2009

# Am I Afraid of My Peers? Understanding the Antecedents of Information Privacy Concerns in the Online Social Context

Jin Chen
*National University of Singapore*, jinchen@nus.edu.sg

Wenjie Ping
*National University of Singapore*, pingwenjie@nus.edu.sg

Yunjie Xu
*National University of Singapore*, xuyj@comp.nus.edu.sg

Bernard C.Y. Tan
*National University of Singapore*, btan@comp.nus.edu.sg

# AM I AFRAID OF MY PEERS? UNDERSTANDING THE ANTECEDENTS OF INFORMATION PRIVACY CONCERNS IN THE ONLINE SOCIAL CONTEXT

*Completed Research Paper*

**Jin Chen**
Department of Information Systems
National University of Singapore
jinchen@nus.edu.sg

**Wenjie Ping**
Department of Information Systems
National University of Singapore
pingwenjie@nus.edu.sg

**Yunjie Xu**
Department of Information Systems
National University of Singapore
xuyj@comp.nus.edu.sg

**Bernard C. Y. Tan**
Department of Information Systems
National University of Singapore
btan@comp.nus.edu.sg

## Abstract

*Privacy concerns about peer's disclosure of one's information (PCAPD) loom as social networking sites (SNSs) getting popular. PCAPD is different from and more complex than privacy concerns in e-commerce contexts. Based on the Communication Privacy Management theory, we propose that decisional control helps reduce a SNS member' PCAPD, and that this effect is contingent on two factors – the overlap between the discloser's social network and that of the disclosed, and information exclusivity. Laboratory experiments were carried out to test the hypotheses. The results showed that decisional control reduces a member's PCAPD. When the discloser's social networks overlaps with that of the disclosed, the effect of decisional control on PCAPD is stronger than when the two do not overlap. In addition, information exclusivity increases PCAPD. This study extends privacy research to the online social network context. It also suggests pragmatic strategies for SNSs to alleviate members' privacy concerns.*

**Keywords:** Information Privacy Concerns, Communication Privacy Management, Decisional Control, Social Network Overlap, Information Exclusivity, Privacy Boundary, Social Networking Sites

## Introduction

Online social interaction flourishes as Social Networking Sites (SNSs) get increasingly popular. However, SNSs also bring potential threats to people's privacy (Grimmelmann 2008; Jones and Soltren 2005). One big threat is unauthorized information disclosure by peers. SNS members are increasingly concerned that they do not always have control over their personal information that is placed online by their friends and exposed to the world (Australian Privacy Commissioner 2009; Riphagen 2008; Yougov 2007). A survey based on 2,447 SNS members showed that 54% of people in the age group of 18-24 said that their friends had posted photos about them with or without their consent, and 19% reported friends' disclosure of their personal information (Yougov 2007). Uncensored or injudicious posts by peers may cause people vulnerable to personal identity theft (Ahearn 2009), career liabilities (Jones and Soltren 2005; Rosenblum 2007), personal life problems (Justice 2007), and even affect their company's reputation (Deloitte 2009).The concerns about peer's disclosures have led to many deaths of SNS profile (Justice 2007).

We term such privacy concerns as "privacy concerns about peer's disclosure of one's information" (PCAPD). Members' disclosure about each other should be considered as a double-edged sword. If SNS members carefully disclose about each other under proper safeguards, they can increase online interactions and develop intimate relationships with one another. However, impropriate disclosures could pose a serious privacy threat to each other and incur social risks and embarrassments. These concerns would deter members from engaging in SNSs in the long run, which is detrimental to both individual member' welfare and company' profits (e.g., SNS providers and marketers on SNS). On the other hand, if a SNS provider can help members allay such privacy concerns, its members would regard it as a more competent, considerate and responsible provider, trust it more, and commit to it. Therefore, it is of great significance for SNS providers to alleviate members' PCAPD.

However, PCAPD in online social context is quite different from privacy concerns in online commercial contexts. In e-commerce contexts, (1) the boundary of privacy is very clear: all personal information (e.g., address and bank account number) disclosed by customers to online vendors in transactions should be regarded as private (Hui et al. 2007; Smith et al. 1996); (2) the social contract between customers and vendors is also clear: vendors are responsible for safeguarding customers' private information (Xu et al. 2006) and maintaining organizational justice for customers (Culnan and Armstrong 1999; Culnan and Bies 2003); and (3) customers have control over personal information (e.g., approval of other use, modification) (Malhotra et al. 2004). However, for PCAPD on SNSs, (1) the boundary of privacy is less clear: in social interactions, the boundary of privacy is dynamically regulated because the desired privacy level varies from time to time (Altman 1975); (2) the social contracts (e.g., norms) between members are less clear because of the complexity of social interaction; and (3) members are often given no option to remove the information disclosed by peers about them due to legal constraints (i.e., copyright). Thus, the findings of privacy research in the e-commerce context may not be applicable to the online social context.

Therefore, our research question is: what are the antecedents of a member's concerns about peer's disclosure of his or her private information on SNSs? Although few studies have pointed out the importance of privacy concerns on SNSs (e.g., Dwyer et al. 2007; Grimmelmann 2008; Jones and Soltren 2005), few attempts have been made to investigate the online social privacy concerns. Therefore, we seek to fill this gap by firstly clarifying a specific definition for privacy concerns about peer's disclosure (PCAPD), and then examining its antecedents. Our findings are expected to extend existing information privacy research to the online social context. Our findings provide guidance to SNS providers to improve their privacy protection strategies and to alleviate members' privacy concerns. The findings would also enlighten SNS users by providing insights into the circumstances under which information privacy violations can have detrimental consequences.

## Literature Review and Theoretical Foundations

Information privacy refers to the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others (Westin 1967). Prior IS studies mostly emphasized on how organizations or Internet service providers can protect online customers' privacy (Dinev and Hart 2006; Malhotra et al. 2004; Smith et al. 1996). Several definitions of privacy concerns have been proposed. Information privacy concerns about organizational practices refer to the extent to which an individual is concerned about organizational practices related to the collection and use of his or her personal information (Smith et al. 1996). Internet users' information privacy concerns (IUIPC) are defined as the degree to which an Internet user is

concerned about online marketers' collection of personal information, the user's control over the collected information, and the user's awareness of how the collected information is used (Malhotra et al. 2004). Internet information privacy concerns denote the concerns about receivers' opportunistic behavior related to the personal information submitted over the Internet (Dinev and Hart 2006).

However, to the best of our knowledge, prior IS research has not addressed the privacy concerns resulting from peer's disclosure in online social interactions. PCAPD is a new kind of online privacy concern in the social interactions among SNS members. In this study, we define *privacy concerns about peer's disclosure of one's information* (PCAPD) as the extent to which an individual is concerned that his or her personal information would be disclosed online by peers. We term "the disclosed" as the person whose information is revealed, "the discloser" as the person who reveals that information, and "the disclosee" as the person who receives that information.

### *Communication Privacy Management Theory*

The counterpart of PCAPD in offline social interactions has been studied by sociologists (Altman 1976; Petronio 2002). Sociological studies have paid attention to people's revealing and concealing of private information in everyay relationship development. Altman (1975) suggested that privacy is an interpersonal boundary-control process, which paces and regulates interaction with others. Privacy is an active and dynamic process which changes over time and circumstances (Altman 1976). Following Altman's research, Petronio (2002) developed the theory of Communication Privacy Management (CPM) and argued that privacy regulation process is fundamentally communicative in nature. CPM also used the term "boundary" to represent the privacy management process. A boundary allows people to identify who has control over or access to the information, and whether the information within the boundary should be protected from those outside of the boundary (Petronio et al. 2004).

