JOURNAL OF PSYCHOSOCIAL RESEARCH ON CYBERSPACE
CYBERPSYCHOLOGY

Jia, H., & Xu, H. (2016). Measuring individuals' concerns over collective privacy on social networking sites. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(1), article 1. doi: 10.5817/CP2016-1-4

Measuring individuals' concerns over collective privacy on social networking sites

Haiyan Jia, Heng Xu

College of Information Sciences and Technology, The Pennsylvania State University, U.S.

Abstract

With the rise of social networking sites (SNSs), individuals not only disclose personal information but also share private information concerning others online. While shared information is co-constructed by self and others, personal and collective privacy boundaries become blurred. Thus there is an increasing concern over information privacy beyond the individual perspective. However, limited research has empirically examined if individuals are concerned about privacy loss not only of their own but their social ties'; nor is there an established instrument for measuring the collective aspect of individuals' privacy concerns. In order to address this gap in existing literature, we propose a conceptual framework of individuals' collective privacy concerns in the context of SNSs. Drawing on the Communication Privacy Management (CPM) theory (Petronio, 2002), we suggest three dimensions of collective privacy concerns, namely, collective information access, control and diffusion. This is followed by the development and empirical validation of a preliminary scale of SNS collective privacy concerns (SNSCPC). Structural model analyses confirm the three-dimensional conceptualization of SNSCPC and reveal antecedents of SNS users' concerns over violations of the collective privacy boundaries. This paper serves as a starting point for theorizing privacy as a collective notion and for understanding online information disclosure as a result of social interaction and group influence.

Keywords: Privacy concern; collective privacy; social networking sites

Introduction

Social networking sites (SNSs) have been widely adopted and used with diverse purposes and in various scenarios in recent years. Despite the fact that some services such as Yammer and IBM Connections are oriented toward niche communication within a given organization or enterprise, most highly trafficked SNSs—Facebook, Twitter and Google Plus—allow millions of users to connect freely with vast networks of friends and strangers. Individuals create online profiles with personal information including names, gender, employment statuses, and social connections, all of which are often shared publicly. By sharing this information, individuals intend to meet new friends or find new opportunities.

Such oversharing of otherwise private information has raised privacy concerns among both users and privacy researchers. An increasing amount of effort has been put into evaluating the privacy settings of SNSs (e.g., Gross & Acquisti 2005), examining individuals' information disclosures and privacy protection behaviors (e.g., Young & Quan-Haase 2009), and highlighting potential privacy risks and harms (e.g., Debatin, Lovejoy, Horn, & Hughes,

2009). However, one key aspect of user privacy that is unique to SNSs has been long overlooked. Different from other online contexts such as e-commerce, individuals on SNSs not only disclose information of themselves, but also share information concerning others (e.g., daily schedules with co-workers, group photos with friends, interesting anecdotes of family members, etc.) inside and outside their social networks. Likewise, they also have to face potential privacy loss as a result of disclosures by their co-workers, friends, or family members.

Given that shared content is co-constructed by oneself and others, and that boundaries between different social circles are often blurred, SNSs bring unprecedented challenges for understanding and managing information privacy. On one hand, the shared information may concern more than one person (e.g., group photos with friends); on the other hand, the control over the access to and reuse of such shared information should be distributed among multiple stakeholders rather than within the original contributors. It seems that the notion of privacy through the individual lens is insufficient to capture the entire scope of privacy issues on SNSs. As a result, privacy scholars most recently have identified the incomprehensiveness of conceptualizing privacy at the individual level in the context of SNSs (e.g., Choi & Jiang, 2013; Hart, Johnson, & Stent, 2007; Xu, 2012). Instead, they have suggested considering the interpersonal and group perspectives of information privacy. However, a limited amount of research has empirically examined whether individuals are concerned about privacy loss, not only of their own, but also of their social ties';. Nor is there an established instrument for measuring individuals' privacy concerns beyond the personal level.

