8-5-2011

Theoretical Framework for Understanding Interpersonal Privacy Protection on Social Network Sites

Rong Chen

Theoretical Framework for Understanding Interpersonal Privacy Protection on Social Network Sites

NOTE: IF YOU USE THIS TEMPLATE FOR THE REVIEW VERSION OF YOUR PAPER, YOU MUST REMOVE ALL THE AUTHOR INFORMATION IN THE LINES BELOW. THE REVIEW PROCESS IS DOUBLE BLIND (reviewers do not know who authors are and authors do not know who reviewers are).

First author's name
Affiliation
e-mail address

Second author's name
Affiliation
e-mail address

Third author's name
Affiliation
e-mail address

or

First author's name
Affiliation
e-mail address

Second author's name
Affiliation
e-mail address

Third author's name
Affiliation
e-mail address

Fourth author's name
Affiliation
e-mail address

ABSTRACT

Traditional privacy research would suggest that whether to disclose personal information or not is an individual-based action. However in this paper, we suggest that the consideration of interpersonal level of interaction would also be of vital importance to privacy protection on Social Network Sites (SNS). Based on the theory of self-efficacy, we postulate a research framework that includes the antecedents of both user' self and collective efficacy beliefs on private information control, and the consequent effects on privacy concern and related protection behavior. This study helps to better understand both types of efficacy beliefs as well as study their impacts on two types of privacy concerns: privacy concerns of self disclosure and peer disclosure. The findings are useful for privacy researchers who are interested in collaborative actions in the context of SNS, and for web designers to develop more group centered solutions for privacy protection.

Keywords (Required)

Social Network Sites (SNS), Self-Efficacy, Collective Efficacy, Privacy Concern, Privacy Protection Intention.

INTRODUCTION

Social Network Sites (SNS) has become increasingly important in our daily lives. Take Facebook for example, by July, 2010, it has reached over 500 million active users (Facebook 2011). However, accompanying with its popularity, criticism on privacy violation issues has also accelerated rapidly. Facebook is often under public criticism for the lack of functionality in protecting user privacy (Jones and Soltren 2005; Gürses, Rizk et al. 2008; Lipford, Besmer et al. 2008). Various risks have also been identified associated with the public accessibility to users' personal information, including sharing, collection and sharing of information by third parties, identity theft or use of the information for phishing (Hogben 2007). Increasingly, recent research has identified a new type of privacy threats within the user community – privacy violations caused by their peers' accessibility to information (Jones and Soltren 2005; Rosenblum 2007; Chen, Ping et al. 2009). For example, being tagged by friends on a shared photo may release the identities of tagged users, especially when the shared photo carries some negative message that tagged users do not want to share with others.

Not surprisingly, more and more research on predicting privacy concern has been established and tested by various researchers in the context of SNS. However, most of current research has focused on identifying antecedents to privacy

concern and disclosure intention at the individual level. The group level analysis is under developed in this context. As a consequence, the potential influence of privacy breaches by peers is under studied. According to Bagozzi and Lee (Bagozzi and Lee 2002), there are three levels of social actions: individual-based (individual act by oneself), normative-based (individual act with consideration of the social influence), and group-based (both personal and social intention for group act). In line with Bagozzi and Lee's categorization of social actions, we argue that the privacy management issues in SNS should be not only examined through the individual-based lens (as most current privacy research does), but also through the normative-based and group-based lenses. In other words, we believe that the investigation of users' privacy concerns and subsequent behaviors on SNS should consider the group interaction dynamics as well as interpersonal relationships on SNS.

In this paper, we will use self-efficacy theory developed by Bandura (Bandura 1997) to study two types of efficacy-related beliefs in the context of SNS: i) self-efficacy, and ii) collective efficacy. Self-efficacy is a theory about exercise of personal control (Bandura 1997). However, compared to other general measures of control (e.g. perceived self-control, self-concept of ability, or cognitive competence), efficacy has more predicting power in human behavior because it can be tailored to specific application domains (Bandura 1986; Bandura 1997). In this research, we adapt Bandura's pioneer work to the specific context of SNS and develop a theoretical framework to identify the antecedents of users' self-efficacy beliefs and collective efficacy beliefs in SNS. Then we investigate the roles of both types of efficacy beliefs in alleviating two types of privacy concern: i) concern by self information disclosure, and ii) concern triggered by peers' information disclosure. We believe that this should be one of the first papers to examine efficacy-related beliefs and privacy concern at both individual and group levels in a relatively new context of SNS.