The permeability of privacy boundary depends on the nature or state of relationship among the discloser, the disclosed, and the disclosee (Petronio 2002). The boundary changes as the social relationships among people and their expectations of interaction with one another vary (Altman 1975). When it comes to peer's disclosure, the disclosed would feel uncomfortable if the disclosee belongs to a social sphere to which the disclosed does not want the information to be disseminated (Riphagen 2008).

The permeability of privacy boundary also depends on the nature of privacy boundaries. CPM theory differentiates two types of boundary – personal boundary and collective boundary (Petronio 2002). "Personal boundaries are those that manage private information about the self", while collective boundaries are for information which is "not solely about the self" (Petronio 2002, p.6). It is possible that two or more persons co-own private information because the private information is shared by the group (Margulis 2003). Privacy boundaries can be constructed by individual's privacy rules and impacted by cultural values, gendered expectations, motivations, contextual issues, and risk factors (Petronio 2002). Although co-owners can establish and enact same rules to control the permeability of a collective boundary (Petronio et al. 2004), conflicts or turbulences often take place in social interactions when they have different understandings of the rules.

Because a discloser does not always know the relationship between the disclosed and the disclosee, and because the discloser does not know the privacy rules of the disclosed, they often clash with each other in the boundary management process during social interactions (Petronio 2002). One way to avoid such dilemmas is to enhance control on the boundary. Control on privacy rules, such as negotiation on a set of privacy rules among members, would be helpful for privacy management (Petronio et al. 2004). However, because negotiation is usually enacted implicitly, the control process may become turbulent. Furthermore, when it comes to online SNS communities, privacy concerns would be magnified because (1) computer-mediated communication may make the negotiation more difficult (e.g., via asynchronous and lean communication channels); (2) SNSs standardize and centralize information to an unprecedented extent (Jones and Soltren 2005), making private information more vulnerable to be copied, transmitted, and integrated; (3) SNSs' social connectedness makes the diffusion of information much faster and wider than offline. Thus, privacy concerns are more complex on SNSs than in offline social interactions.

## Research Model and Hypotheses

Our research model of social privacy concerns is developed mainly based on the CPM theory. The rationale of the model is that people' PCAPD is a function of the kind of information (e.g., information exclusivity), the kind of potential disclosee (e.g., via social network overlap), and the degree of control (e.g., decisional control). In this

study, the disclosed information refers to the kind that puts the disclosed into a risky or vulnerable situation in social interaction.

### *Decisional Control*

The boundary regulation process serves to maximize the freedom of choices and behavioral options, thereby permitting control over social activities (Proshansky et al. 1970). "A key vehicle to obtaining behavioral options is to control space, i.e., territory, and to determine what will and will not transpire in territories" (Altman 1976, p.10). Therefore, means of control is central to information privacy (Altman 1976; Foddy and Finnighan 1980; Kelvin 1973; Marshall 1974; Xu 2007). CPM theory also maintains that, because people feel they own or co-own their private information and because revealing private information makes them vulnerable, they want to exercise control over it (Petronio 2002).

Psychology literature on control suggests that empowering people with decisional control is a prominent way to make them feel more in control and thus less in concern (Skinner 1996). *Decisional control* is defined here as the availability of opportunity to choose among various courses of action with respect to a potential privacy violation (Averill 1973; Fiske and Taylor 1991). An individual's concerns for information privacy center on whether the individual has decisional control over personal information as manifested by the existence of voice (i.e., approval, modification) or right to exit (i.e., opt-out) (Malhotra et al. 2004). Providing people with choices is a common proxy of granting decisional control (Averill 1973; Corah and Boffa 1970; Skinner 1996). Such choices give people options to reduce unexpected social risks. Lack of such choices will directly lead to an increase in privacy concerns. Thus, we hypothesize:

**H1:** *The higher a SNS member's decisional control is, the lower the member's PCAPD will be.*

Moreover, in social interactions, privacy is a dynamic interpersonal boundary regulation process. Privacy rules change as the nature of relationship and type of information vary (Petronio 2002). In some occasions, people want to stay alone, while in other occasions they may want to be with others. Thus the control becomes "a selective control" (Altman 1976, p.8), which implies that people may prefer a different control strategy in accord with various situations. The need to control will depend on some moderators. Therefore, in this study, we want to identify the circumstances that make people more sensitive to the availability of decisional control to alleviate PCAPD.

The identification of such moderators is both practically and theoretically important. Practically speaking, we note that many SNSs are reluctant to offer members decisional control over peer's disclosure because such decisional control may restrict members' freedom to interact, reduce the fun between peers, and impede the amount of social interactions. Theoretically speaking, moderators answer the critical "who-where-when" questions needed for sound theory development (Whetten 1989). Moderators are especially important and necessary for privacy research because the desired privacy level varies due to individual and contextual differences (Altman 1975; Petronio 2002). For each moderator, we will posit its main effect firstly, followed by its moderation effect.

### *Social Network Overlap*

We first propose that social network overlap, as a proxy of social relationships, moderates the effect of decisional control on PCAPD. This is because the permeability of privacy boundary varies as disclosees change (Petronio 2002). *Social network overlap* refers to whether or not the disclosed person and the discloser share friends in common (Milardo 1982; Sprecher and Felmlee 1992). Although social network overlap on surface describes the relationship between the discloser and the disclosed person, it implies the relationship between the disclosee and the disclosed. If there is no social network overlap between the discloser and the disclosed, the disclosees are not friends of the disclosed.

When there is no social network overlap between the disclosed and the discloser, it is very likely that the disadvantageous information will not be seen by other friends of the disclosed, but only by some strangers. People are less worried about strangers' evaluations of themselves because there is no social interaction with strangers. Strangers' perceptions and feelings have little impact on the disclosed. Furthermore, people may perceive themselves less vulnerable to strangers because strangers have little knowledge about them to exploit their weaknesses. Therefore, when there is no overlap, the disclosed may have fewer concerns about the privacy violation. In contrast, when there is some overlap, at least one friend of the disclosed could see the disadvantageous information. It is very likely that the information would be quickly dispersed among other friends of the disclosed.

Consequently, the disclosed would bear a greater social risk, and have a higher level of privacy concerns. Thus, we hypothesize:

> **H2:** *A SNS member's PCAPD will be higher when the discloser's social network overlaps with the member's than when the two do not overlap.*

We also posit that the effect of decisional control on PCAPD will be stronger when the two networks overlap than they do not. As explained earlier, when the discloser's network overlaps with that of the disclosed, the possibility of some other friends seeing the disadvantageous information is higher. The social risk will be higher. Under such a higher risk, empowering the disclosed with higher decisional control would shield him or her from some stressful events and reduce his or her PCAPD. When the two networks do not overlap, it is very likely that the information would not be seen by the friends of the disclosed. The social risk of the privacy disclosure is relatively lower. Under such a lower risk, empowering the disclosed person with higher decisional control may not be as much appreciated. Thus, we hypothesize:

> **H3:** *The effect of decisional control on PCAPD will be stronger under the condition of overlapped social networks than under the condition of non-overlapped social networks.*

### *Information Exclusivity*

In addition to network overlap, information exclusivity which characterizes the type of privacy boundary moderates the effect of control. *Information exclusivity* is defined here as the extent to which an individual perceives that the information is solely about himself or herself. The information held in a personal boundary is regarded as of high exclusivity because the information only involves that person, whereas the information held in a collective boundary is regarded as of low exclusivity because the information is also about others.

