PRIVACY IN ONLINE SOCIAL NETWORKS

Completed Research Paper

Nan (Andy) ZHANG[1]
Department of ISOM
Hong Kong University of Science and Technology
Clear Water Bay, Kowloon, Hong Kong
znxab@ust.hk

Chong (Alex) Wang
Department of ISOM
Hong Kong University of Science and Technology
Clear Water Bay, Kowloon, Hong Kong
alexwch@ust.hk

Yan XU
Department of ISOM
Hong Kong University of Science and Technology
Clear Water Bay, Kowloon, Hong Kong
xuyan@ust.hk

Abstract

Debates about privacy issues on the social networking websites never stop. As social media becomes ubiquitous, better understanding about users' privacy in the context of online social networks is critical. However, the information privacy concern used by e-commerce research is not sufficient to capture the specificities of individuals' privacy concern under this new context. In this paper, we propose and empirically validate a new multi-dimensional privacy concept fit to the complex features of online social interactions. Further, we propose that role related constructs are critical source of privacy concern in online social networks. The four dimensions of privacy concern aggregate to form general privacy concern which predicts individual's risk belief. Data were collected on the Amazon Mechanical Turks platform. Empirical results support the validity of the proposed scale of the multi-dimensional privacy concern construct. We also find evidence that the different dimensions of privacy concern may be influenced differently by role related constructs (role overload and role conflict).

Keywords: multi-dimensional privacy, privacy concern, online social network, role overload, role conflict

[1] corresponding author

Introduction

"People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time." – Mark Zukerberg, CEO, Facebook.

Social media sites and online social networks have become ubiquitous in just a few years. Sites like MySpace, Facebook, YouTube, and Twitter, to name a few, are experiencing explosive diffusion. The wide accessibility and fast dissemination of user-generated content through these sites and online social networks has intensified interpersonal communications, enhanced business transparency, and generated new value creation opportunities. It has led to an era of sharing where consumers have become the *prosumers*. At the same time, by making it easy to share valuable contents, the technology has also made the life of ordinary Internet users more "transparent". While the users enjoy the opportunity to share and learn, their online privacy is endangered, which, time and again, has drawn the attention of the government and even the relevant firms.

Debates about Internet privacy issues have been ongoing. Some argue that the norm about sharing personal information is changing and people are becoming more open with their personal information. While there is no doubt that people and society will adapt eventually to the technology environment, understanding and protecting Internet users' privacy is still critical for the government and the firms. The intensity of related discussions has been growing. For example, the recent change (December, 2009) in Facebook's privacy setting has generated uproar about how ordinary users can protect their online privacy[2]. As a reaction to growing online privacy concerns, policy actions have also been taken in the U.S., with Senators John Kerry and John McCain introduced the "Commercial Privacy Bill of Rights Act of 2011" that aims at protecting consumers' privacy, both online and offline.

In order to protect the privacy of Internet users, we need to understand what is considered as private and what is not; which aspects of privacy the users are concerned about; and which actions increase concerns about privacy and which ones reduce such concerns. In other words, we need to define the privacy of Internet users; understand its dimensions, its antecedents, and its consequences. To date, privacy concerns in the context of social media are not widely discussed in the academic literature. Most of previous research focused on e-commerce, where consumers' privacy concerns focus on factual personal information (Malhotra et al. 2004). In online social networks, information about individuals and interactions between them are much more in-depth than what a simple business transaction would entail. In fact, online social interactions are mostly interpersonal. Contents shared in online social networks cover all aspects of personal life and these are digitized and diffused through online social connections. Clearly, concepts about privacy in the context of e-commerce that focus on factual personal information only are not sufficient to capture all the ramifications of privacy in online social interactions. As a result, it is important to extend the definition of online privacy to reflect the complexity of online social interactions, and this is the primary goal of the paper.

To achieve this goal, we propose and test a multi-dimensional privacy concern construct tailored to the broader definition of privacy that is suitable to the context of social media. Specifically, we propose that online social network users are concerned about their *virtual territorial privacy*, *factual privacy, interactional privacy*, and *psychological privacy*. To explore the utility of this extended conceptualization of privacy, we propose a theory that links role related constructs (role overload and role conflict) to privacy concerns in online social networks. The four dimensions of privacy concerns then aggregate to form the general privacy concern that predicts the risk perception of Internet users.

Survey data is collected on the Amazon Mechanical Turks platform to test for the proposed scale and theory. We find support for both the validity of the construct and the proposed theory in our empirical tests. Interestingly, we find that while role overload and role conflict lead to virtual territorial,

[2] "Facebook faces criticism on privacy change." BBC news, Dec 10th, 2009 (http://news.bbc.co.uk/2/hi/8405334.stm).

interactional and psychological privacy concerns, they do not exhibit a significant effect on factual privacy concern. This finding reveals the uniqueness of privacy in online social interactions.

This paper contributes to the literature in several ways. In terms of theoretical contribution, we extend the previous definition of privacy concern. The multi-dimensional privacy concern construct is empirically validated. Our paper provides a theoretical foundation for future privacy research. We introduce role-taking theory to privacy research and show that role related constructs are important antecedents of privacy concerns. Consistent with previous literature, we also show that privacy concerns influence users' risk perceptions. In terms of practical implications, our study enhances the understanding about user privacy concerns in online social networks. It generates guidelines for website vendors and marketers trying to take advantage of social media and online social networks, about designing applications that safeguard privacy and release users from privacy concerns.

The rest of this paper is organized as follows. Section 2 presents the theoretical background. The research model and hypotheses are developed in Section 3. Section 4 describes our empirical studies and Section 5 presents the results. Section 6 concludes.

Privacy in Online Social Networks

The idea of privacy is intuitive. However, despite years of discussions among researchers, there is no agreement on the definition of "privacy" (Joinson and Carina 2007; Yao et al. 2007). One reason for this ambiguity in the literature is the complexity of the concept of privacy. Privacy involves different dimensions whose salience change with the context (Smith et al. 2011). Overall, scholars tend to conclude that privacy can mean different things to different people. Therefore, the roots and consequences of its violation depend on the context being considered (Bennett 1992).

Also contributing to the ambiguity in the concept of privacy are other overlapping concepts such as information security and information privacy perception (Dutta and McCrohan 2002; Margulis 2003a, 2003b). Some studies use global terms to represent both privacy and security concerns (e.g. Jones 1991). However, privacy and security are different psychological constructs. For example, on one hand, information security involves the protection of personal data (Belanger et al. 2002); on the other hand, information privacy focuses on the control over personal information and may include dimensions such as the collection, control, and awareness of the practices of privacy (Malhotra et al. 2004). Information security is a prerequisite for privacy protection. However, information security alone is not a sufficient safeguard against invasions to privacy, such as the secondary use of personal information by the vendor and the unauthorized access of personal information (Ackerman 2004). As for the perception of information privacy perception, it refers to the consumers' understanding on how their personal data are used and protected. It is based on the privacy construct and relates closely to the privacy concern construct. In this paper, we focus on the privacy construct and the privacy concern construct as they are broadly defined in the psychology literature. However, it is important to keep in mind the related concepts as we proceed.

To define privacy in the context of online social networks, we reviewed the literature on privacy as a psychological construct focusing on its sub-dimensions. Based on this review, we propose a multi-dimensional privacy construct that is general enough to capture the nuances in online social interactions.

Privacy as a Multi-dimensional Construct

The concept of general privacy originates from the classical discussions about privacy by Westin (1967). As one of the most frequently referred definitions of privacy in the IS literature (e.g. Malhotra et al. 2004; Smith et al. 1996), Westin (1967) defines the privacy as a multi-dimensional construct. Four types of privacy are identified there: solitude, intimacy, anonymity, and reserve. A series of follow up studies validate and extend Westin's original privacy definition (e.g. Marshall 1974; Burgoon 1982; Pedersen 1999; Phelps et al. 2000; Smith et al. 1996; Stone and Stone 1990). The focus of the discussion also evolve from the original emphasis on physical separation to the later discussion about psychological status.