As a first step to address this gap in existing literature, we have conducted an empirical study to examine whether individuals are concerned about the privacy loss related to information in their social circles. We first provided a review of relevant privacy literature to introduce the construct of privacy concern and existing scales. Drawing on the Communication Privacy Management (CPM) theory (Petronio, 2002), we propose that individuals establish collectively held privacy boundaries through the sharing of information, and therefore form collective privacy concerns over three aspects of the shared information (i.e., collective information control, access, and diffusion). Subsequently, a preliminary scale for measuring individuals' collective privacy concerns in the context of SNSs has been developed and validated. Specifically, the scale aims at capturing users' concerns over violations of the collectively held privacy boundaries and expectations. We believe that the development of such a scale is an important first step for empirically identifying the social and collective considerations of privacy, and for measuring the different aspects of privacy concerns over collective boundaries on SNSs. We conclude this paper by discussing key findings, research implications, and future research directions.

Theoretical Background

Privacy Concerns and Existing Scales

Privacy concerns is considered as a central construct in empirical privacy research, a measurable proxy for the concept of privacy itself, and a predictor of privacy-protective behaviors (Smith, Dinev, & Xu, 2011). The privacy literature has documented various approaches for measuring privacy concerns, from categorizing individuals' different levels of innate privacy concerns, to measuring concerns over general information privacy (e.g., CFIP scale by Smith, Milberg, & Burke, 1996), to scales that measure the specific concerns over online privacy (e.g., IUIPC by Malhotra, Kim, & Agarwal, 2004), information abuse and unauthorized access (Dinev & Hart, 2004), or mobile privacy (e.g., Xu, Gupta, Rosson, & Carroll, 2012). These scales have operationalized privacy concerns as individuals' anxiety toward the collection, inaccuracy, secondary use, unauthorized access, control, and awareness of their private information.

Few of these operationalizations, however, capture the social/communication dimension of privacy, which Burgoon et al. (1989) proposed as one's ability and effort to control social relationships for privacy protection. The social aspect of privacy is especially important in understanding individuals' privacy perceptions and behaviors on SNSs, as social and communication needs underlie and drive SNS users' disclosure of private information (Ellison, Steinfield, & Lampe, 2011). General information privacy concerns alone can hardly predict individuals' information revelations and privacy management, whereas social factors (e.g., personal network size) become more prominent predictors of privacy behaviors (Young & Quan-Haase, 2009). Therefore, many privacy scholars (e.g., Dwyer, Hiltz, & Passerini, 2007; Strater & Lipford, 2008) have included new items that are more relevant to SNS activities, perceptions, or attitudes when applying existing scales to studies of SNS privacy

concerns. More importantly, privacy expectations vary significantly toward trusted social contacts versus the general public or third parties (Stutzman & Kramer-Duffield, 2010). Therefore, in the context of SNSs, the social aspect of privacy considerations plays a more significant role than other contexts; thus, conceptualizing SNS privacy through a collective lens is needed for better understanding how privacy perceptions are formed in online social interactions.

The Social Aspect of Privacy Concerns on SNSs

Conceptualizing privacy concerns beyond the personal perspective is especially important for understanding information disclosure on SNSs. In the context of SNSs, users' perceptions of groups, communities or collectives are one of the key factors that determine people's information disclosures. The sense of belonging to the online community or group is likely to enhance users' senses of trust in social networking sites, and individuals become more likely to disclose private information to other users of this "imagined community" (Fogel & Nehmad, 2009). They reveal personal information to trusted social contacts on SNSs for social support and for developing and maintaining social relationships (Ellison et al., 2007; 2011). Such an illusion of a closed online community encourages information disclosure on SNSs, even though, in reality, the disclosed information is often accessible to a wider public (Acquisti & Gross, 2006).

However, this is not to say that SNS users are not concerned that their private information may be accessed by unwanted audience. Their intended and expected audience usually comprises social categories and groups with whom they have established social relationships (e.g., family members, close friends, etc.). While they consider it socially beneficial to share and exchange private information with these social contacts, these users would experience expectancy violations when people or entities outside of the intended or expected audience, such as potential employers, marketers, corporations or strangers, attain access to private information they shared online (Stutzman & Kramer-Duffield, 2010).