Regarding highly exclusive information, prior research posits that people have a part of themselves that they want kept hidden or private from others (Bies 1996; Greenberg and Cropanzano 2001; Stone and Stone 1990). People feel that only they have the right to decide whether their hidden self can be disclosed or not in certain circumstances. Thus, when the hidden self is invaded by others, the violation should arouse a strong sense of injustice and a higher level of privacy concerns (Bies 1996; Greenberg and Cropanzano 2001).

Regarding less exclusive information, the disclosed understands that he or she co-owns the information with some friends. Firstly, the disclosed might know that those friends may hold idiosyncratic rules different from his or hers (Petronio et al. 2004). The disclosed would have a psychological preparation for possible privacy violation. Psychological preparation has been found able to decrease distress (Johnston and Vögele 1993). When violation happens, the privacy concerns of the disclosed would be dampened by the ex-ante psychological preparation. Second, the disclosed knows that others are also entitled to deal with that information. When others disclose the information, the disclosed may feel less injustice and hence a lower level of privacy concerns. Therefore, we hypothesize:

> **H4:** *The higher information exclusivity is, the higher the member's PCAPD will be.*

Beyond the main effect of information exclusivity, we also propose an interaction effect between information exclusivity and decisional control. That is, the effect of decisional control on PCAPD will be stronger when the information exclusivity is higher. This is because, when information exclusivity is high, the privacy boundary serves as a barrier demarcating the private and public spheres of life (Bies 1996). This interface of the self and the social world is pivotal to one's self identity and self esteem. If people fail to control this interface, they would have strong negative feelings of incompetence to deal with the world. Their concerns about the self identity and personal space would increase accordingly. Higher decisional control to avoid future stress becomes more desirable. Thus, empowering the disclosed person with higher decisional control on highly exclusive information will produce a salient effect on PCAPD.

On the other hand, when information exclusivity is low, the information is about the person as well as others. In such circumstance, people would also have a part of in-group self that they want to keep hidden or private from out-group world (Riphagen 2008). The privacy boundary serves as a barrier demarcating the in-group and out-group world. The control on this boundary is usually regarded as less definitive of self identity and self esteem. If this boundary is invaded by co-owners, the failure will be more attributed to co-owners' behavior rather than to the person's own competence. Moreover, people are aware of their limited ability to control this boundary when other

co-owners hold privacy rules different from theirs (Petronio 2002). Thus the effect of giving the person high decisional control might be weaker. Empowering the disclosed with higher decisional control on less exclusive information produces less effect on PCAPD. Therefore, we hypothesize:

> **H5:** *The effect of decisional control on PCAPD will be stronger under the condition of high information exclusivity than under the condition of low information exclusivity.*

Furthermore, it is noted that a set of *information privacy protective responses (IPPR)* are associated with privacy concerns. IPPR is a set of Internet users' behavioral responses to their perception of information privacy threats (Son and Kim 2008). In particular, IPPR include three broad types of behavioral responses: information provision (e.g., refusal, misrepresentation), private action (e.g., removal, negative word-of-mouth), and public action (e.g., complaining directly to online companies, complaining indirectly to third-party organizations). We focus on the private and public actions here because information provision is not appropriate in the PCAPD context. When people have a higher level of privacy concerns with a website, they are more likely to remove their information and complain to others. Thus, we hypothesize:

> **H6:** *The higher a member's PCAPD is, the more the members' IPPR will be.*

Although third-order interaction may occur among the independent variables, no attempt has been made to predict its significance because of the lack of sound theoretical justification and the difficulties of result interpretation (Kumar and Benbasat 2004). In conclusion, the research model for this study is depicted in Figure 1.

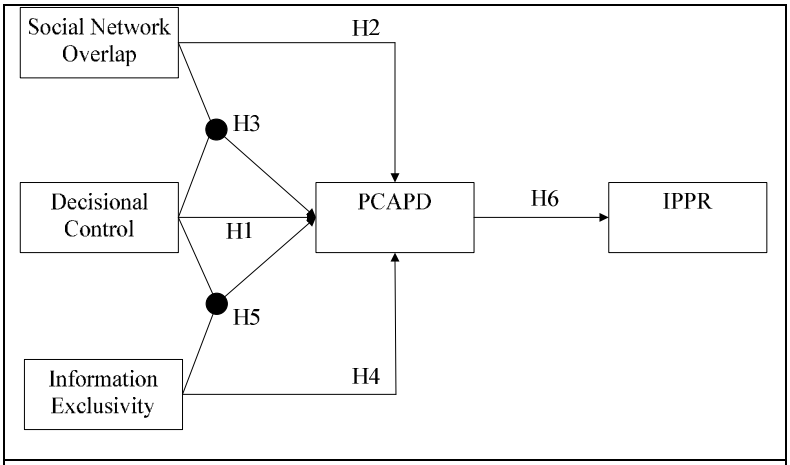


**Figure 1. The Research Model**

### *Control Variables*

Prior research has identified a number of factors that may affect privacy concerns, including demographic variables (e.g., age, gender, and education, see Malhotra et al. 2004; Petronio 2002), related experiences (e.g., SNS experience, and past privacy invasion, see Hui et al. 2007), and psychological dispositions (e.g., privacy disposition, and trust propensity, see Hui et al. 2007; Xu et al. 2008). We include these factors as covariates in this study to isolate the effects of two independent variables.

## Research Methodology

### *Experimental Context*

A 2×2×2 factorial design was carried out by manipulating decisional control (low versus high), information exclusivity (low versus high), and social network overlap (zero versus one). Consistent with previous studies that examined privacy concerns (Sheng et al. 2008; Xu 2007), a vignette technique was employed in the experiment. Vignette technique uses short scenarios in a written or pictorial form to elicit perceptions, opinions, beliefs, and attitudes toward typical situations (Finch 1987).

To get subjects more involved in the experiment, a simulated Facebook website was developed because Facebook is the most popular SNS world-wide (TopTenREVIEWS 2009). Subjects assumed the role of the disclosed. The interface and features of the website were designed to mock Facebook as much as possible (see Figure 2). However, on this simulated website, subjects could only access our manipulated features. Other unrelated features and applications (e.g., chatting or posting) were disabled to exclude potential confounding effects. Moreover, discussion in a focus group suggested that it was easier for subjects to imagine a blank profile figure as themselves rather than a real photo of someone else. Therefore, in the web design, blank profile figure was used in all web pages.