There exist extensive discussions about privacy in the IS literature as well. However, previous privacy research in IS focuses on the information privacy in the context of e-commerce (Bélanger and Crossler 2011). Privacy within the context of online social networks has not been clearly defined (Dwyer 2007). As

stated in the introduction, compared to the e-commerce environment, social media and online social networks involve a different set of social interactions and information sharing activities that have similarities with offline social interactions. Privacy in such a context is multifaceted. Information privacy only captures a subset of the complete conceptualization of privacy in a broader context of online social interactions and communications among peers (Bélanger and Crossler 2011). For example, a survey conducted by Gross and Acquisti (2005) shows that, in addition to the concern about personal identity information, users of online social networking services have concerns about the disclosure of their political opinions as well. An extended conceptualization over information privacy is needed to reflect users' privacy concerns in the current online social environment.

In addition to extending the previous definition of privacy in IS literature, a new conceptualization of privacy in online social interactions should also reflect the specificities of the context. Extending Westin's (1967) privacy definition, Burgoon (1982) proposes a four-dimensional privacy concept that includes *physical privacy, informational privacy*, *interactional privacy*, and *psychological privacy*. Physical privacy refers to the degree to which a person is physically accessible. Informational privacy refers to an individual's right to determine how, when and to what extent the information about the person will be revealed to others. Interactional privacy refers to an individual's ability and effort to control social contacts. Psychological privacy refers to the ability to control inputs and outputs to form values, as well as the right to decide with whom and under what circumstances thoughts and intimate information will be shared or revealed. Compared to Westin's (1967) original conceptualization, the four-dimensional privacy definition gives a richer elaboration over the full range of an individual's personal and social experiences. In current online social networks, information exchange covers the full range of individual experiences, from social interactions with intimate friends to professional connections with work related contacts. As such, the four-dimensional privacy construct fits in with the context of online social interactions in terms of its coverage. We thus follow and extend the four-dimensional privacy conceptualization and develop a definition of privacy in the context of online social networks.

Multi-dimensional Privacy Concept in Online Social Networks

Based on the four-dimensional framework proposed by Burgoon et al. (1982), we propose the following four-dimensional privacy concept to reflect the broad spectrum of activities that take place in online social networks. Specifically, we propose that the integrity of virtual territory, the control over personal factual information, interactional freedom, and psychological independence are the major components of individual privacy in online social networks.

Virtual Territory Privacy

In the offline environment, physical privacy is defined as the freedom from surveillance and unwanted intrusions upon one's space by the physical presence, touch, sights, sounds, or odors of others. This privacy helps people to create a spatial and/or temporal buffer from intrusions and observations. Further, people have an innate need to possess objects (Burk 1900; Porteous 1976). "*The impulse to collect various objects is displayed by almost all human beings, and seems to be due to a true instinct*" (McDougall 1923). When ownership of an object is claimed, interactions with the object are considered as private. For example, in the offline environment, people use walls or fences to define and defend their private territories. Any unauthorized access to the individual's private territory within the walls or fences is considered as invasion of the individual's privacy.

In the virtual social context, there are no physical boundaries that help define the private territory. However, people still feel ownership of the digital belongings that they are entitled to or that are created by them (for example, web-logs, personal spaces, profile pages, etc.). The digital contents represent a person's virtual presence and comprise of a private virtual presence. Virtual presence is thus the natural extension of the physical existence to the online social environment. To maintain the separation of one's virtual presence, psychological boundaries are set to create a buffer from intrusions and interactions. Such boundaries make up an individual's virtual territory. Virtual territory privacy thus refers to the control that an individual has over who has access to his/her virtual private territory. We thus define the virtual territorial privacy as the freedom from surveillance and unwanted intrusions upon one's virtual space by others. As an example, Facebook users may post second-hand sales information on the Market Place application. However, it is not acceptable in most of the cases, for such information to be posted on the

Facebook Wall of their friends. In this case, Facebook Wall is considered as part of the virtual territory of a Facebook user. Posting unwanted information into that territory is considered to be a violation of privacy.

Factual Privacy

Factual privacy refers to ability to control identifiable personal information about oneself. This dimension of privacy is a reiteration of information privacy as defined in previous IS literature (see Bélanger and Crossler 2011; Smith et al. 2011 for comprehensive reviews) in the context of online social network. The emphasis of factual privacy is on issues about the access, collection, dissemination, and use of personal factual information. We choose to call it factual privacy to differentiate it from other dimensions of privacy that also depend on, but do not focus on, the flow of information.

Interactional Privacy

Individuals may feel compelled by or uncomfortable under some circumstances relating to social interaction. For example, conversation requests may be initiated obtrusively or at inappropriate times. Interactional privacy refers to people's ability to control their encounters with others with respect to when, where and with whom they want to interact. These controls satisfy an individual's needs for security, affiliation and intimacy. They help to limit interpersonal annoyances and avoid unwanted conversations or involvements (Knowles 1980).

Interactional privacy is critical in the context of online social networks where the temporal and spatial constrains of (physical) communications are removed by modern technologies. Electronic communication (e.g. instant message systems and emails) enriches the channel through which one can be reached by potential contacts. The by-product of enhanced accessibility is the loss of controllability of communication. With electronic communication, people are accessible as long as they are online, which greatly increase the occurrences of unwanted conversions. Interactional privacy is thus a critical aspect of privacy in the virtual environment.

Psychological Privacy

Another dimension that is missing from information privacy discussions is psychological privacy. People need the freedom to express their own views and the capability to hide themselves from norm that they do not agree with. Psychological privacy protects the individual from intrusions upon one's thoughts, feelings, and values. It includes the freedom to introspect, reflect, assimilate, plan, analyze, regroup, disclose, or seek advice. It also includes the freedom from intentional or unintentional persuasive pressures, assaults on one's ego, or other forms of cognitive and affective interference (Burgoon et al. 1989).

Personal experience is highly transparent in online social networks. The hyper-connectivity enabled by online social networks exposes people to a higher level of monitoring from others. Further, online social networks often compose of contacts from different social circles of the users. This means that monitoring not only intensifies but also diversifies. Such increase in monitoring exposes people to sources of psychological intrusion and may lead to insecure feelings about psychological independence as well as preventative behavior. One striking example of psychological intrusion in the online social network is the "post-breakup Facebook effect", where the breaking up of a personal relationship exposes the related parties to judgments from different parts of their entire social circles.

Privacy Concern

Conceptually, privacy relates to the degree of control over access to self. However, the actual content of privacy depends more on the cognition and perception than on rational assessments. It is thus nearly impossible to measure privacy itself directly (Smith et al. 2011). Instead, most of the empirical privacy research measures privacy concern as a proxy for privacy cognition. The antecedents and consequences of privacy are mostly directly related to privacy concern. Following this line of thoughts, we propose and test a measure of privacy concern rather than privacy itself. As defined in the previous discussion, privacy relates to the degree of control that an entity has about privacy components. Privacy concern is defined as the "*individual's subjective views of fairness within the context of privacy*" (Malhotra et al. 2004). Studies in the IS literature have proposed the operationalization of information privacy concerns in different contexts (Malhotra et al. 2004, Smith et al. 1996, Stewart and Segars 2002), and this serves as the basis

for our operationalization of the concern for multi-dimensional privacy in the context of online social networks. Based on the proposed four-dimensional privacy concept, privacy concern refers to an individual's subjective views of fairness in losing the ability to control his/her virtual territorial, factual, interactional, and psychological privacy.

It is important to note is that, while in empirical analyses it is essential to focus on one technology platform to keep the discussion concrete, the extended privacy definition discussed in this paper is not narrowly designed with respect to any specific technology or application. Our goal is to extend the discussion of privacy to reflect the complex nature of current online interactions that reach every corner of one's personal life.

Theory Development

To establish the utility of the extended privacy concept, it is necessary to explore the nomological network around it. In this section, we develop a theory that links role taking behavior to the multi-dimensional privacy concern. The four dimensions of the privacy concern constructs are then aggregated to predict the general privacy concern that in turn is linked to the risk perception about sharing information on an online social network. The theory development is exploratory, focusing on discussing the relationship between the role taking behavior and the proposed privacy constructs. Our research model is shown in Figure 1.