More importantly, while posting and sharing information on SNSs, individuals are not only concerned about their personal privacy but also the privacy of their social connections and groups. The social aspects of privacy concerns, however, are rarely researched or discussed. Contrasting with the personal aspect of privacy, or the right to be left alone (Warren & Brandeis, 1890), Bloustein (1976) was one of the first to propose the notion of collective privacy, which suggests that individuals are also concerned about the right to "associate privately with one another" (p. 222). Such a definition indicates two integral components of collective privacy. One, collective privacy encompasses the privacy of the individual members of a collective. In the context of SNSs, because content shared on SNSs often contains information of multiple individuals, rather than just the original sharer, users of SNSs are concerned about the privacy of their friends being unexpectedly exposed or violated due to their disclosure behaviors. They are worried about revealing sensitive topics about friends, losing control over the information that their friends have shared with them, and leaking shared information to unintended others (Choi & Jiang, 2013; Xu, 2012). Two, in addition to the private information regarding each individual in their social groups, information of the entire group or collective—in terms of the existence of such a collective, the social associations that comprise the collective, and the interactions within the collective—is also part of this collective level of privacy. In other words, the social aspect of privacy is so much more than the private information of each individual; rather, it entails the characteristics of the collective itself—its members, its purposes, its cohesiveness, its structure, and dynamics. Hence, to whom the information is shared, and interactions and associations within that collective of data recipients, are also regarded as private. Moreover, individuals' privacy behaviors and decision-making are influenced by social and group norms. Utz and Krämer (2009) have found that SNS users tend to have more restrictive privacy settings if they perceive others, especially their friends and peers, as maintaining restrictive privacy settings. Such an influence of perceived norms is likely to enhance one's a person's awareness of the privacy preferences and expectations of their social connections and thus affect disclosure behaviors through collective privacy concerns.

In sum, individuals' privacy concerns are multi-faceted. They are not only concerned about the potential violation of the privacy of their own, but also the privacy of their friends and the collectives that they form together. The collective exceeds far beyond the personal scope of privacy concerns researched in current literature. In fact, Xu (2012) states that there is an urgent need "to address the acute concerns for collective information privacy in the context of SNSs" (p. 1078). In order to conceptualize the collective aspects of privacy concerns in a social context

such as SNSs, we introduce the conceptual framework of the collective privacy concerns, which is based on the Communication Privacy Management (CPM) theory (Petronio, 2002).

Communication Privacy Management (CPM) Theory

The Communication Privacy Management (CPM) theory (Petronio, 1991; 2002) is especially useful for understanding individuals' privacy concerns at various levels because this theory "not only gives the option of examining personal privacy boundaries around an individual's information but also allows for the notion of multiple privacy boundaries or collectively held private information (Petronio, 2010, p. 180)." After individuals share their private information online, the shared information moves to a collective domain where collectives (e.g., data subjects and data recipients) manage mutually held privacy boundaries. One of the main contributions of CPM is that the theory recognizes the co-existence of *personal* and *collectively* held privacy boundaries.

Previous research has adopted CPM in online communication contexts such as blogging (Child, Pearson, & Petronio, 2009) and family interaction (Child & Petronio, 2011). In both contexts, the presence of others (i.e., the public and family members as audiences) functions as a significant influence on individuals' self-consciousness (Child et al., 2009) and concern for appropriateness (Child & Agyeman-Budu, 2010), which would consequently affect their privacy rules and disclosure choices. Child et al. (2009) further demonstrate how individuals are concerned about violations of other people's privacy expectations and use the existence of other people as decision criteria when they consider different aspects of their privacy decision-making.

However, the existing literature that applies CPM to computer-mediated communication research addresses concerns only over *personal* privacy (e.g., "I would be upset if my friends shared what's written on my blog"; "I think my parents read my blog regularly"; etc.) in information-sharing scenarios. These studies tend to overlook individuals' concerns over the collectively held boundaries and the distributed responsibilities for keeping shared information private. Information disclosure on SNSs creates shared privacy boundaries among information subjects and recipients, each of whom experiences a sense of co-ownership and responsibility, which contributes to their concerns over the potential privacy loss of their friends' as much as their own, and their mutual desire to exert effort to control and regulate the flow of shared information. Therefore, it is crucial to go beyond the individual scope and examine privacy concerns at the collective level in order to fully capture what drives individuals' privacy decisions and behaviors on SNSs.

Individuals' Concerns over Collective Privacy on SNSs

CPM makes a compelling case for studying individuals' concerns over collective privacy, which calls for a boundary coordination process among both data subjects and data recipients through three boundary coordination rules: boundary ownership rules, boundary permeability rules, and boundary linkage rules (Petronio 2010). These coordination rules "illustrate the modes of change for the dialectic of privacy-disclosure as managed in a collective manner" (Petronio 2002, p. 127):

(1) *Boundary ownership* refers to the extent to which the original owner of private information (i.e., data subject) and co-owner (i.e., data recipient) are able to control further possession or solicitation of that information (Child et al. 2009; Petronio 2010).