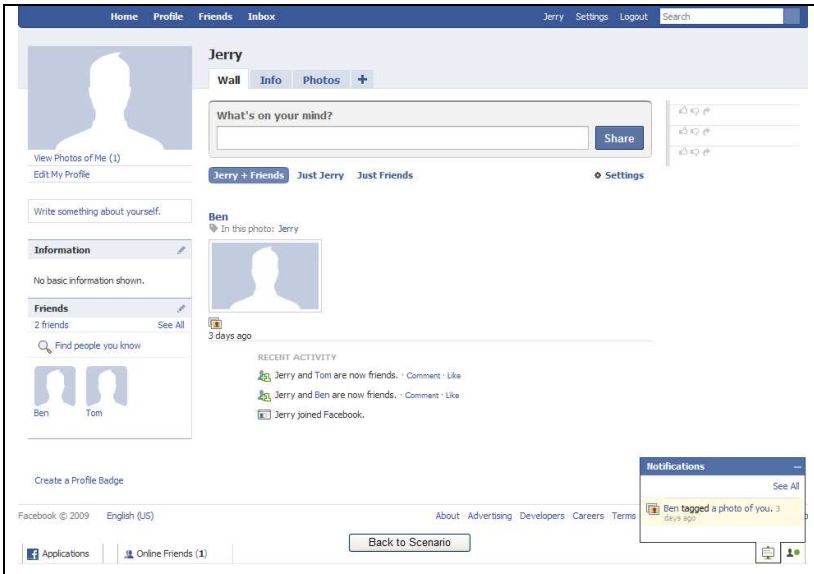


**Figure 2. Website Interface Illustration**

The tagging feature of SNSs was chosen as the privacy-bearing feature in our scenarios. In our simulated website, one of Jerry's (i.e., the disclosed) friends, Ben (i.e., the discloser), could attach Jerry's name as a tag to a photo with Jerry in it. Jerry's name would show beside the photo (see Figure 2), and any viewer of the photo could tell that was Jerry in the picture. The tag also linked to Jerry's profile.

Tagging was chosen for several reasons. First, tagging is a well-accepted feature. Seven out of the top 10 SNSs have adopted it (TopTenREVIEWS 2009). Second, the openness (i.e., availability and operability to any visitor) (Grimmelmann 2008), identifiability (i.e., link to the tagged person's profile) (Rosenblum 2007), and searchability (i.e., searchable by Google) (Nussbaum 2007) of tags suggest that unauthorized tags may infringe upon people's privacy. Third, tagging is an IT enabled activity with a standardized process, and is thus suitable for both experimenters and SNS providers to manipulate.

### *Manipulations*

For decisional control, manipulating the range of choice or number of options to an individual is a common way to operationalize it (Averill 1973; Corah and Boffa 1970; Lewis and Blanchard 1971; Skinner 1996). At the high decisional control level, subjects had complete freedom to approve or disapprove peer's tagging requests before the actual tagging, and also had the option to remove existing tags. This level emulated the statutory privacy rights in offline lives, requiring the discloser to get other's permission first before revealing other's private information. At the low decisional control level, subjects were given no option to approve peer's tagging requests, but only the option to remove existing tags. This level emulated the status quo of most SNSs which allow both freely tagging and freely untagging.

For information exclusivity, the CPM theory suggested to use two types of privacy boundary to create different levels of exclusivity (Petronio 2002). In the condition of high exclusivity, information held in a personal boundary was utilized to represent information solely pertinent to a person. Uncensored personal information, e.g., posts about

health conditions, may become people's career liabilities because about 11.5 percent of employers screened job candidates using SNSs (Rosenblum 2007). In the experiment, the subject was told that a friend wanted to tag the subject with a note that indicated he or she was a HBV carrier. In the condition of low exclusivity, although the information held in a collective boundary pertains to a group of people, disclosure of uncensored collective information may still cause social risks because the disclosed wants to conceal it from the out-group world (Jones and Soltren 2005; Riphagen 2008). In the experiment, the subject was told that one of his friends, friend A wanted to tag the subject to a photo taken in a party one night given the background that the subject had declined friend B's request to work on a project at the same night.

For social network overlap, it is often operationalized as the amount of mutual friends (Milardo 1982; Sprecher and Felmlee 2000). In particular, we compared the zero overlap level (i.e., no mutual friend) and the minimum overlap level (i.e., one mutual friend). One mutual friend was chosen because it is a representative symbol which contrasts against zero. It suggests that, at least one acquaintance could see the disclosed information. The effect is representative of more additional mutual friends they could have (Watts 1999). Thus at the level of one overlap, the subject was told explicitly that he or she had one mutual friend with the discloser on the SNS. At the level of zero overlap, the subject was told explicitly that he or she did not have any mutual friend with the discloser on the SNS.

### *Procedure*

Since this study was a new attempt in online social contexts, a pilot study was used to check the success of manipulations (Perdue and Summers 1986). In the pilot study, 44 undergraduates were recruited and presented with the scenarios in the form of web pages. The simulated Facebook web pages were shown to subjects to demonstrate tagging feature and the privacy violation instance. After understanding the scenario, subjects were requested to fill out a questionnaire including manipulation checks, comprehension checks, and demographic variables. The comprehension checks were to make sure that the subjects treated the experiment seriously. In all, 30 subjects passed comprehension checks, and their responses were used for manipulation checks.

In the main study, all subjects began the experiment by answering a pre-experiment questionnaire about their disposition to value privacy (DVP) and trust propensity (TRUST). Then subjects were asked to read the scenarios, after which they were requested to finish another questionnaire that measured their PCAPD, IPPR, demographic variables, comprehension checks, and other covariates.

### *Subjects*

A total of 209 students of ten ethnicities were recruited from six faculties in a large university, representing diverse backgrounds. To avoid selection bias, subjects were only apprised that it was an experiment on SNS usage behavior. The objective of the study was not revealed. Subjects were randomly assigned to eight treatments. Each subject received S$5 as an incentive for participation. As an additional incentive, two subjects received an extra of S$50 in a lucky draw. The responses of 156 subjects who passed the comprehension checks were used for data analysis. A demographic summary of the sample is shown in Table 1. There was no significant difference in gender and age distribution across the eight groups.

**Table 1. Demographics of the Sample (N=156)**

| **Demographic Variable** | Sample Composition | | | |
|---|---|---|---|---|
| **Age (years old)** | Mean | 22.77 | Std. | 2.784 |
| **Gender** | Male | 52.6% | Female | 47.4% |
| **Degree in Education** | Undergraduate | 76.9% | Graduate | 23.1% |
| **Education Background** | Sciences | 88.5% | Humanities | 11.5% |

### *Measurements*

Instrument was developed by adopting and adapting existing validated scales whenever possible (see Table 2). In particular, we adapted the instrument of privacy concerns from Xu (2007) and Xu et al. (2008). The instrument of IPPR was adapted from Son and Kim (2008). The instruments for covariate are listed in Table 2.