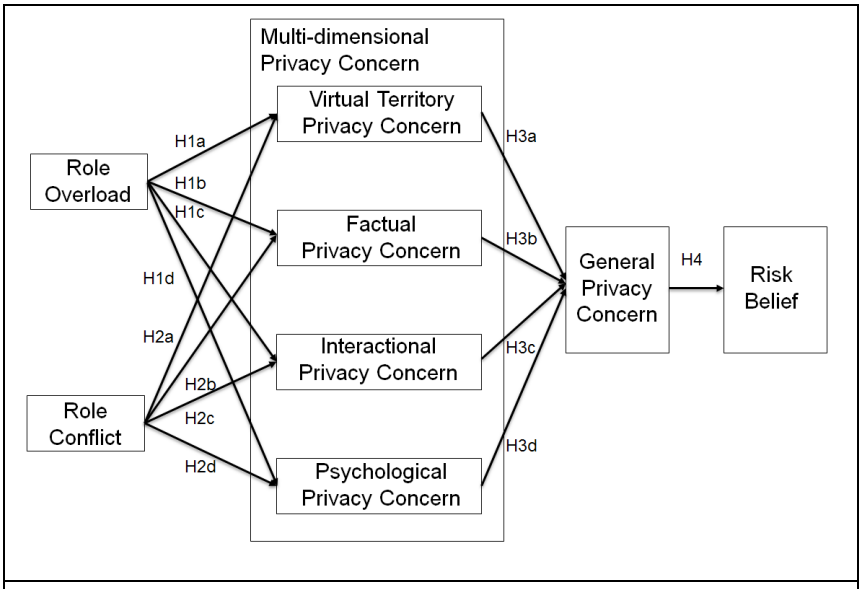


Figure 1. Research Model

Role Taking in Online Social Networks

Online social networks free individuals from the geographical boundary and alter the structure of social interactions. Communication in online social network is not constrained by temporal and spatial separations. Internet technology thus blurs the natural boundaries of social communications that help individuals to separate their social networks. Unlike in the traditional offline networks, online social network is a platform where all kinds of the individuals' social connections collocate. A typical Facebook user may connect to his/her family members, co-workers, classmates, and pure online acquaintances simultaneously. In such a situation, individuals need to switch between roles constantly in different activities. A survey conducted by Hoadley et al. (2010) has shown that the more the number of friends a user has on Facebook, the more likely it is that the user would adjust his/her privacy settings. This suggests that role structures may influence an individual's privacy concern.

A role is generally defined as a person's perception about himself/herself when he/she relates to the surrounding environment and people he/she interacts with (Hall 1971). Roles are evoked in social

activities to help people behave (Perlman 1968). Each role is associated with a different set of role expectations. People need to take on different roles in different social environments (social networks). The role needs to be changed when the environment changes. For example, an individual may take on a role as a subordinate at work, as a son in family, or as a partner in some collaborative effort. When people have to conduct cross (social network) boundary activities, they need to switch their roles accordingly. The role transitions become more difficult when a person moves among more segmented roles (Ashforth et al. 2000). Role overload and role conflict are two consequences of role transitions (Friday 1980, 1983; Friday and Hage 1976).

Role overload refers to the extent to which various role expectations regarding the focal person exceed the amount of resources available for their accomplishment (Bostrom 1981). An individual is limited in the amount of information he/she can process within a given period of time (Carpenter et al. 1994). Due to cognitive constraint, an increase in role overload results in having limited time and cognitive resources to assimilate and interpret new information (Ho et al. 2003). An individual with a high degree of role overload will feel that the available resources are inadequate to deal with multiple role demands (Kahn et al. 1964). For example, an individual can be occupied by several conversations started by different groups of people and therefore would have difficulty to really engage in each activity.

Role conflict is defined as the incompatibility and incongruity in the expectations between different roles (Guimaraes and Igbaria 1992). It describes the extent to which role expectations from the counterparts are incongruent with the norms, standards, or values of another role taken by the focal person (Goldstein and Rockart 1984). The main source of role conflict is role transitions caused by boundary spanning activities (Baroudi 1985; Lysonski 1985). When people participate in a social group, they intend to behave and evaluate themselves along the same dimensions and values that are used by the group in evaluating its members. The norms of the group provide a frame of reference for perceiving and evaluating oneself. However, the norms are usually different across different social networks or groups. As a result, other peers from different networks may try to evaluate the focal person based on different norms. When social activities are conducted across multiple networks with conflicting norms, it is hard for an individual to fulfill these conflicting expectations at the same time. For example, people from job related networks tend to evaluate an individual by how hard he/she is working while people from a game group may evaluate an individual by how much he/she can earn from the game.

Role and Privacy Concern

To get out of multiple roles, people need to be isolated from some social networks. According to what can be loosely described as the "boundary theory" (Michaelsen and Johnson 1997; Nippert-Eng 1996; Zerubavel 1991), individuals create and maintain boundaries as a means of simplifying and ordering the social activities. "Home," "office," and "church" are examples of the social domains created by boundaries (Nippert-Eng 1996). Xu et al. (2008) also suggest that each individual forms a physical or virtual space around him/her with clearly defined boundaries. Depending on the situational and personal conditions, individuals can choose to disclose the information across different boundaries or keep them completely private.

When social interactions are moved online, traditional boundaries become blurred. To reduce the pressure from multiple role expectations, an individual needs new ways to better control the boundary. Private virtual territory serves such purposes. In an online social network, the more the number of roles that an individual has to take on, the more role expectations the individual needs to handle and satisfy, and the more important it is for him/her to keep the boundaries clear. Further, when there are conflicts between the different roles that an individual has to take on, the need to keep these conflicting roles separate grows stronger. Therefore the need to control the boundary between different roles is even stronger. Limiting the access of different parties to the private space can lead to the avoidance of unfavorable consequences. For example, a user may want to prevent his/her spouse and coworker to debate about the importance of work and life on his Facebook page. Therefore, we expect both role overload and role conflict to have positive effects on an individual's virtual territory privacy concern.

H1a: The degree of role overload positively relates to an online social network user's virtual territorial privacy concern.

H2a: The degree of role conflict positively relates to an online social network user's virtual territorial privacy concern.

Consistent with previous e-commerce research, in online social networks, people are concerned with the unauthorized collection, distribution, and use of their personal factual information. When a user needs to take multiple roles in online social network, it is hard for him/her to fully identify and manage the potential access to identifiable personal information. Furthermore, as the online social network grows more complex, it becomes harder to control the ways in which that information is used. As a result, concerns about factual privacy will increase with role overload. Further, when there is a conflict between the different roles, individuals need to take extra care about their identifiable information as the access and usage of the information may also be in conflict.

H1b: The degree of role overload positively relates to an online social network user's factual privacy concern.

H2b: The degree of role conflict positively relates to an online social network user's factual privacy concern.

Human conversations are governed by "unspoken rules" (Taylor and Van Every 2000). Participants cannot allow gaps of silence, cannot intentionally overlap in speaking, and should remain attentive in anticipation of their speaking turns (Sacks et al. 1974). Although technologies, such as chat software, can help individuals handle multiple conversations at the same time, extra effort is required to follow the "unspoken rules" in each conversation (Reinsch et al. 2008), and individuals need to change their roles from conversation to conversation in order to behave appropriately. When the number of contacts from multiple networks becomes excessive, the chance of being involved in multiple open conversations increases, and this may become overwhelming. An individual will feel exhausted when trying to fit into the "rules" of different conversations simultaneously. The resulting stress increases the motivation for the individual to seek greater interactional privacy (Burgoon 1982). Further, when the open conversations involve conflicting roles, they overload the individual even faster. As an example, it would be hard to have a conversation with one's wife about kids' education while engaging in another conversation about the prospects of an ongoing project on Facebook chats. As a result, we expect that both role overload and role conflict lead to higher concern about interactional privacy.

H1c: The degree of role overload positively relates to an online social network user's interactional privacy concern.

H2c: The degree of role conflict positively relates to an online social network user's interactional privacy concern.

The Internet often symbolizes greater democracy, and individuals express opinions freely online. However, social influence and social pressure are also present on the Internet, especially with the advent of online social networks. When exposed to different social circles simultaneously online, psychological freedom may be significantly compromised. In online social network, opinions from different sources are presented simultaneously, which leads to information overload and can be confounding. The more roles a person takes on, the more role expectations and norms he/she has to adhere to. It becomes difficult to balance role exceptions or norms and to form opinion freely. Furthermore, conflicting roles may compete and making decisions may become even harder. Psychological privacy concern increases as a result of the increase in role overload and role conflict.

H1d: The degree of role overload positively relates to an online social network user's psychological privacy concern.

H2d: The degree of role conflict positively relates to an online social network user's psychological privacy concern.