(2) *Boundary permeability* refers to how much others are able to access the shared information within the co-owned privacy boundary (Petronio 2010).

(3) *Boundary linkage* denotes the associations through which shared information within the co-owned privacy boundary could be reshared and leaked (Petronio 2010).

In this paper, we discuss three dimensions of collective privacy concerns in the context of SNSs (or SNSCPC), corresponding to the three boundary coordination rules outlined in the CPM theory. Specifically, we argue that: First, information co-ownership will be practically defined in terms of the collective *control* over the shared content, which defines the collective boundary and who are capable of making decisions about the co-owned

information. Second, the permeability rules will be manifested in the *access* restrictions of the shared information, which determines the closeness and openness of the collective boundary structure. Third, *diffusion* of the shared information beyond the original boundaries and its regulation signals the violation of boundary linkage rules. Now, we discuss these three dimensions of SNSCPC.

Concerns over Collective Information Control

At the personal level, ownership rules capture the extent to which the original owner feels that he/she has right to own private information (Petronio, 2002) and control to make independent decisions about further disclosure (Child et al., 2009). In the SNS context, it often takes shape in the publishing and sharing of certain private content. As the original owner, individuals may assume they have absolute control over their private information and are able to independently regulate access or diffusion of their shared information (Child & Petronio, 2011).

However, such perceptions are challenged as soon as information is shared from the original owner to others and/or when the shared information concerns several other parties or stakeholders. On Facebook, for example, collective ownership takes the form of distributed control that designates who has the ability to regulate the information flow: The original owner no longer has sole control over the information; rather, those who have received the shared information (information recipients) and those whose private information is also revealed in the shared content (information stakeholders) are information co-owners and also able to make decisions about information access and diffusion (Fong, Anwar, & Zhao, 2009). Thus, ownership rules need to be negotiated among all information co-owners who have been granted access to the shared information. Overlooking the collectively shared control would lead to potential conflicts among co-owners and concerns over the inability to control their own social spheres (Houghton & Joinson, 2010). Moreover, concerns over collective information control would also arise if mechanisms and options for specifying co-ownership and explicit negotiation of ownership rules were lacking in SNS services (Squicciarini, Xu, & Zhang, 2010). Individuals would be concerned about unintentional violations of collectively held privacy expectations. Therefore, based on the ownership rules in the CPM theory, we posit that concerns about coordinating the collective information control and the potential privacy loss constitute an important dimension of SNSCPC.

Concerns over Collective Information Access

At the personal level, individuals often create boundary structures to reduce boundary permeability and the possibility of information leakage (Petronio, 2002). On social networking sites, individuals can modify privacy settings to adjust accessibility of their shared information in order to meet their social, contextual or personal needs (Petronio & Reierson, 2009). However, the actual privacy settings will not always be consistent with their privacy expectations. Therefore, individuals might be concerned with unwanted access to, or abuse of, their private information by strangers or unintended audiences (Hoadley, Xu, Lee, & Rosson, 2010).

At the collective level, violation of boundary permeability rules is more likely as current SNSs support only individual privacy decisions without offering effective mechanisms for collaborative privacy management among all information stakeholders or co-owners (Squicciarini et al., 2010). Therefore, one can set a privacy policy with a certain level of information accessibility that may conflict with the privacy preferences of other co-owners. Situations like this will give rise to concerns over the collective information access, as the executed privacy policy that supposedly regulates collective privacy boundaries reflects or prioritizes only the privacy preferences of the original owner or some (but not all) co-owners (Swathi, Radharani, & Babu, 2014). A third party may also obtain and use, without permission, the private information that concerns multiple stakeholders, resulting in potential privacy loss for the collective. Therefore, based on the permeability rules in the CPM theory, we propose concerns over regulating the collective information access comprise another key dimension of SNSCPC.

