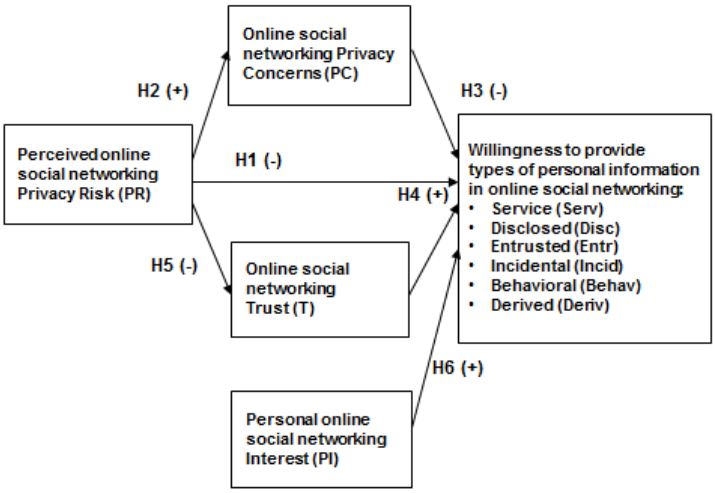

Figure 1. Proposed research model.

Construct category	Construct	Acronym	Definition
Willingness to provide personal information	Willingness to provide personal information to social websites:	PPITSW	Willingness to provide personal information to social websites, based on Schneier's (2009) taxonomy of data integral to social media's operations:
	• Service information	Serv	– Information users must share to gain access to a social network
	• Disclosed information	Disc	– Information users make available to other users through online engagement
	• Entrusted information	Ent	– Information users post on other users' profiles
	• Incidental information	Incid	– Information other users disclose about a user-in-question, either on their own or on the user-in-question's profile
	• Behavioral information	Behav	– Information a social networking site collects about users' habits by capturing what they do online
	• Derived information	Deriv	– Information derived from one or more of the above types of information
Risk beliefs	Perceived social networking privacy risk	SNPR	Perceived risk of opportunistic behavior related to the disclosure of personal information submitted by social networking users *in general*
	Social networking privacy concerns	SNPC	Concerns about opportunistic behavior related to the personal information submitted to social networking by the respondent *in particular*
Confidence and enticement beliefs	Social networking trust	SNT	Trust beliefs reflecting confidence that personal information submitted to social networking websites will be handled competently, reliably, and safely
	Personal social networking interest	PSNI	Personal interest or cognitive attraction to social networking content overriding privacy concerns

Table 3. Constructs in the Extended Privacy Calculus Model for OSN (Based on and expanded from Dinev and Hart 2006a).

Our proposed research model identifies five constructs and the relationships between them. Based on the privacy calculus, it is hypothesized that behavioral intention will be influenced by the perceived costs and benefits. Behavioral intention, the dependent variable, is the willingness to provide personal information to social websites. Costs, an independent variable, are risk beliefs and privacy concerns. Benefits, an independent variable, are the confidence and enticement beliefs, which are trust and personal OSN interest, respectively. Each of these variables, and their hypothesized relationships, are discussed below. For hypothesis testing, structural equations modeling will be used.

3.1 Costs: Privacy Risk Beliefs and Privacy Concerns

Dinev and Hart (2006a) note that higher levels of privacy risk beliefs suggest user resistance to personal information disclosure. This observation was supported by their findings that a higher level of perceived Internet privacy risk is related to a lower level of willingness to provide personal information to transact on the Internet. Consistent results regarding users' concerns about privacy risk have been attained in research on OSN. Krasnova et al. (2010) found privacy risk to be a critical barrier to personal information disclosure. However, this privacy risk was mitigated by the user's trust in the social network provider and the availability of control options. Lo (2010) evaluated a trust-risk model of information disclosure which considered privacy concern to be a dispositional factor and an

antecedent of trust. The results revealed privacy concern significantly impacted perceived risk and thus personal information disclosure. Consistent with these findings, we hypothesize:

Hypothesis 1a-f. A higher level of perceived online social networking privacy risk (PR) is associated with a lower level of willingness to provide types of personal information in online social networking:
a. Service Information (Serv)
b. Disclosed Information (Disc)
c. Entrusted Information (Entr)
d. Incidental Information (Incid)
e. Behavioral Information (Behav)
f. Derived Information (Deriv)

In calculating privacy risk, user assesses the likelihood of negative consequences and the perceived severity of these consequences with the disclosure of personal information (Xu et al. 2011). Previous empirical research in e-commerce has revealed a positive relationship between risk perception and privacy concerns (Dinev & Hart 2006a). Consistent with the previous privacy calculus research of Dinev and Hart (2006a), Dinev and Hart (2006b), Dinev et al. (2006), and Xu et al. (2011), we assess privacy risks as antecedent to privacy concerns:

Hypothesis 2. A higher level of perceived online social networking privacy risk (PR) is associated with a higher level of online social networking privacy concerns (PC):

We concur with Xu et al. (2011) about the "complexity of and inconsistencies in defining and measuring privacy" (p. 800) and adopt the movement they noted within the field of IS to consider privacy "concerns" as the central construct to capture "beliefs," "attitudes," and "perceptions" of privacy. Previous research has examined privacy concerns as an antecedent to behavior, including willingness to disclose personal information (Chellappa & Sin 2005), intention to transact (Dinev & Hart 2006b), and willingness to disclose personal information to transact. The empirical findings of Dinev and Hart (2006a) support a negative relationship, as we hypothesize, between privacy concerns and revealing personal information:

Hypothesis 3a-f. A higher level of online social networking privacy concerns (PC) is associated with a lower level of willingness to provide types of personal information in online social networking:
a. Service Information (Serv)
b. Disclosed Information (Disc)
c. Entrusted Information (Entr)
d. Incidental Information (Incid)
e. Behavioral Information (Behav)
f. Derived Information (Deriv)

3.2 Benefits: Trust and Personal Interest

Trust is regarded as a central aspect in the acceptance of technology (Gefen 2002). For example, consumer satisfaction with an online firm is based upon trust and credibility (Schoenbachler & Gordon 2002). Gross and Acquisti (2005) noted that privacy may be conducive to and necessary for intimacy, but trust may decrease within an OSN. However, Dinev and Hart (2006a) found that higher OSN trust was associated with willingness to provide personal information. We therefore hypothesize that:

Hypothesis 4a-f. A higher level of online social networking trust (T) is associated with a higher level of willingness to provide types of personal information in online social networking:
a. Service Information (Serv)
b. Disclosed Information (Disc)
c. Entrusted Information (Entr)
d. Incidental Information (Incid)
e. Behavioral Information (Behav)
f. Derived Information (Deriv)

Consistent with Dinev and Hart (2006a), who found a negative relationship between privacy risk and trust, we assess privacy risks as antecedent to trust in OSN:

Hypothesis 5. A lower level of perceived online social networking privacy risk (PR) is associated with a higher level of online social networking trust (T).

In accordance with (Dinev & Hart 2006a), we consider personal interest to be an intrinsic motivation based on a belief that engaging in an activity provides self-fulfilling satisfaction, which is captured by the degree of cognitive attraction in computer interactions (Dinev & Hart 2006a). Their empirical findings provide support for a positive relationship between personal interest and the users' willingness to provide personal information:

Hypothesis 6a-f. A higher level of personal online social networking Interest (PI) is associated with a higher level of willingness to provide types of personal information in online social networking:

a. Service Information (Serv)
b. Disclosed Information (Disc)
c. Entrusted Information (Entr)
d. Incidental Information (Incid)
e. Behavioral Information (Behav)
f. Derived Information (Deriv)

4 RESEARCH METHODOLOGY

A questionnaire administered to undergraduate students will be utilized for this study because this methodology increases generalisability, facilitates replicability, and provides statistical power (Dooley 2001). The use of students as subjects is appropriate because they are, as high volume users of both the Internet and OSN, appropriate for the context. We acknowledge the limitation of the use of a convenience sample, collected from a specific geographic location (i.e., a private university located in the mid-Atlantic U.S.), for this study.

4.1 Measures

Questionnaire items, based on previous research, will be used to measure the research variables. The questionnaire will also capture demographic information. All variables will be measured using multiple items, with the exception of demographics.

4.2 Procedure

The questionnaire was reviewed by three colleagues who have expertise in both methodology and in the subject area resulting in very minor corrections. Additionally, we undertook a pilot test to confirm that the questions were worded properly and are appropriate for our sample. As was done for the pilot study, we will distribute our questionnaire through a systematic email accompanied by clear instructions for completing the questionnaire. The questionnaire will be administered through the web-based survey tool Survey Monkey, to present a clear layout and instructions for the questions.

5 RESEARCH CONTRIBUTION

We expect our study to contribute to the nascent body of research addressing the privacy calculus in the context of OSN by extending the extended privacy calculus model for e-commerce transactions, developed by Dinev and Hart (2006a), to this realm. We also expect our study to have practical implications for online vendors regarding privacy concerns about types of information users disclose.

References

Acquisti, A. and Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In Proceedings of 6th Privacy Enhancing Technologies Symposium, Cambridge, UK, 36-58.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Understanding Emergence and Outcomes of Information Privacy Concerns: A Case of Facebook. In ICIS 2010 Proceedings, Saint Louis, MO, USA. Paper 230, http://aisel.aisnet.org/icis2010_submissions/230.

www.checkfacebook.com. (2013). Retrieved 10 February 2013.