General Privacy Concern

As discussed, it is important to extend the privacy concern construct and add specificity when extending the discussion on privacy to the context of online social networks. Only by opening the "box" of general privacy concern can one discover the nuance in the theory about privacy in online social networks. Each dimension of the extended privacy construct may appear separately and have different antecedents and

consequences. Meanwhile, different dimensions of privacy aggregate to form the general privacy concept (and concern) that influences the overall beliefs (such as the risk belief about sharing behavior) and attitudes. In the current discussion, we propose the four dimensions of privacy concern to aggregate to a general privacy concern that is then used to predict risk perception.

H3: The four dimensions of privacy concern aggregate to form the users' general privacy concern.

Risk Belief

The risk belief about information sharing is defined as the expectation that a high potential for loss is associated with the release of personal information to the public (Dowling and Staelin 1994). In the context of e-commerce, previous research finds that an individual's privacy concerns influence his/her risk belief. A positive correlation between privacy concern and risk belief is generally supported (Dinev et al. 2006; Dinev and Hart 2004, 2006; Malhotra et al. 2004; Milne and Rohm 2000; Miyazaki and Fernandez 2002; Sheehan and Hoy 2000; Stewart and Segars 2002; Van Slyke et al. 2006; Xu et al. 2005). Similarly, in online social networks, we expect general privacy concern to lead to higher risk belief about information sharing on social networking platforms, which leads to the following hypothesis.

H4: Online social network users' general privacy concern will have a positive effect on their risk beliefs on information sharing.

Control Variables

Several factors besides those we have theorized about, may also influence online social network users' privacy concern and risk belief. For example, it is shown that personal traits influence people's risk beliefs (Mayer et al. 1995; McKnight et al. 1998). To control for these confounding factors, we include several control variables in the model. This also provides additional support for the nomological validity of the proposed privacy constructs.

Based on related discussion, first, we control for demographic characteristics of the participants, including gender, age, income, and education (Culnan 1995, Milne and Rohm 2000, Phelps et al. 2000, Wang and Petrison 1993). Second, we control for experiences, including Internet experience, experience about identity information falsification, experience about privacy invasion, and media exposure about incidents of privacy invasion (Culnan 2000; Hoffman et al. 1999; Malhotra et al. 2004; Milne and Rohm 2000; Miyazaki and Fernandez 2001; Pew Internet Project 2000; Phelps et al. 2000; Smith et al. 1996). Third, we control for the user's trust level towards the vendor of a social networking website. Finally, since some online social networks provide privacy setting functions to help users manage their privacy, we also include privacy setting system usage as a control variable.

Method

Study Context and Sample

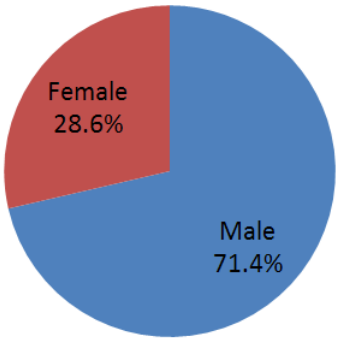
The approach we take in empirically testing our proposed theoretical constructs and research model is a field study using a survey for data collection. Given our research interest in online social networks and the popularity of websites, we choose Facebook as the target Internet social networking service. Besides being widely adopted, Facebook has received intense media attention about its privacy practices. As a result, participants in our research are more likely to have intensive use of the service, and be aware of the privacy issues there. The percentage of people who have been exposed to the invasion of privacy on the site and who have heard extensively about privacy invasion on the site from media are 17.6% and 61.4% respectively.

Answering the call for a more diverse sample frame in privacy research (Bélanger and Crossler, 2011), we use online survey to collect data. The main data collection is implemented with the Surveymonkey platform[3]. Participants are recruited from Amazon's Mechanical Turk Platform (henceforth Turk)[4]. On

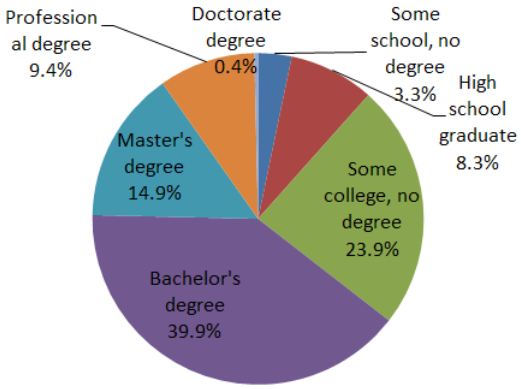
3 http://www.surveymonkey.com/

Turk, tasks are published by requesters. Workers can then accept the assignment and complete the task. Payments are made after the requesters review the completed task. Each worker has a unique worker ID associated with his/her working history on Turk. If a worker has been rejected too often, future requesters can forbid him/her from taking up their tasks. This offers a reputation mechanism that motivates workers to treat each assignment they accept seriously. For our survey, we gave 3 US dollars for each complete response, which is comparable to similar tasks on Turk. The researchers go through each response carefully before accepting it. Low quality responses are rejected. Prior to conducting the analysis, we screen the dataset for outliers using Cook's Distance. We exclude 20 cases that met the minimum criteria set by Bollen and Jackman (1990). The final sample size is 276. This procedure allows us to collect responses from a more diverse population as compared to US-centric, student sample that is dominant in previous research on information privacy. In our sample, 28.6% are female, 64.5% hold a Bachelor's degree or above. The majority of the respondents are between 21 and 30 years of age, with the average being 25. Over half (53.3%) of the respondents are Indian, followed by White (23.6%). On average, our respondents have 9 years of Internet experience and 180 friends on Facebook. The following figures illustrate our sample distribution. Ipeirotis (2010) conducts a survey about the demographic distribution of Turk workers, which reveals similar patterns as our sample.

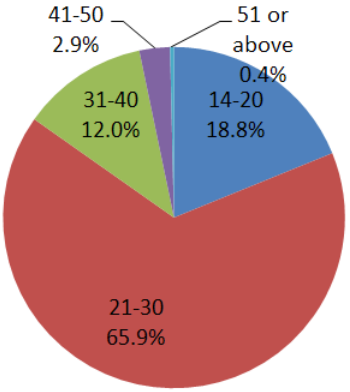
Gender Distribution



Education Distribution



Age Distribution



Ethnic Group Distribution

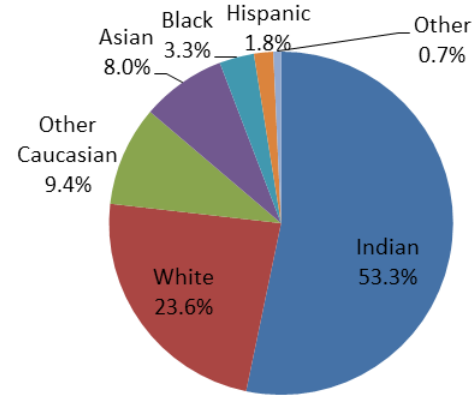


Figure 2. Sample Distribution

4 https://www.mturk.com/mturk/welcome

Scale Development

All research constructs are measured using multi-item scales (see the appendix). Scales for global privacy concern are adapted from Malhotra et al. (2004) and Smith et al. (1996). Scales for risk belief are adapted from Jarvenpaa and Tractinsky (1999). Scales for role overload are adapted from Duxbury et al. (1992), Ho et al. (2003), and Peterson et al. (1995). Scales for role conflict are adapted from Moore (2000), Rizzo et al. (1970), and Rutner et al. (2008). All items are revised to fit the context of online social networking services. Seven-point scales, anchored with "1 = strongly disagree" and "7 = strongly agree", are used.

As the four-dimensional privacy construct is new, we need to design scales to measure the proposed construct. In our scale development, we use a multi-stage iterative procedure following the approach proposed by Agarwal and Karahanna (2000). First, existing scales from Burgoon (1982), Burgoon et al. (1989), and Malhotra et al. (2004) are reviewed and modified to assure their fit with the research context. An initial set of items is then constructed, drawing upon prior work and our underlying conceptualization. These items are discussed with fellow researchers and frequent users of social networking websites through face to face interviews (convenient sample). Interviewees are asked to complete a draft questionnaire as well as to discuss privacy issues they face in their usage of social networking services. Based on the comments from these interviews, the initial items are then revised, where some items are dropped from the study, while others are added. The updated items are then tested in two consecutive pilot studies. The first one is conducted among 56 (out of 200) students enrolled in an undergraduate level business class from a well-known university in Hong Kong. Based on the analysis of this small student sample, items that are confusing or confounding are revised again. Then, a second pilot study is conducted on Amazon's Mechanical Turk Platform. 50 responses are collected. Some useful comments from the participants of the second pilot study are incorporated. Results of the pilot tests based on the data collected are then used to further refine the research scales and establish preliminary convergent and discriminant validity.