Concerns over Collective Information Diffusion

The linkage rules refer to "the establishment of mutually agreed-upon privacy rules used to choose others who may be privy to the collectively held information" (Jin, 2012, p.70). In the SNS context, the linkage rules involve the establishment of a linkage to become an information co-owner, or the selection of a member of one's social connections to be allowed into the collective privacy boundary (Child et al., 2009). When a linkage is established,

the new confidant is expected to assume shared responsibility for protecting the collectively held information boundary. Personal concerns over information diffusion often are triggered by secondary uses of personal information, either by unintended users or for unpermitted purposes (Smith et al., 1996; Xu et al., 2012). Individuals are also concerned with information being used out of context, and the consequences of such context collapse, which may include damage to their social relationships (Shi, Xu, & Chen, 2013).

More importantly, SNSs bring more opportunities to violate linkage rules at the collective level. As information sharing potentially increases the number of information co-owners and stakeholders, it also extends the degree to which information could flow through associations and social connections, with a richer range of possible relational ties and context crossovers (Hoadley et al., 2010; Kane, Alavi, Labianca, & Borgatti, 2012). Therefore, individuals now face the potentially wider diffusion of their private information through the social connections of all the co-owners. Their concerns over the collective information diffusion would thus involve not only the structural features of one's personal networks (i.e., the closeness of the networks), but also the extended reach of these social networks and even the overall online community (i.e. the density of networks). Consequently, we believe that concern over the collective information diffusion, stemming from the linkage rules in the CPM theory, is a complex factor that contributes to SNS users' collective privacy concerns.

Measuring Collective Privacy as an Individual's Concern

In the development of the SNSCPC scale, we adopt Bloustein's (1976) proposition that collective privacy is an extension of personal privacy, and considered collective privacy as "an attribute of individuals in association with one another within a group, rather than an attribute of the group itself" (p. 124). This conceptualization lends itself to the operationalization of collective privacy concerns in the form of individuals' concerns for the potential privacy loss experienced by the other members of a collective. Individuals' concerns for collective privacy can also be examined through control agency theory. While privacy is often defined as the perceived control over one's private information (Westin, 1967), when such information is shared through one's social connections, the agency of privacy protection transitions from the realm of personal control, with the self as the control agent to protect one's own privacy, to collective control, with a social group acting as the control agent to protect collective privacy (Xu, 2012). In other words, the sharing of private information within a collective privacy boundary is accompanied by the distribution of responsibilities for protecting collective privacy among the group members. The distributed responsibility and agency leads to individual members' concerns for the privacy of the collective, while the latter further determines collective-level processes such as coordinated privacy management. Hence, we propose to measure individual users' perceptions regarding concerns for collective privacy by asking about the extent to which they are concerned about the invasion of collective privacy boundaries and the violations of different aspects of collective privacy rules.

Instrument Development and Validation

Following the conceptual framework outlined above, we set out to develop and validate a preliminary instrument to measure individuals' collective privacy concerns in SNSs (SNSCPC). The process of our instrument development and validation followed the steps suggested by MacKenzie, Podsakff, and Podsakff (2011) in the general context of behavioral research and those outlined by Smith et al. (1996) in the specific context of privacy research.

The process includes three stages. Stage 1 involves specifying the conceptualization and dimensions of the construct, generation of sample items, and assessment of the validity of the items. Stage 2 involves an exploratory factor analysis of the instrument items. During this stage, an online survey (N = 427) with undergraduate student participants was conducted to gather empirical data. Stage 3 involves an assessment of the internal validity and the reliability of the instrument. Confirmatory factor analysis is conducted to compare the alternative models of the construct to confirm the dimensionality of the construct. The three stages are detailed as follows.

Stage 1

To specify the dimensions and to establish the instrument, an extensive literature review was conducted. Based on the literature review, the theoretical definition of the *SNSCPC* was proposed. As discussed earlier, *SNSCPC* refers to concerns about privacy rule violations (e.g., inappropriate information handling, access, and misuse) related to private information collectively owned by social networks. Drawing upon the CPM theory, three dimensions were identified as underlying privacy concerns over collective information: *control, access*, and *diffusion*. More specifically, collective privacy concerns encompass concerns over collective control over the shared information, unpermitted information access and diffusion beyond the collectively held boundaries by current stakeholders.