**Table 2. Operationalization of Constructs**

| **Dependent Variables** | **Item Description** | **Reference** |
|---|---|---|
| Privacy Concerns About Peer's Disclosure of one's information (PCAPD) | (1-7 Likert scale, 1=Strongly disagree, 7=Strongly agree)<br>PCAPD1: It bothers me when Ben* disclosed this personal information about me on this website.<br>PCAPD2: I am concerned that, on this website, Ben can disclose too much of my personal information.<br>PCAPD3: I am concerned that, this website may not take measures to prevent Ben's unauthorized disclosure of my personal information.<br>PCAPD4: I am concerned that, on this website, Ben can reveal my personal information in a non-accurate manner.<br>PCAPD5: I am concerned that, on this website, Ben can reveal my personal information without getting my authorization.<br>PCAPD6: Overall, I feel unsafe that Ben may disclose my personal information on this website.<br>PCAPD7: I am concerned that, on this website, unauthorized people may see my personal information from Ben's web pages. | Adapted from (Xu 2007; Xu et al. 2008) |
| Information Privacy Protection Response (IPPR) | (1-7 Likert scale, 1=Strongly disagree, 7=Strongly agree)<br>IPPR1: I would take actions to have my personal information removed from this website.<br>IPPR2: I would speak to my friends and/or relatives about the way this website allows Ben to disclose my personal information.<br>IPPR3: I would write or call this website to complain about the way this website allows Ben to disclose my personal information.<br>IPPR4: I will write or call an elected official or consumer organization to complain about the way this website allows Ben to disclose my personal information. | Adapted from (Son and Kim 2008) |
| **Control Variables** | **Item Description** | **Reference** |
| Disposition to Value Privacy (Subjective DVP) | (1-7 Likert scale, 1=Strongly disagree, 7=Strongly agree)<br>DVP1. Compared to others, I am more sensitive about the way my personal information is handled.<br>DVP2. To me, it is the most important thing to keep my personal privacy.<br>DVP3. Compared to others, I tend to be more concerned about threats to my personal privacy. | Adopted from (Xu et al. 2008) |
| Cookie Setting (Objective DVP) | Please select your cookie policy for your Internet browser from the following list. (Subjects who chose one of the last three options were considered more concerned about privacy)<br>- My preferences are set to always accept cookies.<br>- I don't know what a cookie is.<br>- I don't know what my cookie preferences are set to.<br>- My browser doesn't support cookies.<br>- My preferences are set to only accept cookies from the same site I am browsing. | Adopted from (Hui et al. 2007) |

| | | |
|---|---|---|
| | - My preferences are set to warn me before accepting cookies.<br>- My preferences are set to ignore/never accept cookies. | |
| Trust Propensity (TRUST) | (1-7 Likert scale, 1=Strongly disagree, 7=Strongly agree)<br>TRUST1. I feel that people are generally trustworthy.<br>TRUST2. I feel that people are generally reliable. | Adopted from (Hui et al. 2007) |
| Invasion of Privacy in Past | Times of personal information misused by others in the last year | Adapted from (Hui et al. 2007) |
| SNS Experience | (1-7 Likert scale, 1= None, 7=Extensive)<br>How much experience do you have with Social Networking Sites? | Adopted from (Wang et al. 2008) |
| *: Ben is the name of discloser in the scenarios. | | |

# Data Analysis

### *Manipulation Check*

The manipulation on decisional control was assessed using a perceptual question asking subjects, on a 1 to 7 scale, whether "I have sufficient options to keep others back from disclosing my personal information on this website." A t-test ($t=-2.775$, $p<0.05$) showed that subjects in high decisional control level perceived more options (mean=5.00, std=1.22) than those in low decisional control level (mean=3.54, std=1.66).

The manipulation on social network overlap was assessed using a perceptual question asking subjects, on a 1 to 7 scale, whether "on this website, I have no mutual friend with the person who discloses my personal information." A t-test ($t=-5.749$, $p<0.001$) showed that subjects in the level of zero overlap (mean=5.40, std=1.92) reported more agreement with the statement than those in the level of one overlap (mean=1.87, std=1.41).

The manipulation on information exclusivity was assessed using a perceptual question asking subjects, on a 1 to 7 scale, whether "the information that is disclosed on the website is about me as well as others." The answers were inversely coded to make 1 denote the lowest exclusivity and 7 denote the highest exclusivity. A t-test ($t=2.281$, $p<0.05$) showed that subjects in a high exclusivity level reported higher exclusivity (mean=2.62, std=0.96) than those in a low exclusivity level (mean=1.94, std=0.66). In all, all manipulations were successful.

### *Measurement Validation*

All statistical tests were carried out at a 5% level of significance. Exploratory factor analysis (EFA) was conducted to test the instrument's convergent and discriminant validity for perceptual constructs. Table 3 reports the EFA results with principal component analysis and varimax rotation using SPSS. First, we found a four-factor structure with eigenvalues greater than 1.0. All constructs explained 69.4 percent of the total variance. However, the first item of IPPR (IPPR1) was cross-loaded over factors, and was dropped from further analysis because of its distinct meaning from other items of IPPR. After that, all items were loaded on target factors with loading above 0.6, and loaded on other factors with loading below 0.36 (Xu 2009). Thus, discriminant validity was established. Second, the internal consistency reliability was measured by Cronbach's alpha with 0.7 as the cut-off (Nunnally and Bernstein 1994). The alphas for all constructs were well above 0.7. Thus, convergent validity was established. After measurement validation, items of each construct were averaged as a measure of the target construct.

**Table 3. Results of Exploratory Factor Analysis**

| Variables | Cronbach's Alpha | Items | Item loading | | | |
|---|---|---|---|---|---|---|
| Disposition to Value Privacy | 0.83 | DVP1 | .115 | .046 | **.860** | -.047 |
| | | DVP2 | .181 | .008 | **.820** | -.125 |

| | | | | | | |
|---|---|---|---|---|---|---|
| (DVP) | | DVP3 | -.039 | .080 | **.886** | -.002 |
| Trust Propensity (TRUST) | 0.92 | TRUST1 | .006 | .019 | -.117 | **.948** |
| | | TRUST2 | -.010 | -.025 | -.047 | **.958** |
| Privacy Concerns About Peer's Disclosure of one's information (PCAPD) | 0.89 | PCAPD1 | **.654** | .242 | -.011 | -.018 |
| | | PCAPD2 | **.828** | .201 | .082 | .042 |
| | | PCAPD3 | **.797** | .134 | .083 | -.079 |
| | | PCAPD4 | **.743** | .106 | .035 | .084 |
| | | PCAPD5 | **.728** | -.020 | .008 | .005 |
| | | PCAPD6 | **.800** | .297 | .150 | -.103 |
| | | PCAPD7 | **.707** | .233 | .171 | .040 |
| Information Privacy Protection Response (IPPR) | 0.78* | IPPR1 | **.522** | **.470** | -.033 | -.267 |
| | | IPPR2 | .270 | **.624** | .147 | .093 |
| | | IPPR3 | .185 | **.898** | .004 | .015 |
| | | IPPR4 | .180 | **.855** | .019 | -.063 |
| Eigen Value | | | 5.53 | 2.29 | 1.78 | 1.51 |
| *: Cronbach' Alpha of IPPR was calculated based on IPPR2, 3, and 4. | | | | | | |

### *Results on PCAPD*

The results of an ANCOVA test on the dependent variable PCAPD showed that H1, H3, and H4 were supported (see Table 4). No covariates had significant interaction with independent variables. However, the residuals of PCAPD did not meet the homogeneity or the normality requirement of the ANCOVA test. Hence, all significant results were confirmed with nonparametric tests.

In support of H1, the main effect of decisional control ($F=4.303$, $p<0.05$) was found to be significant. However, the main effect for social network overlap ($F=0.899$, $p>0.05$) was insignificant, lending no support to H2. In support of H3, the interaction, involving decisional control and social network overlap was significant in ANCOVA ($F=5.299$, $p<0.05$). As a reconfirmation under the violation of normality, we decomposed the data along social network overlap (Keppel 1991). In the condition of one overlap, a significant main effect for decisional control was detected ($F=6.718$, $p<0.05$) and confirmed by a Mann-Whitney test ($Z=-2.150$, $p<0.05$). Subjects given high decisional control had lower privacy concerns (mean=5.03, std=1.41) than those given low decisional control (mean=5.72, std=0.91). In the condition of zero overlap, no significant main effect for decisional control was detected ($F=0.129$, $p>0.05$) and confirmed by a Mann-Whitney test ($Z=-0.552$, $p>0.05$). Hence, for zero-overlap, decisional control appeared to have no impact on privacy concerns. Thus, H3 was supported (see Figure 3).