The paper is organized as follows. We start with a literature review of interpersonal privacy issues in SNS. Drawing on the self-efficacy theory, we develop a theoretical framework that models the individual privacy behavioral responses through proposing the mediating roles of privacy concerns and efficacy-related beliefs at both individual and group levels. The paper concludes with a discussion of theoretical and practical implications, and directions for future research.

CONCEPTUAL UNDERSTANDING OF INTERPERSONAL PRIVACY ON SNS

Previous researchers have studied privacy issues in SNS from various perspective, ranging from users' concerns and perceived control over privacy breaches (Xu, Dinev et al. 2008; Bulgurcu, Cavusoglu et al. 2010), resulted online privacy management tools and behaviors (Hempel and Lehman 2005; Read 2006; Dwyer, Hiltz et al. 2010), SNS privacy policy and ethics (Acquisti and Gross 2006; Hodge 2006; Light, McGrath et al. 2008), to actual privacy designs on SNS (Felt and Evans 2008; Gürses, Rizk et al. 2008; Fong, Anwar et al. 2010; Squicciarini, Xu et al. 2011). However, many of these studies are based on the notion of public accessibility to private information, while neglecting the risk caused by semi-public accessibility, in other words, peers' actions toward personal information. Since SNS such as Facebook, Twitter has dramatically expanded into every aspect of people's daily lives; it becomes equally important to understand the violations caused by peer disclosure. And this kind of violation is harder to prevent due to the lack of online monitoring or negotiation system on SNS. As Krasnova et al. (2010) pointed out, the uncertainty of negative outcomes might be magnified by the lack of face-to-face contact and visual cues, which will in turn influence information disclosure on SNS.

Interpersonal Relationship in SNS

Interpersonal relationships can be measured by an individual's intention to interact with others (Schutz 1958). Thus, interpersonal behaviors will be result from phenomena involving more than one person, and determined by the collective conceptions of what is appropriate (Li and Lai 2007). According to Bagozzi (2007), many human behaviors cannot be best characterized by an individual's action in isolation. In accordance with this research, Cheung and Lee (2010) asserted that the adoption decision of online social networking technologies largely depends on the interactions among users. Specifically, Cheung and Lee (2010) adopted the three levels of social actions identified by Bagozzi and Lee (2002): classical individual-based models (individual act by oneself), normative-based models (individual act with consideration of the social influence), and group-based models (both personal and social intention for group act), to promote "We-intentions" in contrast to "I-intention" in deciding the usage of online social network.

This interpersonal relationship investigation can also been understood from structural embeddedness perspective adopted by some other researchers. Structural embeddedness refers to the number of ties an actor has to other actors (Nov and Ye 2008). Researchers argued that individuals inside a unit are more likely to adopt values and norms through inter-unit social interactions (Tsai and Ghoshal 1998). Therefore, users' behaviors on SNS will be shaped by the different networks they are dealing with. For example on Facebook, the attitude a student hold toward friends will be different from what they hold toward teachers (Mazer, Murphy et al. 2007; Atay 2009). The interaction of users will be constrained by specific context.

Interpersonal relationship on SNS will not only influence individuals' privacy beliefs and behaviors, but may also lead to negative results for impression management. For example, being tagged in a photo without notification would be annoying because people tend to garner impression for both acquainted and unacquainted target from the photo and tags (Walther, Van Der Heide et al. 2008). Generally speaking, SNS users desire to be perceived by others, but in certain ways (Bozeman and Kacmar 1997) and their impression requirements impact their desire for privacy with regard to others (Kobsa, Patil et al. 2010).