Table 1. *Collective Privacy Concerns on SNSs (SNSCPC).*

Factors	***Items***
Please think about you and your social ties—a group of your friends with whom you frequently interact on social networking sites (e.g., Facebook, Twitter, Pinterest, Instagram, etc.), and answer the following questions.	
Social Networking Sites (SNSs) such as Facebook provide users with various features to facilitate social connectivity and content sharing. Your shared information may not only reveal your own identity but also connect with your social ties (e.g., tagging a friend in a photo or place checked-in). Likewise, your personal information could be shared by your social ties on SNSs. Regarding the shared information you and your social ties co-manage, please indicate how strongly ***you and your social ties*** *may agree with the following statements:*	
Control	1. It usually bothers us when we do not have control over who can get access to our conversations on social networking sites. 2. It usually bothers us when we do not have control over which parts of our interactions are displayed on social networking sites. 3. It usually bothers us when we do not have control over decisions about how our information and interactions are collected, used, and shared by others. 4. We are concerned that our control over our information and interactions are reduced as a result of oversharing by others.
Access	1. We are concerned that as a result of using social networking sites, others may know more about us than we are comfortable with. 2. We are concerned that as a result of using social networking sites, information about us that we consider private is now more readily available to others than we would want. 3. We are concerned that as a result of using social networking sites, information about us is out there that, if used, would invade our privacy. 4. It bothers us that social networking sites shows everyone a history of our interaction from the past till now.
Diffusion	1. We are concerned that other people may see what we post on social networking sites when we do not intend to. 2. We are concerned that what we share within our group might be seen by others without our knowledge. 3. We are concerned that other people may use what we post on social networking sites for other purposes without notifying us or getting our permission. 4. We are concerned that other people may share what we post on social networking sites with people outside of our networks without getting our permission.

Scale items from existing empirical literature that measures privacy concerns and related concepts were sampled with privacy experts and scholars, and assessed for content validity, overlapping or irrelevant items as well as applicability to the respective dimensions before being used in the online survey study. The assessment resulted in a 12-item instrument, as shown in Table 1, with four items measuring each of the three dimensions of SNSCPC. To prime participants about the notion of "collective," they were asked to think about "a group of friends" with whom they frequently interact on SNSs while answering the questions.

Stage 2

To empirically assess the instrument through exploratory methods, an online survey was administered using a sample of 427 undergraduate student participants from a large northeastern university in the United States, aged 18 to 33 (M = 20.1, SD = 1.47), with 168 (39.3%) female respondents. With the empirical data from the student sample, an exploratory factor analysis was conducted and inter-item reliability (Cronbach's alphas) was assessed. The exploratory factor analysis with oblique rotation, using direct oblimin method in SPSS, showed all factor correlation coefficients equal to or greater than 0.69, providing initial evidence of factor correlation. It also yielded all factor loadings equal to or greater than .61 and the inter-item reliabilities (Cronbach's alpha) greater than .90. As shown in Table 2, the results indicated three dimensions of collective privacy concern, and that the items were sufficiently loaded to the three factors—collective information access, control, and diffusion—as hypothesized, each factor consisting of four items, with all loadings larger than 0.60. The three factors of the collective privacy concern scale also showed strong inter-item reliabilities, with Cronbach's alphas larger than .90.

Table 2. *Factor Analysis of SNSCPC with Direct Oblimin Rotation*.

Factors	***Items (M, SD)***	***Component***			***Cronbach's Alpha***
		1	***2***	***3***	
Collective Information Diffusion (CID)	CID1 (4.39, 1.55)	**.864**	0.046	0.004	0.958
	CID2 (4.36, 1.55)	**.770**	0.104	0.072	
	CID3 (4.31, 1.50)	**.922**	0.031	0.029	
	CID4 (4.31, 1.54)	**.994**	0.093	0.005	
Collective Information Access (CIA)	CIA1 (4.16, 1.51)	0.040	**.985**	0.110	0.947
	CIA2 (4.19, 1.49)	0.026	**.968**	0.003	
	CIA3 (4.28, 1.53)	0.003	**.856**	0.103	
	CIA4 (4.08, 1.53)	0.028	**.750**	0.112	
Collective Information Control (CIC)	CIC1 (4.56, 1.48)	0.009	0.102	**.854**	0.958
	CIC2 (4.56, 1.53)	0.010	0.022	**.958**	
	CIC3 (4.66, 1.48)	0.014	0.026	**.964**	
	CIC4 (4.31, 1.52)	0.321	0.119	**.610**	
Rotation Sum of Squared Loadings	Total	7.013	6.738	6.744	

Stage 3

Following the preliminary factor analysis, we further validated the scale in Stage 3 through assessments of the dimensionality, the construct validity, and the nomological validity of the instrument.