Similarly, the significant main effect for information exclusivity ($F=33.923$, $p<0.01$) was confirmed by a Mann-Whitney test ($Z=-5.748$, $p<0.01$). Subjects with highly exclusive information had higher privacy concerns (mean=5.77, std=0.93) than those with lowly exclusive information (mean=4.85, std=1.06). H4 was supported. However, there was no interaction between information exclusivity and decisional control ($F=0.010$, $p>0.05$) in either ANCOVA or nonparametric test. H5 was not supported.

**Table 4. Results of ANCOVA (Dependent Variable: PCAPD) $R^2$=36.7%**

| Source | | df | Mean Square | F | p |
|---|---|---|---|---|---|
| Covariates | Cookie Setting | 1 | .505 | .591 | .443 |
| | Disposition to Value Privacy | 1 | 8.834 | 10.330 | .002** |
| | Trust Propensity | 1 | .420 | .492 | .484 |
| | Gender | 1 | 1.226 | 1.434 | .233 |
| | Age | 1 | .371 | .433 | .511 |

| | | | | | |
|---|---|---|---|---|---|
| | Humanities/Sciences | 1 | 4.565 | 5.339 | .022* |
| | Graduate/Undergraduate | 1 | 1.003 | 1.173 | .281 |
| | SNS Experience | 1 | 4.860 | 5.683 | .018* |
| | Invasion of Privacy in Past | 1 | 3.122 | 3.650 | .058 |
| Main Effect | Decisional Control (DC) | 1 | 3.680 | 4.303 | .040* |
| | Social Network Overlap (SNO) | 1 | .769 | .899 | .345 |
| | Information Exclusivity (IE) | 1 | 29.009 | 33.923 | .000** |
| Interaction Effect | DC * SNO | 1 | 4.531 | 5.299 | .023* |
| | DC * IE | 1 | .008 | .010 | .922 |
| | SNO * IE | 1 | 1.952 | 2.282 | .133 |
| | DC * SNO * IE | 1 | .031 | .036 | .849 |
| *: p<0.05, **: p<0.01 | | | | | |

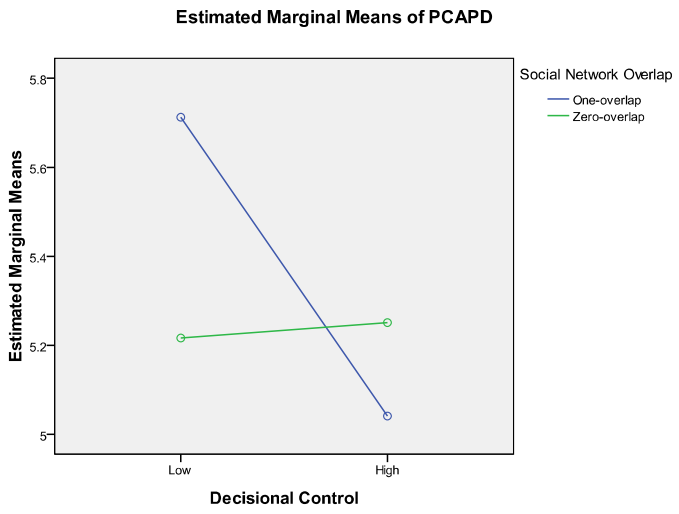


**Figure 3. Plots of Interaction Effect between Decisional Control and Social Network Overlap on PCAPD**

### *Results on IPPR*

A regression was conducted on the second dependent variable, IPPR (see Table 5). After excluding the effects of all manipulated factors and control variables, PCAPD still had a significant positive effect on IPPR (t=4.703, p<0.01). Thus, H6 was supported.

**Table 5. Results of Regression (Dependent Variable: IPPR)**

| | Standardized Coefficient | | |
|---|---|---|---|
| | Model 1 | Model 2 | Model 3 |
| Cookie Setting | .136 | .092 | .072 |
| Disposition to Value Privacy | .114 | .138 | .047 |
| Trust Propensity | .010 | .030 | .038 |

| | | | |
|---|---|---|---|
| Gender | .149 | .125 | .092 |
| Age | -.040 | .018 | .034 |
| Humanities/Sciences | .045 | .066 | .117 |
| Graduate/Undergraduate | -.047 | -.082 | -.111 |
| SNS Experience | .096 | .115 | .052 |
| Invasion of Privacy in Past | -.094 | -.070 | -.123 |
| Decisional Control | | .076 | .137 |
| Social Network Overlap | | .078 | .053 |
| Information Exclusivity | | .350** | .183** |
| PCAPD | | | .398** |
| $R^2$ | 8.6% | 21.5% | 32.1% |
| $R^2$ change | 8.6% | 12.9%** | 10.6%** |
| **: p<0.01 | | | |

# Discussion and Implication

## *Discussion of Findings*

The aim of this study is to identify the antecedents of privacy concerns about peer's disclosure of one's information (PCAPD) on SNSs. We propose that decisional control helps reduce members' PCAPD. Moreover, we theorize that the effect of decisional control on PCAPD is contingent on social network overlap (between the discloser and the disclosed) and information exclusivity. Four major findings can be derived from comparing our study in the online social context with previous studies in the online commercial context and with those in the offline social context.

First, the impact of decisional control on privacy concerns is contingent on social network overlap. In the condition of one overlap, high decisional control is more desirable than low decisional control to alleviate privacy concerns. Without decisional control, privacy concerns become much higher. In contrast, in the condition of zero overlap, decisional control seems immaterial in allaying privacy concerns. This result echoes with the CPM theory which theoretically argues that the permeability of privacy boundary will vary in terms of different disclosees (Petronio 2002). It also provides an empirical support for the theoretical argument of "selective control" effect in the Privacy Regulation Theory (Altman 1976). It contributes to the online privacy literature by suggesting that the effectiveness of privacy control strategy depends on pertinent disclosee.

Second, information exclusivity has a significant impact on members' privacy concerns about peers' disclosure. People have higher privacy concerns as the information exclusivity increases. The result suggests that the CPM theory can be applied to online context of social interactions (Petronio 2002). It extends prior study by suggesting that social privacy concerns could be affected by the kind of information in concern.

Third, the impact of decisional control on privacy concerns appears to be independent of information exclusivity. This could be due to the possible counter-effect of negative asymmetry (Labianca and Brass 2006). Prior research suggests that that negative events elicit greater physiological, affective, cognitive, and behavioral activities than neutral or positive events (Taylor 1991). Negative events arouse negative affective states which lead people to narrow and focus their attention particularly onto the negative information that seems to be the cause (Schwarz 1990). In the experiment, although negative affective states were aroused by both lowly and highly exclusive information, as a result of negative asymmetry, people may focus mainly on stressful events, and neglect the positive affects aroused by decisional control.

Fourth, when members have more concerns about peer's disclosure, they are more inclined to complain to SNSs as well as other friends. This finding resonates well with Son and Kim's (2008) study. Moreover, it extends the prior study by implying that social privacy concerns among members are detrimental to their loyalty to the SNS provider (e.g., complaining to other friends). Such negative word-of-mouth may turn back potential SNS users, trigger

current members to cease membership, or make them switch to other SNSs. This finding underlines the important role of social privacy in SNSs which has been neglected by prior studies.