SNS Privacy at Interpersonal Level

The metaphor of information boundary from Communication Privacy Management Theory (CPM) (Petronio 2002) can help us better understand privacy issues at interpersonal level. In CPM, one needs to draw privacy boundaries for different kinds of information and set up boundary rules with information recipients. While in Facebook context, there is no negotiation mechanism available among friends to agree on privacy rules and there is no monitor systems on each other within the network (Krasnova, Spiekermann et al. 2010). Thus, it becomes difficult for individual users to effectively make privacy decision together with their social networks. On one hand, in order to accumulate a good social capital (Christofides, Muise et al. 2009; Krasnova, Spiekermann et al. 2010), one has to give out information and manage different kinds of friendships on Facebook, e.g., family based, school based, work based and so on. On the other hand, it becomes hard to draw a boundary to the personal information because potential overlaps among different social networks are everywhere. The potential of privacy violation by peers' disclosure exists.

In CPM theory, once a piece of information is disclosed to others, it enters into a co-ownership shared by all recipients. And anyone who receives the information will face the challenge to keep the information within certain boundary, and obey the privacy rules set up on collective agreement (Petronio 2002). However, developed from offline-based context, CPM theory may not easily be applied on SNS. Two problems arise regarding the privacy boundary management in online social network. First, the complex social network overlaps in SNS makes privacy boundary hard to define and maintain. Social network overlap refers to whether or not the disclosed person and the discloser share friends in common (Chen, Ping et al. 2009). While on SNS, people can easily get to know each other through a mutual friend without being directly introduced (Zhao, Grasmuck et al. 2008) and the person's private information can easily be revealed and invaded by this connection (Boyd 2008; Squicciarini, Xu et al. 2011). Second, there is still a lack of technical and operational tools for collective privacy management (Besmer and Lipford 2009; Squicciarini, Xu et al. 2011), which means the action of co-owners on SNS cannot be regulated by collective rules. And the possibility of information disclosure across boundary by random individuals will increase one's privacy related concerns or worries.

Recently, a few studies have been done to explore the interpersonal privacy issues of SNS. For example, Chen et al. (2009) proposed a construct named privacy concerns about peer's disclosure of one's information (PCAPD) and tested its causal relationship with information privacy protection response. Squicciarini et al. (2011) proposed some new privacy enhancing features on Facebook to enable users' collective control over photo privacy management together with their friends.

In line with this stream of research, we believe it is important to differentiate two types of privacy concern on SNS: i) users' privacy concern regarding self information disclosure, and ii) users' privacy concern triggered by peers' disclosure. The first type of privacy concern has already been widely studied in the literature. Our focus will be on the second type of privacy concern as well as comparing the relative effectiveness of these two types of privacy concerns on influencing privacy protection behaviors.

THEORETICAL LENS: SELF-EFFICACY

The conceptualization of privacy is highly related to individuals' ability to control the conditions on how their personal information would be accessed and used (Squicciarini, Xu et al. 2011). Widely accepted definitions of privacy also include the notion of control. For example, Margulis (1977) defined privacy as "the control of transactions between persons(s) and other(s), the ultimate aim of which is to enhance autonomy and/or minimize vulnerability". And internet users' information privacy concern can been understood through users' control over the collected information (Chen, Ping et al. 2009).

Self-efficacy theory is a theory about the exercise of personal control(Bandura 1997), capturing individuals' beliefs in their capabilities for specific achievements, given domain-specific obstacles. Since personal control enables one to predict events and shape them into thinking (Bandura 1997), perceived self-efficacy is considered to be very important in influencing individuals' motivations and behaviors (Gibbs, Ellison et al. 2011).

Bandura later extended the concept of self-efficacy to collective efficacy. Perceived collective efficacy is a group's shared belief in its conjoint capabilities to organize and execute the courses of action required to produce given levels of attainments

(Bandura 1997). In other words, collective efficacy is about beliefs on collective capabilities (Carroll, Rosson et al. 2009). And measurements for community collective efficacy have been developed and tested by Carroll et al. (2005). Both self-efficacy and collective efficacy perspectives suggest a possible way to understand the two parts of SNS privacy concern mentioned earlier : 1) Privacy concern on self disclosure might be a result of users' self-efficacy beliefs in protecting their own information, while 2) privacy concern by peers' disclosure has largely to do with collective efficacy (i.e., the beliefs whether others can be counted on for protecting one's personal information).