The final scales used in the study as reported in this paper consist of three items for virtual territorial privacy concern, six items for factual privacy concern, four items for interactional privacy concern, and four items for psychological privacy concern. Detailed description of the final items and our references are discussed in the appendix. Throughout the scale development process, considerable effort is made to ensure that each statement captures precisely, without confusion, the intended meaning of a specific dimension of privacy concern in online social networking context.

Results

We use SmartPLS[5] for data analysis. PLS is suitable for handling a large number of constructs (Chin 1998). Compared to covariance-based structural models, PLS is more flexible and thus is more appropriate for exploratory studies aiming at finding new theories or extending the current literature to new contexts (Gefen et al. 2000). Since the main focus of the current study is about extending current privacy concern constructs and exploring potential antecedents, we choose to use PLS as the main method for empirical analyses.

Measurement Model

Descriptive statistics for the research constructs are shown in Table 1. Consistent with the literature, all the constructs are modeled as reflective in the empirical analysis.

To discover discernible patterns of privacy dimensions, we performed an exploratory factor analysis (EFA) with SPSS first. The data was examined using principal components analysis as the extraction technique and varimax as a method of rotation. Four components are extracted. About 67.05% variance can be explained under this setting. All indicators, except InterP1 for interaction privacy concern, load more highly on their own construct than on other constructs (see appendix).

[5] SmartPLS, version 2.0-M3 (http://www.smartpls.de/forum/release.php)

We assess internal consistency and convergent validity by examining the item loadings, average variance extracted (AVE), composite reliability, and Cronbach's alpha (Gefen and Straub 2005). All the item loadings except for the two relating to general privacy concern (0.686 and 0.697) are higher than 0.707 as reported in the appendix. Although standardized loadings of 0.707 or greater are needed for the shared variance between each item and its construct to exceed the error variance, loadings between .60 and .70 are considered acceptable if the loadings of the other items within the same construct are high (Chin 1998). Furthermore, while removing them would improve the psychometric properties of the measures, it would also reduce the content validity of the constructs. Therefore, we keep these two items. The scores of composite reliability are higher than 0.842. The scores of AVE are higher than the recommended 0.5 value. The Cronbach's alpha values for all constructs are above the recommended 0.7 value, indicating good reliability. As a result, the internal (convergent) validity is supported (Chin 1998; Fornell and Larcker 1981; Kamis et al. 2008; Nunnally 1967).

Table 1. Descriptive Statistics

Construct	Abbr.	Mean	Std. Dev.	Cronbach's α
Virtual Territory Privacy Concern	TerrPC	4.166	1.439	0.719
Factual Privacy Concern	FactPC	5.187	1.143	0.879
Interactional Privacy Concern	IntePC	3.768	1.339	0.790
Psychological Privacy Concern	PsyPC	4.042	1.410	0.872
General Privacy Concern	GenPC	4.387	1.120	0.767
Risk Belief	Risk	4.218	1.302	0.884
Role Overload	RO	3.334	1.369	0.916
Role Conflict	RC	3.496	1.314	0.819

To assess the discriminant validity of our measurements, we compare the square root of each construct's AVE with the maximum of the absolute values of its correlations with other constructs as suggested by Chin (1998). As shown in Tables 2, the square root of AVE of each construct in our model (in the diagonal cells) is significantly larger than its correlation with the other constructs. As a result, the discriminant validity is satisfactory. In addition to this comparison, we also calculate cross-loadings between items using the procedure recommended for PLS (Gefen and Straub 2005). The result suggests that all items load highest on the constructs they are measuring (see appendix). Further, the differences are all higher than the suggested threshold of 0.1 (Gefen and Straub 2005). Thus, the discriminant validity of our measurements is supported.

Taken together, the above results suggest good measurement properties.

Table 2. Correlation Matrix and Average Variance Extracted

	Composite Reliability	1	2	3	4	5	6	7	8
1 TerrPC	0.843	0.801							
2 FactPC	0.908	0.343	0.788						
3 IntePC	0.864	0.566	0.129	0.783					
4 PsyPC	0.913	0.464	0.256	0.600	0.851				
5 GenPC	0.842	0.480	0.477	0.406	0.469	0.718			
6 Risk	0.920	0.380	0.403	0.236	0.358	0.658	0.861		
7 RO	0.933	0.409	-0.043	0.459	0.382	0.283	0.218	0.816	
8 RC	0.879	0.346	-0.011	0.481	0.389	0.219	0.157	0.704	0.803

Notes:
Square roots of the AVE are reported in the diagonal cells.

Structural Model

With an adequate measurement model in place, the structural model is tested. To test for the significance of path coefficients, we run a bootstrap analysis with 500 samples and calculate the t-statistics. The resulting model explains a significant amount of variance in the dependent and mediating variables. Figure 3 presents the standardized path coefficients and the explained construct variances.

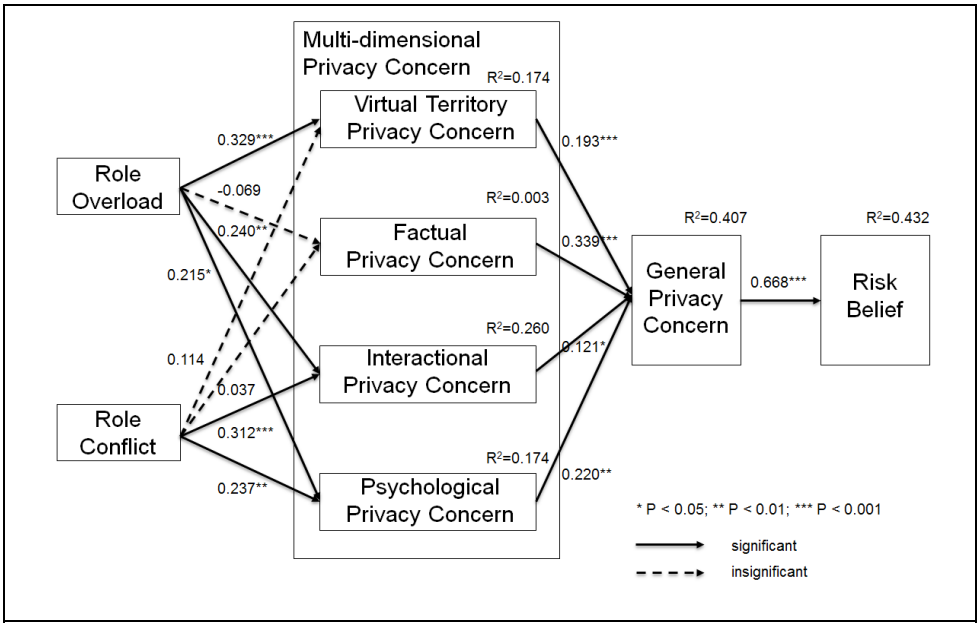


Figure 3. PLS Result

Role overload and role conflict together explain 17.4% of the variance in virtual territorial privacy, 0.3% of the variance in factual privacy concern, 26.0% of the variance in interactional privacy concern, and 17.4% of the variance in psychological privacy concern. The multi-dimensional privacy concern construct accounts for 40.7% of the variance in general privacy concern. General privacy concern can explain 43.2% of the variance in risk belief.

Table 3. Summary of Hypothesis Tests

Hypothesis		Path Coefficient	Significant Level	Support	Effect Size	Statistical Power
H1	a: RO -> TerrPC	0.329	P < 0.001	Yes	0.202	0.791
	b: RO -> FactPC	-0.069	P = 0.407	No	0.002	0.053
	c: RO -> IntePC	0.240	P < 0.010	Yes	0.285	0.966
	d: RO -> PsyPC	0.215	P < 0.050	Yes	0.177	0.694
H2	a: RC -> TerrPC	0.114	P = 0.167	No	0.144	0.542
	b: RC -> FactPC	0.037	P = 0.653	No	0.000	0.000
	c: RC -> IntePC	0.312	P < 0.001	Yes	0.312	0.984
	d: RC -> PsyPC	0.237	P < 0.010	Yes	0.183	0.719
H3	TerrPC -> GenPC	0.193	P < 0.001	Yes	0.410	0.999
	FactPC -> GenPC	0.339	P < 0.001	Yes	0.390	0.999
	IntePC -> GenPC	0.121	P < 0.050	Yes	0.295	0.974
	PsyPC -> GenPC	0.220	P < 0.001	Yes	0.383	0.999
H4	GenPC -> Risk	0.668	P < 0.001	Yes	0.845	0.999

The path coefficients are shown in Figure 3.