### *Contributions*

From the theoretical perspective, this study makes important contributions to the privacy literature. First, this study explores the nature of privacy concerns about peer's disclosure of one's information in online social context. PCAPD is different from privacy concerns in e-commerce because of the complexity of social interactions. We extend the privacy research from online commercial context to online social context. We also provide a reliable and valid measurement for PCAPD which can be used in future studies.

Second, this study contributes to the privacy literature by advancing the theoretical development for privacy concerns in online social contexts. Because social privacy concerns are different from commercial privacy concerns, this paper provides a new theoretical model for social privacy concerns based on the CPM theory. It is proposed that people's social privacy concerns depend on the degree of control they have in deciding what kind of information (i.e., information exclusivity) would be disclosed, and to whom (i.e., social network overlap).

Third, this study reveals the role of an important antecedent of PCAPD – decisional control. While prior study focused on the effect of perceived control (Xu 2007), we employ actual control – decisional control (Skinner 1996). We posit that actual control deserves more attention because (1) perceived control is derived from actual control, and (2) manipulating actual control is a pragmatic approach to system design whereas perceived control is hard to measure and manipulate for system developers.

Fourth, this study examines the moderating effect of social network overlap. Although CPM theory implies that social relationships affects privacy concerns, it did not provide specific metrics for social relationship. Nor did it specify the pattern of effects. Our study illustrates that social network overlap can be regarded as a metric of online social relationships. Moreover, we also provide empirical support for the moderating effect of social network overlap.

Fifth, our study also highlights the role of information exclusivity as a proxy of privacy boundary. The concept of boundary has been suggested by the CPM theory; however, no empirical study has been carried out for it. We propose a new concept, information exclusivity, which can be used to differentiate a personal boundary holding private information and a collective boundary. Our study is the first attempt to incorporate this new concept into online privacy study. The direct effect of information exclusivity on social privacy concerns has been proposed and supported by our study.

From the practical perspective, this study also suggests a set of pragmatic strategies for SNSs to improve their privacy protection for members. First, SNSs should pay attention to reducing members' privacy concerns about peers' disclosure. Such privacy concerns will affect members' word-of-mouth and memberships in a long run.

Second, SNSs could reduce members' PCAPD by giving members higher decisional control on peer's disclosure of information related to them. For example, when the tagging function was first implemented, Facebook did not allow people to remove tags, which aroused high privacy concerns among members. Nowadays, Facebook has changed its strategy by allowing people to remove any tag that they are not comfortable with. However, according to our study, this strategy would still induce high privacy concerns because people have no choice before they are tagged by peers. It would be better for SNSs to consider equipping people with a power to disapprove peer's disclosure.

Third, SNSs can provide more functions for people to customize their privacy settings relating to on peer's disclosure. Because members often share a large number of friends between each other, customized decisional control is important to them. For example, if the SNS allows its members to choose from a list of who can see their information uploaded by peers, that would help reduce members' privacy concerns in social interactions.

Fourth, for SNS members, this study also sheds lights on the circumstances under which information privacy violations can have detrimental consequences. SNSs can suggest members to set privacy rules to the information they upload, hence remind members of possible consequences of disclosure, and assist members to properly manage the information in social interactions rather than incurring privacy concerns. Kaixin001.com, a popular SNS in China, represents a case for this point. It updated its privacy reminder mechanism recently. In the past, it allowed members to forward friends' posts freely. Now, when members forward others' posts, it will pop up a reminder asking them to think twice before diffusing others' personal information. This new policy is embraced by its

members. Members appreciate its efforts to create a healthy environment for them and to minimize their social privacy concerns.

Fifth, policy makers can also learn from this study to propagandize the importance of citizens protecting each other's privacy in all virtual communities. For example, the Australian Privacy Commissioner, have suggested SNS users to ask others for permission before disclosing others' information (Australian Privacy Commissioner 2009).

### *Future Research*

This line of research can be continued in several ways. First, this study shows that decisional control is useful for alleviating privacy concerns in online social contexts, especially when peers share common friends on SNSs. Besides decisional control, other ways to accomplish this purpose should be sought. One possibility is to allow people to have informational control (Skinner 1996), which refers to "a sense of control that is achieved when the self obtains or is provided with information about a noxious event" (Fiske and Taylor 1991, p.201). Informational control alerts in the recipient, helps the recipient to manage future surprises, and avail them of more privacy protections. Another direction for future research is to explore other privacy-preserving functions to realize decisional control. For example, decisional control can be achieved when SNS members are allowed to adjust the degree that their information can be searched. With the development of SNSs, more options for decisional control will become available for members. Because this study is an initial attempt to construct decisional control in the SNS context, more ways of operationalization would increase the convergent validity of this construct.

Second, the operationalization of social network overlap can be improved. Since members usually have many mutual friends on SNS, comparing more levels of overlap (e.g., zero, one, and fifty) could be considered in future studies. Another direction is to investigate the effects of other relational factors, e.g., intimacy between the disclosee and disclosed, on privacy concerns. Intuitively, people may not care about information disclosure to the closest friends because they believe that close friends would not hurt them. However, it is also possible that people interact a lot with close friends and feel unsafe that they might know too much about them.

Third, besides information exclusivity, it would also be useful to employ other typologies of private information, e.g., work-related information and life-related information. Some people may insist on demarcating between work and life. People may also worry about their colleagues' disclosure of identifiable information about their working content that is commercially confidential.

Fourth, this study focuses on the disclosure of disadvantageous information. It can be extended to information that may be advantageous to people to see whether people still care decisional control. It would be possible that people regard others' disclosure of advantageous information as another kind of privacy violation. However, the effect of control may be different from this study.

Fifth, the theoretical framework may be extended to other contexts where technology advances raise the issue of social privacy concerns. For example, practitioners are considering combining e-commerce websites with social networking websites, which may trigger multiple types of privacy concerns in the social-commercial contexts.

## Conclusion

In conclusion, this study served as an initial attempt to investigate information privacy concerns in online social contexts. It extends information privacy research into the social networking context. The results showed that higher decisional control reduces a member's PCAPD. When the discloser's social networks overlap with that of the disclosed, the effect of decisional control on PCAPD is stronger than when the two do not overlap. In addition, information exclusivity reduces PCAPD. This study suggests that future research in this direction is both theoretically important and practically interesting.

## Acknowledgements

We thank the Associate Editor and two anonymous reviewers for their many helpful suggestions on improving this paper.

## References


Ahearn, T. "Survey Finds College Students May Put Parents At Risk For Identity Theft," 2009.

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

Altman, I. "Privacy: A Conceptual Analysis," *Environment and Behavior* (8:1) 1976, pp 7-29.

Australian Privacy Commissioner "Are there any privacy risks associated with using social networking sites?," 2009.

Averill, J.R. "Personal control over aversive stimuli and its relationship to stress," *Psychological Bulletin* (80:4) 1973, pp 286-303.

Bies, R.J. "Beyond the hidden self: Psychological and ethical aspects of privacy in organizations," in: *Codes of conduct: behavioral research into business ethics,* D. Messick and A. Tenbrunsel (eds.), Russel Sage Foundation, New York, 1996, pp. 104-116.

Corah, N., and Boffa, J. "Perceived control, self-observation, and response to aversive stimulation," *Journal of Personality & Social Psychology* (16:1) 1970, pp 1-4.

Culnan, M.J., and Armstrong, P.K. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1) 1999, pp 104-115.