CONCEPTUAL FRAMEWORK AND PROPOSITIONS

Drawing on Self-efficacy theory (Bandura 1997; Carroll, Rosson et al. 2009) and related privacy research on SNS, we propose a conceptual framework relating self-efficacy and collective efficacy with privacy concerns and privacy protection behaviors (see Figure 1). Specifically, we separate users' self-efficacy beliefs and collective efficacy beliefs in SNS, and further propose two types of privacy concerns in predicting users' privacy protective behaviors. From this framework, we seek to understand individual privacy behavioral responses through the mediating roles of privacy concerns and efficacy-related beliefs at both individual and group levels.

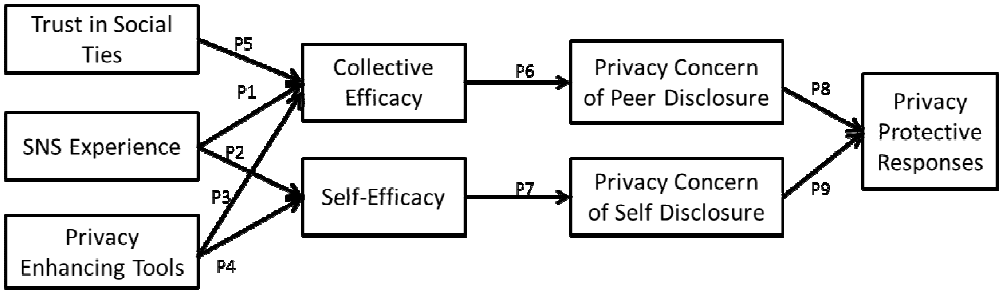

Figure 1. Conceptual model of interpersonal privacy protection in SNS

Efficacy beliefs vary in level, strength, and generality (Bandura 1997). To better predict behaviors in different specific IS domains, the concept of self-efficacy has been adapted into different contexts, ranging from more general ones (Compeau and Higgins 1995) to specific ones for a particular job or task. For example, computer self-efficacy (CSE) has been involved from a general computing level (Marakas, Yi et al. 1998), to specific application-level tasks (Marakas, Yi et al. 1998; Eastin and LaRose 2005; Wang, Xu et al. 2008). Specific self-efficacy has been proved to be more predictive in a particular context than generalized self-efficacy measures do (Marakas, Yi et al. 1998; Gibbs, Ellison et al. 2011).

Therefore we choose to examine self-efficacy at a specific level in SNS in our theoretical framework. In addition, we will distinguish collective efficacy from specific self-efficacy. Collective efficacy is the beliefs about collective capacities on certain tasks (Bandura 1997). It deals with individuals' confidence in others to collaborate and complete the same task. As we mentioned before, on SNS, once being disclosed, and individual's information will enter a collective boundary which is co-managed by all recipients. Thus, beliefs on whether others can effectively control the co-owned information will greatly affect one's own behavior decision. Before disclosing information, the disclosers need to make judgment on whether the information is appropriate for small group sharing and whether they can afford any further disclosure to unexpected audience.

Antecedents of Self Efficacy and Collective Efficacy in SNS

There are four major sources for self-efficacy (Bandura 1997): enactive mastery experiences that serve as indicators of capability; vicarious experiences through comparison with the attainments of others; verbal persuasion and social influence; physiological and affective states from which people partly judge their capabilities. Among the four, the first enactive mastery experience is considered to be the most influential source of efficacy information (Bandura 1997). Successful experience can build strong sense of efficacy beliefs, and failed experience can provide learning opportunities on how to turn failure into success by exercise better control.