Dimensionality. To determine whether the proposed three-dimension construct provided the best fit to the data, the overall model fit statistics of three theoretical plausible models—a unidimensional model, a three-dimensional model, and a model with a second-order construct with three sub-factors—were compared using structural equation modeling program AMOS (Arbuckle, 2013):

1. The *unidimensional model* hypothesizes that all items of collective SNSCPC form into a single factor, which accounts for all the variance among the 12 items. Previous research (e.g., Dinev & Hart, 2004; Smith et al., 1996) has measured general privacy concern as a unidimensional construct. If this model is accepted, it indicates that it is appropriate to conceptualize SNSCPC as a single dimension rather than a three-dimension construct.

2. The *three-factor model* hypothesizes that the 12 items of SNSCPC form into three first-order factors: collective information control, access and diffusion. The assumption of this model is to conceptualize SNS users' collective privacy concerns over three aspects, and each aspect is an important, independent component in computing an overall score for SNSCPC.

3. The *second-order model* hypothesizes that the 12 items of SNSCPC form into three first-order factors, which are measured by a second-order factor SNSCPC. In this model, we consider the first-order factors (i.e., control, access, and diffusion) as inter-correlated. Each of the three factors and the second-order factor of SNSCPC itself are important in capturing the nature of the entirety of the construct. If this model is accepted, it indicates that SNSCPC is conceptualized as the three factors and the interrelationships among these factors.

Model fit statistics including CMIN/DF, CFI, and SRMR were calculated to assess the model fit. Comparison of the three models—the one-factor model, the three-factor model, and the second-order model—indicates that the proposed second-order model performs better on the overall model fit statistics than the alternative models. The second-order model of SNSCPC yielded better model fit statistics, confirming previous research that has conceptualized a CPM-based three-dimensional model of privacy concern in other contexts (e.g., Xu et al., 2012). As shown in Table 3, the chi-square statistics for all three models were significant, but the significant chi-squares likely resulted from the large sample size. Therefore, CFI and SRMR, which are independent of sample size, were used as indicators of the model fit. The CFI statistics of the second-order model was higher than the other two competing models. The SRMRs were also higher in the competing models than in the hypothesized model. Thus, the comparison shows that the proposed second-order model provided the best fit to the data of all three models compared.

Table 3. *Comparison of Three Models of SNSCPC*.

	One-Factor Model	**Three-Factor Model**	**Second-Order Model**
Chi-square*	1060.106	256.645	229.615
DF	51	51	51
CMIN/DF	20.786	5.032	4.502
CFI	0.822	0.955	0.961
SRMR	0.096	0.053	0.045

Note: *$p < 0.001$ for all models tested.

Construct Validity. To assess construct validity, we examined (1) the adequacy of the model fit of the confirmatory factor analysis (CFA) and (2) the convergent and discriminant validity of the second-order model. CFA results shown in Table 3 revealed satisfactory model fit statistics for the second-order model of SNSCPC (see Figure 1): *Chi-square* = 229.615, *DF* = 51, *CMIN/DF* = 4.50, $p < 0.001$; *CFI* = 0.96; *RMSEA* = 0.07; *SRMR* = 0.04. Following recommendations by Hu and Bentler (1999) and MacCallum, Browne, and Sugawara (1996), the results indicate an acceptable to good model fit (*CMIN/DF* < 5; *CFI* > 0.95; *RMSEA* < 0.08; *SRMR* < 0.08). CFA results were also used to assess convergent and discriminant validity of the scale. First, convergence implies that within-factor correlations are high and of approximately the same magnitude. The CFA test of the model showed that: (1) the fit of the internal structure of the model was sufficient (as discussed above); (2) standardized factor loadings for all items were greater than 0.60 (Table 2); and (3) the correlations between the three dimensions are all significantly different from zero ($p < 0.05$), indicating that the three factors all measured some aspect of the same construct (see Appendix A). To assess the discriminant validity, subscales of the construct were examined to ensure that they were not perfectly correlated (correlations equal to 1). Appendix A showed that the factor correlations range from 0.74 to 0.82, indicating that while the factors measure aspects of the same construct, they measure unique dimensions of that construct. Furthermore, a scale measuring personal privacy concerns

was administered to the study participants. A model comparison showed significant *chi-square* difference between the one-factor model, which hypothesizes one factor with six factors at both the personal and collective levels, and the two-factor model, which hypothesizes two factors capturing personal and collective privacy concerns, respectively (see Appendix B). Such results indicated statistical evidence of the distinction between individuals' responses to the two scales.