H1a, H1c, and H1d are supported. Higher level of role overload leads to higher concerns on virtual territorial privacy concern, interactional privacy concern, and psychological privacy concern. As expected, multiple roles make it more difficult for people to protect virtual territorial integrity, interactional freedom, and psychological independence. However, role overload does not influence people's concerns about disclosing identifiable information (H1b). While participants reported the highest score on the factual privacy concern (with mean at 5.187), role overload does not lead to factual privacy concern. One explanation for this is that although people are concerned about inappropriate access and use of their information, the target of this concern is third parties rather than their online peers. For online peers, they are willing to provide identifiable information due to the level of trust established.

Role conflict is a significant predictor for both interactional privacy concern (H2c) and psychological privacy concern (H2d). We do not find significant effects of role conflict on virtual territorial privacy concern (H2a). It appears that conflicting roles do not necessarily lead to higher concern about invasion of personal space as overload roles do. This suggests that, for virtual territorial privacy concern, simultaneous multiple role-taking is more detrimental than taking conflicting roles. We also do not find any significant effect of role conflict on factual privacy concern (H2b). Again, this may be caused by the fact that online peers may have a higher level of trust among themselves.

In general, the dimensions of privacy concern have significant loading on general privacy concern (supporting H3). The PLS results also provide strong support for H4, which is consistent with the previous study (e.g. Malhotra et al. 2004). Thus, general privacy concern is a significant predictor of a user's risk belief about information sharing.

Summarized results for the hypothesis tests are shown in Table 3. As a supplemental analysis, we examine a model containing additional direct paths from role overload and role conflict to risk belief in order to determine if the data supports the posited full mediation of the effects of role constructs on risk belief by privacy concern constructs. The result suggests that the direct paths from role constructs to people's risk belief are not significant. Following the procedure in Cohen (1988), we analyze the statistical power and effect size for each link in our model. The results are shown in Table 3. Low power for insignificant results is common when the sample size is not very big. This indicates that the sample may not be sufficient to reveal all the real relationships and that future research is needed (Cohen 1988; Goodhue et al. 2007).

Control Variables

To control for confounding factors such as individual characteristics, we conduct a supplemental analysis with several control variables. Several results of the analysis deserve attention. Specifically, older participants exhibit less concern about the risk of information sharing. Previous experience with any invasion of privacy and the amount of exposure to media reports of incidents of privacy invasion increase people's privacy concerns, while the trust toward the site vendor reduces users' general privacy and risk beliefs. The privacy setting function provided by Facebook reduces people's factual privacy concern. Female users on average perceive higher risk about online social networking but are less concerned about interactional privacy. The results indicate areas for potential improvement in any future study.

Conclusion

The objective of this study is three-fold: (1) to extend the definition of privacy in IS literature to reflect the state of privacy in online social networks, (2) to develop a reliable and valid scale for the multi-dimensional privacy concern construct, and (3) to develop and test a causal model centering on multiple-dimensional privacy concerns, role overload, and role conflict.

With the proliferation of social media, IS research about privacy should be moved from information privacy to a broader area that covers the full spectrum of online privacy concerns. We propose and find that the multi-dimensional privacy concern construct is able to capture the specificity of privacy concern of users of online social networks. Our results also demonstrate that the role related constructs are important antecedents to privacy concerns. Further, different dimensions have different loads on role constructs as well as on general privacy concern. This further validates the necessity to open the issue of general privacy and discuss the subtle nature of different dimensions of privacy constructs.

Our research makes several contributions. Theoretically, we extend the definition of privacy in the context of online social networks. The multi-dimensional privacy concern construct is a useful tool for analyzing users' privacy concerns and behavioral reactions to various privacy threats in online social networks. Second, we develop and empirically validate measurement scales for the multi-dimensional privacy concerns. Third, we build an exploratory theory featuring role related constructs as antecedents to privacy concerns. While privacy is intensively discussed, the research on the antecedents of privacy concerns is not sufficient (Smith et al. 2011). The introduction of role theory to this literature will extend our understanding of the predictors of people's privacy concerns.

In terms of practical contribution, we provide guidelines for the managers to discuss the different aspects of user's privacy in their services. Users' privacy concerns are multi-dimensional. There is probably no single function that can fulfill all privacy protection requirements. Further, our study can remind the vendors of online social networking services that more friends do not always provide positive influence to their users. If users cannot control their networks, pressure will arise due to the role overload and role conflict, which in turn lead to higher concerns about privacy and lower motivation of information sharing. Functions need to be developed for users to manage their own online social networks. For example, the recently launched Google Plus service provides users a new function, Google Circles. On Google Plus, users put people from different aspects of their lives into different "circles", that is, groups or categories. For each activity on the site, users can specify exactly which circle is the intended audience. With this function, Google has solved the layers-of-privacy problem that has dogged Facebook for years. People can share the right things with the right people easily and create clear boundaries between circles in their online social network. This alleviates the factual privacy concern that arises from role overload and role conflict. Users can also click on a circle to filter the scrolling blurbs. For example, people may want to view only work-related posts. The filtering then helps them to block unwanted information from certain groups. The function thus enables users to manage psychological privacy in an information rich environment. Overall, Google's new design significantly alleviates privacy concerns in different aspects. However, there are still some aspects (for example, virtual territory and interaction) of privacy concern that are left unsolved, which calls for future innovations and refined view about online privacy.

In conclusion, the goal of this paper is to enrich our understanding of users' privacy concerns in online social networks. We propose a multi-dimensional privacy concept that extends previous discussion about information privacy in IS literature. We believe fruitful future discussion could be built upon this extended conceptualization of user privacy (concern). While the theory proposed in the current work is quite exploratory, it does show the value of adding specificity to any discussion about privacy.

Acknowledgement

This project is financially supported by the funding from Research Project Competition (RPC) established by the University Grants Council (UGC) of Hong Kong University of Science and Technology. The project number is RPC11BM20.

Appendix

Research Constructs and Measures

Virtual Territorial Privacy Concern: Seven-point scales anchored with "strongly disagree" and "strongly agree". Adapted from Burgoon (1982), Burgoon et al. (1989) and altered to fit the context of online social network.

(1) It bothers me if my friends on Facebook access my homepage, wall, or album without my authorization.
(2) It bothers me if my friends on Facebook leave unwanted comments on my homepage or wall.
(3) My Facebook is my private territory.

Factual Privacy Concern: Seven-point scales anchored with "strongly disagree" and "strongly agree". Adapted from Malhotra et al. (2004) and altered to fit the context of online social network.

(1) I have the right to exercise control and autonomy over decisions about how my personal factual information is collected, used, and shared on Facebook.

(2) My control of personal factual information lies at the heart of my Facebook privacy.
(3) I believe that my factual information privacy is invaded when control is lost or unwillingly reduced.
(4) It bothers me if my friends on Facebook reveal my personal factual information I shared on Facebook to others.
(5) It is very important to me that I am aware and knowledgeable about how my factual information I shared will be used by my friends on Facebook.
(6) When my friends on Facebook want to use my factual information I shared on Facebook, they should let me know first.

Interactional Privacy Concern: Seven-point scales anchored with "strongly disagree" and "strongly agree". Adapted from Burgoon (1982) and Burgoon et al. (1989) and altered to fit the context of online social network.

(1) It bothers me when my friends on Facebook disrupt me from an ongoing online conversation.
(2) It bothers me when my friends on Facebook "poke" (send greeting message) me unexpectedly.
(3) It bothers me when my friends on Facebook start a conversation with me unexpectedly.
(4) It bothers me if I am interrupted by irrelevant messages or information from my friends on Facebook.

Psychological Privacy Concern: Seven-point scales anchored with "strongly disagree" and "strongly agree". Adapted from Burgoon (1982) and Burgoon et al. (1989) and altered to fit the context of online social network.

(1) It bothers me if my friends on Facebook publicly dislike the contents I post.
(2) It bothers me if my friends on Facebook joke about the content I post.
(3) It bothers me if my friends on Facebook judge my mood or feelings I shared in my space.
(4) It bothers me if my friends on Facebook judge me about my opinions.

Global Information Privacy Concern: Seven-point scales anchored with "strongly disagree" and "strongly agree". Adapted from Malhotra et al. (2004) and Smith et al. (1996) and altered to fit the context of online social network.