A number of IS researchers have identified how computer experience, prior performance will lead to computer self-efficacy beliefs (Wang, Xu et al. 2008). SNS experience is usually gauged by the length and amount of SNS and number of online friends (Wang, Xu et al. 2008; Chen, Ping et al. 2009). Prior internet experience may serve as an important source for self-efficacy beliefs because users with higher levels of SNS experience and greater variety of online activities tend to be more familiar with website operation (Gibbs, Ellison et al. 2011). With the accumulated actual online skills , they will have higher beliefs in the ability to process information and more likely to use privacy features (Stutzman and Kramer-Duffield 2010).

On collective efficacy level, the mix of knowledge and competencies of group gained from previous experience also contribute to the interactive beliefs (Bandura 2006). Therefore, we have the following propositions:

Proposition 1: *Users' SNS experiences will positively associate with their collective efficacy beliefs.*

Proposition 2: *Users' SNS experiences will positively associate with their self-efficacy beliefs.*

In the context of SNS (e.g. Facebook), a person can be tagged in a photo by his/her friend, or be mentioned on the wallpost with direct links to his/her personal profile. Such kind of information disclosure activities are conducted by others, which is out of one's own control domain. In this respect, whether a website can provide privacy enhancing tools for the information management that are disclosed by peers will be vital to the forming and degree of individual's efficacy beliefs.

At the interpersonal privacy level in SNS, SNS providers have been rolling out privacy enhancing tools that allow users to control who can access their personal information, to provide the technological affordances to construct privacy rules (Stutzman and Kramer-Duffield 2010). Privacy enhancing tools will affect the extent to which efficacy beliefs shape outcome expectations (Bandura 1997). Squicciarini et al. (2011) has pointed out the problem on the lack of collaborative privacy management design in current system research. To solve the privacy problems caused by peer disclosure, they designed a tool named CoPE (Colleborative Privacy Management) for Facebook photo sharing. The result shows that users believe a tool like this can be useful to manage their personal information shared within a social network. Thus, we propose:

Proposition 3: *The availability of privacy enhancing tools will positively associate with users' collective efficacy beliefs.*

Proposition 4: *The availability of privacy enhancing tools will positively associate with users' self-efficacy beliefs.*

Besides trust in the SNS provider (Facebook.com), Hoadley et. al (2010) highlights the importance of trust in the social ties (e.g., friends, friends of friends on Facebook, and the university's Facebook users) in the case of Facebook News Feed privacy outcry. When a user disclose her personal information in SNS, the personal information moves to a collective domain where the user and her friends in SNS become co-owners with joint responsibilities for keeping the information safe and private (Petronio 2002). Individuals/friends on the user's contact list usually have certain amount of information access to the user's profile and personal information thus may abuse it if the relationship changes. In addition, it has been recently reported that personal details of Facebook users could potentially be stolen due to their friends' adding applications (Kelly 2008). That is to say, even if some users think they have tight privacy settings, their personal information could be released due to their friends' ignorance of privacy and security (Kelly 2008). The need for trust in social ties arises due to the inability to monitor other members on the network and being uncertain about their behaviors. Trust in social ties, therefore could be an effective mechanism to reduce the complexity of human conduct in situations where people have to cope with uncertainty (Luhmann 1988). Therefore, we propose:

Proposition 5: *Trust in the social ties positively affects associate with users' self-efficacy beliefs.*

Self-Efficacy and Privacy Concern

Privacy concern is defined as the concern about possible loss of privacy as a result of information disclosure (Xu, Dinev et al. 2008). Although this concept has been examined by various scholars, little research has differentiated this construct by levels (e.g., individual vs. group levels) . In this framework, we propose two types of privacy concerns on SNS: privacy concern of self disclosure, and privacy concern of peer disclosure.

Previous research has identified the relationship between "control" and privacy concern. Individuals will perceive information disclosure less invasive when they believe they have the ability to control future use of the information (Culnan and Armstrong 1999). As a result, they will have fewer privacy concerns when they have a greater sense of control over the disclosure and subsequent use of information (Stone and Stone 1990; Dinev and Hart 2004).

In the context of group activities, such as co-managing a shared photo on Facebook, if the person realizes that "I" or "We" (with other members) hold the same beliefs in the intention and ability to control the accessibility to the information, related privacy concern will be alleviated. Thus we'd like to propose that self-efficacy and collective efficacy is likely to influence the degree of privacy concern.