Chellappa, R.K. and Sin, R. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. Information Technology and Management, 6 (2), 181-202.

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

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. (2006). Privacy calculus model in ecommerce: A study of Italy and the United States. European Journal of Information Systems, 15 (4), 389-402.

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

Dinev, T. and Hart, P. (2006b). Internet privacy concerns and social awareness as determinants of intention to transact. International Journal of Electronic Commerce, 10 (2), 7-29.

Dinev, T., Xu, H., and Smith, H.J. (2009). Information Privacy Values, Beliefs and Attitudes: An Empirical Analysis of Web 2.0 Privacy. In Proceedings of 42nd Hawaii International Conference on System Sciences, Big Island, HI, USA, IEEE Computer Society Press, Los Alamitos, CA, USA.

Dooley, D. (2001). Social Research Methods. Prentice-Hall, Upper Saddle River, NJ, USA.

Gefen, D. (2002). Reflections on the Dimensions of Trust and Trustworthiness among Online Consumers. Data Base, 33 (3), 38-53.

Gordon, M.E. and L.A. Slade, L.A., Schmitt, N. (1986). The ‘Science of Sophomore’ Revisited: From Conjecture to Empiricism. Academy of Management Review, 11 (1), 191-207.

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, Alexandria, VA.

Hugl, U. (2011). Reviewing person's value of privacy of online social networking. Internet Research, 21 (4), 384-407. doi: http://dx.doi.org/10.1108/10662241111158290.

Jensen, C., Potts, C., and Jensen, C. (2005). Privacy Practices of Internet Users: Self-reports versus observed behaviour. International Journal Human-Computer Studies, 63 (1-2), 203-227.

Krasnova, H., Hildebrand, T., and Guenther, O. (2009a). Investigating the Value of Privacy in Online Social Networks: Conjoint Analysis. In ICIS 2009 Proceedings, Phoenix, AZ, USA. Paper 173, http://aisel.aisnet.org/icis2009/173.

Krasnova, H., Kolesnikova, E., and Guenther, O. (2009b). "It Won't Happen To Me!": Self-Disclosure in Online Social Networks. In AMCIS 2009 Proceedings, San Francisco, CA, USA. Paper 343, http://aisel.aisnet.org/amcis2009/343.

Krasnova, F. and Veltri, N.F. (2010). Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA. In Proceedings of the 43rd Hawaii International Conference on System Sciences, Kauai, HI, USA.

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), 1-135. doi: http://dx.doi.org/10.1007/s12599-012-0216-6.

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. (2010). Online social networks: why we disclose. Journal of Information Technology, 25, 109–125.

Lo, J. (2010). Privacy Concern, Locus of Control, and Salience in a Trust-Risk Model of Information Disclosure on Social Networking Sites. In AMCIS 2010 Proceedings, Lima, Peru. Paper 110, http://aisel.aisnet.org/amcis2010/110.

O'Brien, D. and Torres, A.M. (2012). Social networking and online privacy: Facebook users' perceptions. Irish Journal of Management, 31(2), 63-97.

Rizk, R., Marx, D., Schrepfer, M., Zimmerman, J., and Guenther, O. (2009). Media Coverage of Online Social Network Privacy Issues in Germany: A Thematic Analysis. AMCIS 2009 Proceedings, San Francisco, CA, USA. Paper 342, http://aisel.aisnet.org/amcis2009/342.

Rosenblum, D. (2007). What Anyone can Know: The Privacy Risks of Social Networking Sites. IEEE Security and Privacy, 5, 40–9.

Schneier, B. (2009). A Taxonomy of Social Networking Data. http://www.schneier.com/blog/archives/2009/11/a_taxonomy_of_s.html. Retrieved 13 February 2013.

Schoenbachler, D.D. and Gordon, G. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. Journal of Interactive Marketing, 16 (3), 2–16.

Sipior, J.C., Ward, B.T., and Rongione, N.M. (2009). Consumer Privacy Expectations in a Virtual Environment: A Framework for Corporate Risk Assessment. International Journal of Networking and Virtual Organisations, 6 (6), 558-573.

Wilson, D.W. and Valacich, J.S. (2012). Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus. In ICIS 2012 Proceedings, Orlando, FL, USA. Research-in-Progress.

Xu, H. (2009). Consumer responses to the introduction of privacy protection measures: An exploratory research framework. International Journal of E-Business Research, 5 (2), 21-47.

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), 798-824.

Xu, H., Dinev, T., Smith, H.J., and Hart, P. (2008). Examining the Formation of Individual's Information Privacy Concerns: Toward an Integrative View. In Proceedings of 29th International Conference on Information Systems, Paris, France.