(1) All things considered, the Facebook would cause serious privacy problems.
(2) Compared to others, I am more sensitive about the way Facebook handles my personal information.
(3) To me, it is the most important thing to keep my privacy intact from Facebook.
(4) Compared with other subjects on my mind, my privacy on Facebook is very important.
(5) I am concerned about threats to my privacy on Facebook today.

Risk Beliefs: Seven-point scales anchored with "strongly disagree" and "strongly agree". Adapted from Jarvenpaa and Tractinsky (1999) and altered to fit the context of online social network.

(1) In general, it would be risky to share information on Facebook.
(2) There would be high potential for loss associated with the information I shared on Facebook.
(3) There would be too much uncertainty associated with sharing information on Facebook.
(4) Sharing information on Facebook would involve many unexpected problems.

Role Overload: Seven-point scales anchored with "strongly disagree" and "strongly agree". Adapted from Duxbury et al. (1992), Ho et al. (2003), and Peterson et al. (1995) and altered to fit the context of online social network.

(1) I think there is a need to reduce some roles I have taken on Facebook.
(2) I feel overburdened by different roles I have taken on Facebook.
(3) I have been given too much role expectation from other peers on Facebook.
(4) I have too many roles to play on Facebook.
(5) The amounts of roles I have to play interfere with the actual things I would like to do on Facebook.
(6) I feel I have too many roles to comfortably handle on Facebook.
(7) Different expectations from my friends on Facebook make me too tired or irritable to participate in or enjoy the activities on Facebook.

Role Conflict: Seven-point scales anchored with "strongly disagree" and "strongly agree". Adapted from Moore (2000), Rizzo et al. (1970), and Rutner et al. (2008) and altered to the context of online social network.

(1) I sometimes have to break a rule or norm to complete the thing I would like to do on Facebook.
(2) I frequently receive incompatible expectations from two or more parties on Facebook.
(3) I often engage in activities with two or more groups whose values or norms are quite different on Facebook.
(4) I often have to try to balance two or more conflicting activities on Facebook.

Misrepresentation of identification: Seven-point scales anchored with "very infrequently" and "very frequently". Adapted from Hoffman et al. (1999) and altered to the context of online social network.

Some Social Networking Websites ask you to register with the site by providing personal information. When asked for such information, do you falsify the information?

Invasion of privacy: Seven-point scales anchored with "very infrequently" and "very frequently". Adapted from Culnan (2000) and altered to the context of online social network.

How frequently have you personally been the victim of what you felt was an improper invasion of your privacy on social networking websites?

Media exposure of privacy victim: Seven-point scales anchored with "very infrequently" and "very frequently" (Smith et al. 1996).

How much have you heard or read, during the last year, about the use and potential misuse of personal information collected from the Internet?

Factor Loadings (Due to page limit, Table A1 and A2 are available upon request

References

Ackerman, M. 2004. "Privacy in Pervasive Environments: Next Generation Labeling Protocols," *Personal and Ubiquitous Computing* (8:6), September, pp. 430-439.

Agarwal, R., and Karahanna, E. 2000. "The Files When You're Having Fun: Cognitive Absorption and Beliefs about Information Technology Usage," *MIS Quarterly* (24:4), December, pp. 665-694.

Ashforth, B. E., Kreiner, G. E., and Fugate, M. 2000. "All in A Day's Work: Boundaries and Micro Role Transitions," *The Academy of Management Review* (25:3), July, pp. 472-491.

Baroudi, J. J. 1985. "The Impact of Role Variables on IS Personnel Work Attitudes and Intentions," *MIS Quarterly* (9:4), December, pp. 341–356.

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly*, (Forthcoming).

Belanger, F., Hiller, J. S., and Smith, W. J. 2002. "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes," *Journal of Strategic Information Systems* (11:3-4), December, pp. 245–270.

Bennett, C. J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, New York: Cornell University Press.

Bollen, K. A., and Jackman, R. W. 1990. "Regression Diagnostics: An Expository Treatment of Outliers and Influential Cases," in *Modern Methods of Data Analysis*, J. Fox and J. S. Long (eds.), Newbury Park, CA: Sage Publications, pp. 257-291.

Bostrom, R. P. 1981. "Role Conflict and Ambiguity: Critical Variables in the User-Designer Relationship," in *Proceedings of the Seventeenth Annual Computer Personnel Research Conference*, pp.88-112.

Burgoon, J. K. 1982. "Privacy and Communication," In *Communication Yearbook 6*, M. Burgoon (ed.), Beverly Hills, CA: Sage.

Burgoon, J. K., Parrott, R., LePoire, B. A., Kelley, D. L., Walther, J. B., and Perry, D. 1989. "Maintaining and Restoring Privacy through Communication in Different Types of Relationship," *Journal of Social and Personal Relationships* (6), May, pp. 131-158.

Burk, C. 1900. "The Collecting Instinct," *Pedagogical Seminary* (7), pp. 179-207.

Carpenter, P., Miyake, A., and Just, M. A. 1994. *Working Memory Constraints in Comprehension: Evidence from Individual Differences, Aphasia, and Aging*, San Diego, CA: Academic Press.

Chin, W. W. 1998. "The Partial Least Square Approach to Structural Equation Modeling," in *Modern Methods for Business Research*, G. A. Marcoulides (ed.), Mahwah, NJ: Lawrence Erlbaum, pp. 150-170.

Cohen, J. 1988. Statistical Power Analysis for the Behavioral Sciences, Hillsdale, NJ: Lawrence Erlbaum Associates, Publishers.

Culnan, M. J. 1995. "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing," *Journal of Direct Marketing* (9:2), Spring, pp.10–19.

Culnan, M. J. 2000. "Protecting Privacy Online: Is Self-regulation Working?" *Journal of Public Policy Marketing* (19:1), Spring, pp. 20–26.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., and Colautti, C. 2006. "Privacy Calculus Model in E-commerce - a Study of Italy and the United States," *European Journal of Information Systems* (15:4), pp. 389-402.

Dinev, T., and Hart, P. 2004. "Internet Privacy Concerns and Their Antecedents – Measurement Validity and a Regression Model," *Behavior and Information Technology* (23:6), pp.413-423.

Dowling, G. R., and Staelin, R. 1994. "A Model of Perceived Risk and Intended Risk-handling Activity," *Journal of Consumer Research* (21), June, pp. 119–134.

Dutta, A. and McCrohan, K., 2002. "Management's Role in Information Security in a Cyber Economy," *California Management Review*, (45:1), pp. 67-87.

Duxbury, L. E., Higgins, C. A., and Mill, S. 1992. "After-Hours Telecommuting and Work-Family Conflict: A Comparative Analysis," *Information Systems Research* (3:2), June, pp. 173-190.

Dwyer, C. 2007. "Digital Relationships in the 'MySpace' Generation: Results from a Qualitative Study," in *Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS)*, Hawaii, 2007.

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

Friday, P. C. 1980. "International Review of Youth Crime and Delinquency," in *Crime and Deviance: A Comparative Perspective*, G. R. Newman (ed.), CA: Sage.