Proposition 6: *Users' beliefs about their collective efficacy in SNS will negatively associate with their privacy concerns of peer disclosure.*

Proposition 7: *Users' beliefs about their self-efficacy in SNS will negatively associate with their privacy concerns of self-disclosure.*

Privacy Concern and Privacy Protection Intention

It is well studied that users' privacy protective behaviors are significantly associated with their privacy concerns (Li and Lai 2007). For example, privacy concern will determine consumer attitudes toward secondary information use (Culnan 1993), influence users' perceptions of the adoption of certain application(Xu 2007).. Son and Kim (2008) concluded that three categories of users' information privacy protective responses (IPPR) are closely related to privacy concerns. The three sets of IPPR includes information provision (refusal, misrepresentation), private action (removal, negative word-of-mouth), and public action (complaining directly to online companies, complaining indirectly to third-party organizations). Followed by this research and through experiment manipulation, (Chen, Ping et al. 2009) further suggested that when members have more concerns about peer's disclosure, they are more inclined to develop privacy protection behaviors. Therefore, we propose:

Proposition 8: *Users' privacy concerns of self- disclosure will positively associate with their privacy protective responses.*

Proposition 9: *Users' privacy concerns of peer disclosure will positively associate with their privacy protective responses.*

FUTURE WORK AND EXPECTED CONTRIBUTION

In this paper, we use self-efficacy theory to investigate users' privacy response behavior at interpersonal level in the context of SNS. Different from previous privacy research, we separate self-efficacy beliefs and collective efficacy beliefs in predicting different levels of privacy concerns, which will in turn lead to privacy protection behavior in SNS. Our theoretical framework consists of SNS experience, privacy enhancing tools and trust in social ties as antecedents of self efficacy beliefs and collective efficacy beliefs, and models the individual privacy behavioral responses through proposing the mediating roles of privacy concerns and efficacy-related beliefs at both individual and group levels. Drawing on the theory of self-efficacy and previous studies, we propose 9 propositions concerning the causal relationships among different constructs.

This would be one of the first papers to examine efficacy-related beliefs and privacy concern at both individual and group levels in SNS. On one hand, SNS greatly improved the quality of users' social networking life. While on the other hand, the overlaps of one's different social networks on SNS have created significant challenges for privacy protection. People by nature require freedom from control by others (Bakke, Faley et al. 2005). However, on SNS like Facebook, the barriers among offline can easily be removed through mutual friends. As result, the personal information updates which was initially shared with friends, can be easily obtained by strangers through application features like photo tag, news feed, wall post and so on. In addition, even if the individual choose not to disclose any personal information, his/her privacy risks still exist because others can disclose information that can directly link to his/her personal profiles. Under this circumstance, it is important and interesting to know how users will make active decisions about when and how to disclose information (Petronio 2002) in the context of SNS.

As for the next step, we will develop our survey instrument and start the data collection. We are interested in knowing whether and how the different constructs function at the interpersonal privacy protection level. The research findings will be insightful for SNS providers to develop more group centered solutions for privacy protection, and will be useful for privacy researchers who are interested in collaborative actions in the context of SNS.

REFERENCES

Acquisti, A. and R. Gross (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook, Springer.

Atay, A. (2009). "Facebooking the Student-Teacher Relationship." *Rocky Mountain Communication Review*: 71.

Bagozzi, R. and K. Lee (2002). "Multiple routes for social influence: The role of compliance, internalization, and social identity." *Social Psychology Quarterly* 65(3): 226-247.

Bagozzi, R. P. (2007). "The legacy of the technology acceptance model and a proposal for a paradigm shift." *Journal of the Association for Information Systems* 8(4): 244-254.

Bakke, S., R. Faley, et al. (2005). "The Impact of Privacy Concerns on the Use of Information Technologies: A Preliminary Conceptual Model." *AMCIS 2005 Proceedings*: 209.

Bandura, A. (1986). Social foundations of thought and action.