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

Deloitte "Social networking and reputational risk in the workplace - Deloitte LLP 2009 Ethics & Workplace Survey results," Deloitte, 2009.

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

Dwyer, C., Hiltz, S.R., and Passerini, K. "Trust and Privacy Concern Within Social Networking Sites: A Comparison ofFacebook and MySpace," the Thirteenth Americas Conference on Information Systems, Keystone, CO, 2007.

Finch, J. "The Vignette Technique in Survey Research," *Sociology* (21) 1987, pp 105-114.

Fiske, S.T., and Taylor, S.E. *Social cognition*, McGraw-Hill, New York, 1991.

Foddy, W.H., and Finnighan, W.R. "The Concept of Privacy From a Symbolic Interactionist Perspective," *Journal of the Theory of Social Behavior* (10) 1980, pp 1-17.

Greenberg, J., and Cropanzano, R. *Advances in Organizational Justice*, Stanford University Press, Stanford, California, 2001, p. 304.

Grimmelmann, J. "Facebook and the Social Dynamics of Privacy (Draft)," 2008.

Hui, K.-L., Teo, H.H., and Lee, S.-Y.T. "THE VALUE OF PRIVACY ASSURANCE: AN EXPLORATORY FIELD EXPERIMENT," *MIS Quarterly* (31:1) 2007, pp 19-33.

Johnston, M., and Vögele, C. "Benefits of psychological preparation for surgery: a meta-analysis," *Annals of Behavioral Medicine* (15:4) 1993, pp 245-256.

Jones, H., and Soltren, J.H. "Facebook: Threats to Privacy," Massachusetts Institute of Technology, 2005.

Justice, E. "Facebook suicide: the end of a virtual life," The Times, 2007.

Kelvin, P. "A Social-Psychological Examination of Privacy," *British Journal of Social and Clinical Psychology* (12) 1973, pp 248-261.

Keppel, G. *Design and Analysis: A Researcher's Handbook*, Prentice-Hall, Eaglewood Cliffs, New Jersey, 1991.

Kumar, N., and Benbasat, I. "The Effect of Relationship Econding, Task type, and Complexity on Information Representation: An Empirical Evaluation of 2D And 3d Line Graphs," *MIS Quarterly* (28:2) 2004, pp 255-281.

Labianca, G., and Brass, D.J. "EXPLORING THE SOCIAL LEDGER: NEGATIVE RELATIONSHIPS AND NEGATIVE ASYMMETRY IN SOCIAL NETWORKS IN ORGANIZATIONS," *Academy of Management Review* (31:3) 2006, pp 596-614.

Lewis, P., and Blanchard, E.B.l. "Perception of Choice and Locus of Control," *Psychological Reports* (28) 1971, pp 67-70.

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

Margulis, S.T. "On the Status and Contribution of Westin's and Altman's Theories of Privacy," *Journal of Social Issues* (59:2) 2003, pp 411-429.

Marshall, N.J. "Dimensions of Privacy Preferences," *Multivariate Behavioral Research* (9) 1974, pp 252-271.

Milardo, R.M. "Friendship Networks in Developing Relationships: Converging and Diverging Social Environments," *Social Psychology Quarterly* (45:3) 1982, pp 162-172.

Nunnally, J., and Bernstein, I. *Psychometric Theory*, McGraw-Hill, New York, 1994.

Nussbaum, B. "Facebook Suicide," BusinessWeek, 2007.

Perdue, B.C., and Summers, J.O. "Checking the Success of Manipulations in Marketing Experiments," *Journal of Marketing Research* (23:4) 1986, pp 317-326.

Petronio, S. *Boundaries of Privacy: Dialectics of Disclosure*, State University of New York Press Albany, 2002, p. 268.

Petronio, S., Sargent, J., Andea, L., Reganis, P., and Cichocki, D. "Family and Friends as Healthcare Advocates: Dilemmas of Confidentiality and Privacy," *Journal of Social and Personal Relationships* (21:1) 2004, pp 33-52.

Proshansky, H., Ittelson, W.H., and Rivlin, L.G. *Environmental Psycholgoy*, Holt, Rinehart and Winstion, New York, 1970.

Riphagen, D. "Privacy Risks for Users of Social Network Sites," 2008.

Rosenblum, D. "What Anyone Can Know: The Privacy Risks of Social Networking Sites," *IEEE Security & Privacy* (5:3) 2007, pp 40-49.

Schwarz, N. "Feelings as information: Informational and motivational functions of affective states," in: *Handbook of motivation and cognition: Foundations of social behavior,* R. Sorrentino and E.T. Higgins (eds.), Guilford Press, New York, 1990, pp. 527-561.

Sheng, H., Nah, F.F.-H., and Siau, K. "An Experimental Study on Ubiquitous commerce Adoption: Impact of Personalization and Privacy Concerns," *Journal of the Association for Information Systems* (9:6) 2008, pp 344-376.

Skinner, E.A. "A Guide to Constructs of Control," *Journal of Personality & Social Psychology* (71:3) 1996, pp 549-570.

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

Son, J.-Y., and Kim, S.S. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), September 2008, pp 503-529.

Sprecher, S., and Felmlee, D. "The Influence of Parents and Friends on the Quality and Stability of Romantic Relationships: A Three-Wave Longitudinal Investigation," *Journal of Marriage and the Family* (54:4) 1992, pp 888-900.

Sprecher, S., and Felmlee, D. "Romantic partners' perceptions of social network attributes with the passage of time and relationship transitions," *Personal Relationships* (7) 2000, pp 325-340.

Stone, E.F., and Stone, D.L. "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms," in: *Research in Personnel and Human Resources Management,* K.M. Rowland and G.R. Ferris (eds.), JAI Press, Green- wich, CT, 1990, pp. 349-411.

Taylor, S.E. "Asymmetrical effects of positive and negative events: The mobilization-minimization hypothesis," *Psychological Bulletin* (110) 1991, pp 67-85.

TopTenREVIEWS "2009 Social Networking Websites Review Product Comparisons," 2009.

Wang, D., Xu, L., and Chan, H.C. "Understanding Users' Continuance of Facebook: The Role of General and Specific Computer Self-Efficacy," in: *the Twenty Ninth International Conference on Information Systems*, Paris, France, 2008.

Watts, D.J. "Networks, Dynamics, and the Small-World Phenomenon," *The American Journal of Sociology* (105:2) 1999, pp 493-527.

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

Whetten, D.A. "What Constitutes a Theoretical Contribution?," *Academy of Management Review* (14) 1989, pp 490-495.

Xu, H. "The Effects of Self-Construal and Perceived Control on Privacy Concerns," in: *the Twenty Eighth International Conference on Information Systems*, Montreal, Canada, 2007.

Xu, H., Dinev, T., Smith, H.J., and Hart, P. "EXAMINING THE FORMATION OF INDIVIDUAL'S PRIVACY CONCERNS: TOWARD AN INTEGRATIVE VIEW," in: *the Twenty Ninth International Conference on Information Systems*, Paris, France, 2008.

Xu, H., Teo, H.H., and Tan, B.C.Y. "Information Privacy in the Digital Era: An Exploratory Research Framework," the Twelfth Annual Americas Conference on Information Systems, Acapulco, Mexico, 2006.

Xu, Y. *Survey Research*, Online Document, http://hi.baidu.com/research001, accessed on September 7, 2009.

Yougov "What does your NetRep say about you?," Viadeo, London, 2007.