Friday, P. C. 1983. "Patterns of Role Relationships and Crime," in *The Many Faces of Crime and Deviance*, S. G. Shoham (ed.), New York: Sheridan House.
Friday, P. C. and Hage, J. 1976. "Youth Crime in Postindustrial Societies: An Integrated Perspective," *Criminology* (14), November, pp. 347-68.
Gefen, D. and Straub, D. 2005. "A Practical Guide to Factorial Validity using PLS-Graph: Tutorial and Annotated Example," *Communications of the Association for Information Systems* (16:5), pp. 91-109.
Gefen, D., Straub, D., and Boudreau, M-C. 2000. "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Communications of the Association for Information Systems* (4:7), pp. 1-78.
Goldstein, D. K. and Rockart, J. F. 1984. "An Examination of Work-Related Correlates of Job Satisfaction in Programmer/Analysts," *MIS Quarterly* (8:2), June, pp. 103-115.
Goodhue, D., Lewis, W., and Thompson, R. 2007. "Statistical Power in Analyzing Interaction Effects: Questioning the Advantage of PLS with Product Indicators," *Information Systems Research* (18:2), pp. 211-227.
Gross, R., and Acquisti, A. 2005. "Information Revelation and Privacy in Online Social Networks," in *Proceedings of the 2005 ACM workshop on privacy in the electronic society*, Alexandria, VA, 2005.
Guimaraes, T. and Igbaria, M. 1992. "Determinants of Turnover Intentions: Comparing IC and IS Personnel," *Information Systems Research* (3:3), September, pp. 273-303.
Hall, D. T. 1971. "A Theoretical Model of Career Subidentity Development in Organizational Settings," *Organizational Behavior and Human Performance* (6:1), January, pp. 50-76.
Ho, V. T., Ang, S., and Straub, D. 2003. "When Subordinates Become IT Contractors: Persistent Managerial Expectations in IT Outsourcing," *Information Systems Research*, (14:1), March, pp. 66-86.
Hoadley, C. M., Xu, H., Lee, J. J., and Rosson, M. B. 2010. "Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry," *Electronic Commerce Research and Applications* (9:1), January-February, pp. 50-60.
Hoffman, D. L., Novak., T. P., and Peralta, M. A. 1999. "Building Consumer Trust Online," *Communications of the ACM* (42:4), April, pp. 80–85.
Ipeirotis, P. G. 2010. "Demographics of Mechanical Turk," *CeDER*, Working Papers.
Jarvenpaa, S. L., Tractinsky, N. 1999. "Consumer Trust in an Internet Store: A Cross-cultural Validation," *Journal of Computer-Mediated Communication* (5:2), December, (online).
Joinson, A. N., and Carina, B. P. 2007. "Self-disclosure, Privacy and the Internet," in The Oxford Handbook of Internet Psychology, A. N. Joinson, K. Y. A. McKenna, T. Postmes, and Ulf-Dietrich. Reips (eds.), New York: Oxford University Press, pp.235-250
Jones, M.G. 1991. "Privacy: A Significant Marketing Issue for the 1990s," *Journal of public Policy and Marketing* (10:1), Spring, pp. 133-148.
Kahn, R. L., Wolfe, D. M., Quinn, R. P., Snoek, J. D., and Rosenthal, R. A. 1964. *Organizational Stress: Studies in Role Conflict and Ambiguity*, Oxford: Wiley.
Kamis, A., Koufaris, M., and Stern, T. 2008. "Using an Attribute-Based Decision Support System for User-Customized Products Online: An Experimental Investigation," *MIS Quarterly* (32:1), March, pp. 159-177.
Knowles, E. D. 1980. "An Affiliative Conflict Theory of Personal and Group Spatial Behavior," In Psychology of Group Influence. P. B. Paulus (ed.), Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.
Lysonski, S. 1985. "A Boundary Theory Investigation of the Product Manager's Role," *Journal of Marketing* (49:1), Winter, pp. 26-40.
Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), December, pp. 336-355.
Margulis, S. T. 2003a. "On the Status and Contribution of Westin's and Altman's Theories of Privacy," *Journal of Social Issues* (59:2), pp. 411-429.
Margulis, S. T. 2003b. "Privacy as a Social Issue and Behavioral Concept," *Journal of Social Issues* (59:2), pp. 243-261.
Marshall, N. J. 1974. "Dimensions of Privacy Preferences," *Multivariate Behavior Research* (9:3), July, pp. 255–272.
Mayer, R. C., Davis, J. H., and Schoorman, F. D. 1995. "An Integrative Model of Organizational Trust," *Academic Management Review* (20:3), July, pp. 709–734.
McDougall, W. 1923. *An Introduction to Social Psychology*, 18th ed. London: Methuen.

Michaelsen, S., and Johnson, D. E. 1997. *Border Theory: The Limits of Cultural Politics*, Minneapolis: University of Minnesota Press.
Milne, G. R., and Rohm, A. J. 2000. "Consumer Privacy and Name Removal across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives," *Journal of Public Policy Marketing* (19:2), Fall, pp. 238–249.
Miyazaki, A., and Krishnamurthy, S. 2002. "Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions," *Journal of Consumer Affairs* (36:1), Summer, pp. 28-49.
Moore, J. E. 2000. "One Road to Turnover: An Examination of Work Exhaustion in Technology Professionals," *MIS Quarterly* (24:1), March, pp. 141-168.
Nippert-Eng, C. 1996. "Calendars and Keys: The Classification of 'Home' and 'Work'," *Sociological Forum* (11:3), pp. 563-582.
Nunnally, J. C. 1967. *Psychometric Theory*, New York: McGraw-Hill.
Pedersen, D. M. 1999. "Model for Types of Privacy by Privacy Functions," *Journal of Environmental Psychology* (19:4), December, pp. 397-405.
Perlman, H. H. 1968. *Persona: Social Role and Personality*, Chicago: University of Chicago Press.
Peterson, M. F., Smith, P. B., Akande, A., Ayestaran, S., Bochner, S., Callan, V., Cho, N. G., Jesuino, J. C., D'Amorim, M., Francois, P. H., Hofmann, K., Koopman, P. L., Leung, K., Lim, T. K., Martazavi, S., Munene, J., Radford, M., Ropo, A., Savage, G., Setiadi, B., Sinha, T. N., Sorenson, R., Viedge. C. 1995. "Role Conflict, Ambiguity, and Overload: A 21-nation Study," *Academy of Management Journal* (38:2), April, pp. 429-452.
Pew Internet Project. 2000. "Trust and Privacy Online: Why Americans Want to Rewrite the Rules," *Pew Internet & American Life Project*, http://www.pewinternet.org.
Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy Marketing* (19:1), Spring, pp. 27-41.
Porteous, J. D. 1976. "Home: The Territorial Core," *Geographical Review* (66:4), October, pp. 383-390.
Reinsch, N. L., Turner, J. W., and Tinsley, C. H. 2008. "Multicommunicating: A Practice Whose Time Has Come?" *Academy of Management Review* (33: 2), pp. 391–403.
Rizzo, J. R., House, R. J., and Lirtzman, S. I. 1970. "Role Conflict and Ambiguity in Complex Organizations," *Administrative Science Quarterly* (15:2), June, pp. 150-163.
Rutner, P. S., Hardgrave, B. C., and McKnight, D. H. 2008. "Emotional Dissonance and the Information Technology Professional," *MIS Quarterly* (32:3), September, pp. 635-652.
Sacks, H., Schegloff, E. A., and Jefferson, G. 1974. "A Simplest Systematics for the Organization of Turn-taking for Conversation," *Language* (50:4), December, pp. 696–735.
Sheehan, K. B., and Hoy, M. G. 2000. "Dimensions of Privacy Concern among Online Consumers," *Journal of Public Policy & Marketing* (19:1), Spring, pp. 62-73.
Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly*, (Forthcoming).
Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20:2), June, pp. 167–196.
Stewart, K. A., and Segars, A. H. (2002). "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research* (13:1), March, pp. 36-49.
Stone, E. F., and Stone, D. L. 1990. "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms," *Research in Personnel and Human Resources Management* (8:3), pp. 349-411.
Taylor, J. R., and Van Every, E. J. 2000. *The Emergent Organization: Communication as Its Site and Surface*, Mahwah, NJ: Lawrence Erlbaum Associates.
Van Slyke, C., Shim, J. T., Johnson, R., and Jiang, J. J. 2006. "Concern for Information Privacy and Online Consumer Purchasing," *Journal of the Association for Information Systems* (7:1), pp. 415-444.
Wang, P., and Petrison, L. A. 1993. "Direct Marketing Activities and Personal Privacy: A Consumer Survey," *Journal of Direct Marketing* (7:1), pp. 7–19.
Westin, A. F. 1967. *Privacy and Freedom*, Atheneum, New York.
Xu, H., Dinev, T., Smith, H. J., and Hart, P. 2008. "Examining the Formation of Individual's Information Privacy Concerns: Toward an Integrative View," in *Proceedings of 29th Annual International Conference on Information Systems (ICIS)*, Paris, France, 2008, paper 6.
Xu, H., Teo, H. H., and Tan, B. C. Y. 2005. "Predicting the Adoption of Location-Based Services: The Roles of Trust and Privacy Risk," in *Proceedings of 26th Annual International Conference on Information Systems (ICIS)*, Las Vegas, NV, 2005, pp. 897-910.

Yao, M. Z., Rice, E. R., and Wallis, K. 2007. "Predicting User Concerns about Online Privacy," *Journal of the American Society for Information Science and Technology* (58:5), March, pp. 710-722.
Zerubavel, E. 1991. *The Fine Line: Making Distinctions in Everyday Life*, New York: Free Press.