Bandura, A. (1997). Self-efficacy: The exercise of control, Worth Publishers.

Bandura, A. (2006). "Guide for constructing self-efficacy scales." Self-efficacy beliefs of adolescents 5: 307-337.

Besmer, A. and H. Lipford (2009). Tagged photos: concerns, perceptions, and protections, ACM.

Boyd, D. (2008). "Facebook's privacy trainwreck: Exposure, invasion, and social convergence." Convergence: The International Journal of Research into New Media Technologies 14(1): 13-20.

Bozeman, D. P. and K. M. Kacmar (1997). "A cybernetic model of impression management processes in organizations." *Organizational behavior and human decision processes* 69(1): 9-30.

Bulgurcu, B., H. Cavusoglu, et al. (2010). "UNDERSTANDING EMERGENCE AND OUTCOMES OF INFORMATION PRIVACY CONCERNS: A CASE OF FACEBOOK."

Carroll, J., M. Rosson, et al. (2009). "Community Collective Efficacy."

Carroll, J. M., M. B. Rosson, et al. (2005). Collective efficacy as a measure of community, ACM.

Chen, J., W. Ping, et al. (2009). "AM IAFRAID OF MY PEERS? UNDERSTANDING THE ANTECEDENTS OF INFORMATION PRIVACY CONCERNS IN THE ONLINE SOCIAL CONTEXT."

Cheung, C. M. K. and M. K. O. Lee (2010). "A theoretical model of intentional social action in online social networks." *Decision Support Systems* 49(1): 24-30.

Christofides, E., A. Muise, et al. (2009). "Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes?" *CyberPsychology & Behavior* 12(3): 341-345.

Compeau, D. R. and C. A. Higgins (1995). "Computer self-efficacy: Development of a measure and initial test." *Mis Quarterly*: 189-211.

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

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

Dinev, T. and P. Hart (2004). "Internet privacy concerns and their antecedents-measurement validity and a regression model." *Behaviour & Information Technology* 23(6): 413-422.

Dwyer, C., S. Hiltz, et al. (2010). Developing Reliable Measures of Privacy Management within Social Networking Sites, IEEE.

Eastin, M. S. and R. LaRose (2005). "Alt. support: Modeling social support online." *Computers in Human Behavior* 21(6): 977-992.

Facebook (2011). "Company Timeline."

Felt, A. and D. Evans (2008). "Privacy protection for social networking APIs." *2008 Web 2.0 Security and Privacy (W2SP'08)*.

Fong, P., M. Anwar, et al. (2010). "A privacy preservation model for facebook-style social network systems." *Computer Security–ESORICS 2009*: 303-320.

Gürses, S., R. Rizk, et al. (2008). Privacy design in online social networks: Learning from privacy breaches and community feedback.

Gibbs, J. L., N. B. Ellison, et al. (2011). "First Comes Love, Then Comes Google: An Investigation of Uncertainty Reduction Strategies and Self-Disclosure in Online Dating." *Communication Research* 38(1): 70.

Hempel, J. and P. Lehman (2005). "The MySpace Generation." *Business Week* 3963: 86.

Hoadley, M. C., H. Xu, et al. (2010). "Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry,." *Electronic Commerce Research and Applications.* Vol. 9(No. 1): 50-60.

Hodge, M. (2006). "Fourth Amendment and Privacy Issues on the New Internet: Facebook. com and Myspace. com, The." *Southern Illinois University Law Journal* 31: 95.

Hogben, G. (2007). "Security issues and recommendations for online social networks." *Position Paper. ENISA, European Network and Information Security Agency*.

Jones, H. and J. Soltren (2005). "Facebook: Threats to privacy." *Project MAC: MIT Project on Mathematics and Computing*.

Jones, H. and J. H. Soltren (2005). "Facebook: Threats to privacy." *Project MAC: MIT Project on Mathematics and Computing*.

Kelly, S. (2008). Identity 'at risk' on Facebook. BBC News.

Kobsa, A., S. Patil, et al. (2010). "Privacy in instant messaging: an impression management model." *Behaviour & Information Technology*(1): 1-16.

Krasnova, H., S. Spiekermann, et al. (2010). "Online social networks: why we disclose." *Journal of Information Technology* 25(2): 109-125.

Li, H. and V. Lai (2007). "The Interpersonal Relationship Perspective on Virtual Community Participation." *ICIS 2007 Proceedings*: 146.

Light, B., K. McGrath, et al. (2008). "More Than Just Friends? Facebook, Disclosive Ethics and the Morality of Technology." *ICIS 2008 Proceedings*: 193.

Lipford, H., A. Besmer, et al. (2008). Understanding privacy settings in facebook with an audience view, USENIX Association.

Luhmann, N. (1988). Familiarity, Confidence, Trust: Problems and Alternatives. Trust. D. Gambetta, G. Basil Blackwell, New York**:** 94-107.

Marakas, G. M., M. Y. Yi, et al. (1998). "The multilevel and multifaceted character of computer self-efficacy: Toward clarification of the construct and an integrative framework for research." *Information Systems Research* 9(2): 126.

Margulis, S. T. (1977). "Conceptions of privacy: Current status and next steps." *Journal of Social Issues* 33(3): 5-21.

Mazer, J. P., R. E. Murphy, et al. (2007). "I'll see you on "Facebook": The effects of computer-mediated teacher self-disclosure on student motivation, affective learning, and classroom climate." *Communication Education* 56(1): 1-17.

Milne, G. R. and M. E. Boza (1999). "Trust and concern in consumers' perceptions of marketing information management practices." *Journal of Interactive Marketing* 13(1): 5-24.

Nov, O. and C. Ye (2008). Community photo sharing: Motivational and structural antecedents.

Petronio, S. (2002). Boundaries of privacy: Dialectics of disclosure, State Univ of New York Pr.

Petronio, S. S. (2002). Boundaries of privacy : dialectics of disclosure. Albany, State University of New York Press.

Read, B. (2006). "Think Before You Share: Students' online socializing can have unintended consequences." *Chronicle of Higher Education* 121.

Rosenblum, D. (2007). "What anyone can know: The privacy risks of social networking sites." *IEEE Security & Privacy*: 40-49.

Schutz, W. C. (1958). "FIRO: A three-dimensional theory of interpersonal behavior."

Shackel, B. (1991). "Usability-context, framework, definition, design and evaluation." *Human factors for informatics usability*: 21-37.

Son, J. Y. and S. S. Kim (2008). "Internet users' information privacy-protective responses: A taxonomy and a nomological model." *Mis Quarterly* 32(3): 503-529.

Squicciarini, A. C., H. Xu, et al. (2011). "CoPE: Enabling collaborative privacy management in online social networks." *Journal of the American Society for Information Science and Technology*.

Stone, E. F. and D. L. Stone (1990). "Privacy in organizations: Theoretical issues, research findings, and protection mechanisms." *Research in personnel and human resources management* 8(3): 349-411.

Stutzman, F. and J. Kramer-Duffield (2010). Friends only: examining a privacy-enhancing behavior in facebook, ACM.

Tsai, W. and S. Ghoshal (1998). "Social capital and value creation: The role of intrafirm networks." *Academy of management Journal* 41(4): 464-476.

Walther, J., B. Van Der Heide, et al. (2008). "The role of friends' appearance and behavior on evaluations of individuals on Facebook: Are we known by the company we keep?" Human Communication Research 34(1): 28-49.

Wang, D., L. Xu, et al. (2008). "Understanding Users' Continuance of Facebook: The Role of General and Specific Computer Self-Efficacy." *ICIS 2008 Proceedings*: 168.

Xu, H. (2007). The effects of self-construal and perceived control on privacy concerns. *Proceedings of 28th Annual International Conference on Information Systems (ICIS)*, Montréal, Canada.

Xu, H., T. Dinev, et al. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view.

Zhao, S., S. Grasmuck, et al. (2008). "Identity construction on Facebook: Digital empowerment in anchored relationships." *Computers in Human Behavior* 24(5): 1816-1836.