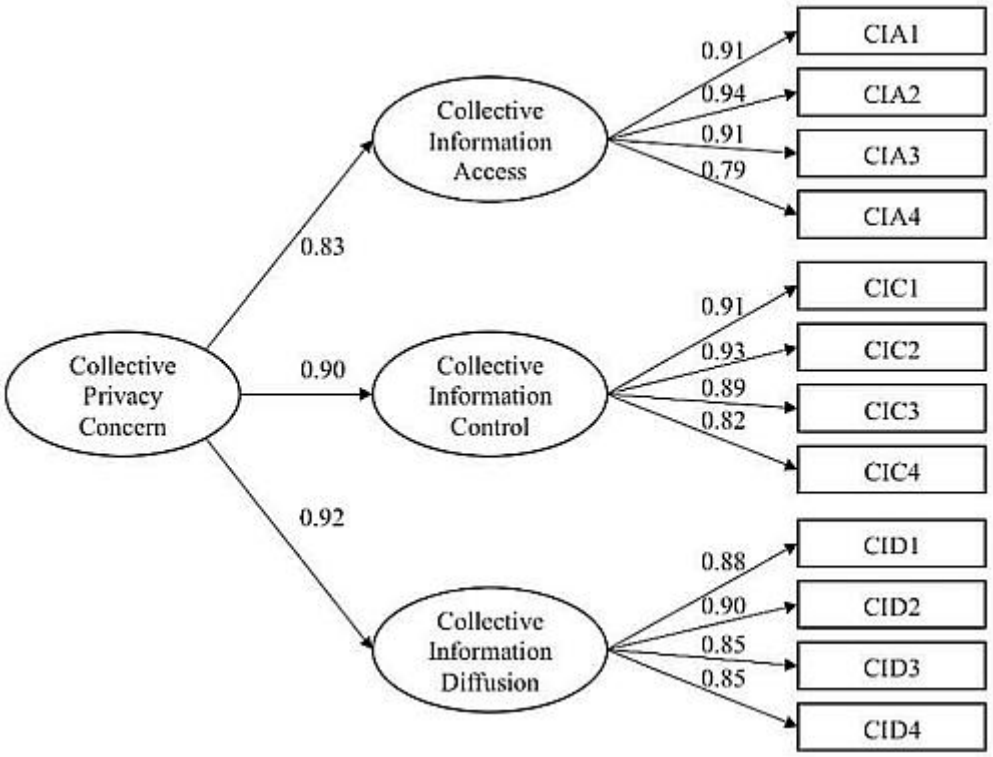

Figure 1. The second-order model of SNSCPC.

Nomological Validity. To examine the instrument's nomological validity, which refers to the extent to which predictions based on the construct are confirmed within a wider theoretical context or a structural model of constructs (Cronbach, 1971), we examined the relationships between some possible antecedents and the construct of collective SNS privacy concern. Specifically, two theoretically plausible causal variables, *perceived risk* and *propensity to value privacy*, were tested, as they were suggested in prior research as antecedents of privacy concerns (Smith et al., 2011; Xu, Dinev, Smith, & Hart, 2011). Existing scales measuring the two variables from the personal perspective were adapted to measure *perceived collective privacy risk* and the *collective's propensity to value privacy* (see Appendix C).

The structural model yielded sufficient model fit statistics results. Specifically, the structural equation modeling test showed: *Chi-square* = 365.26, *DF* = 128, *CMIN/DF* = 2.85, $p < 0.001$; *CFI* = 0.97; *RMSEA* = 0.06; *SRMR* = 0.04. Figure 2 shows that perceptions of the collective and the collective's propensity to value its privacy are both positively associated with the level of collective SNS privacy concerns. The findings strongly support research propositions regarding privacy concerns established in personal privacy research as applicable at the collective level.

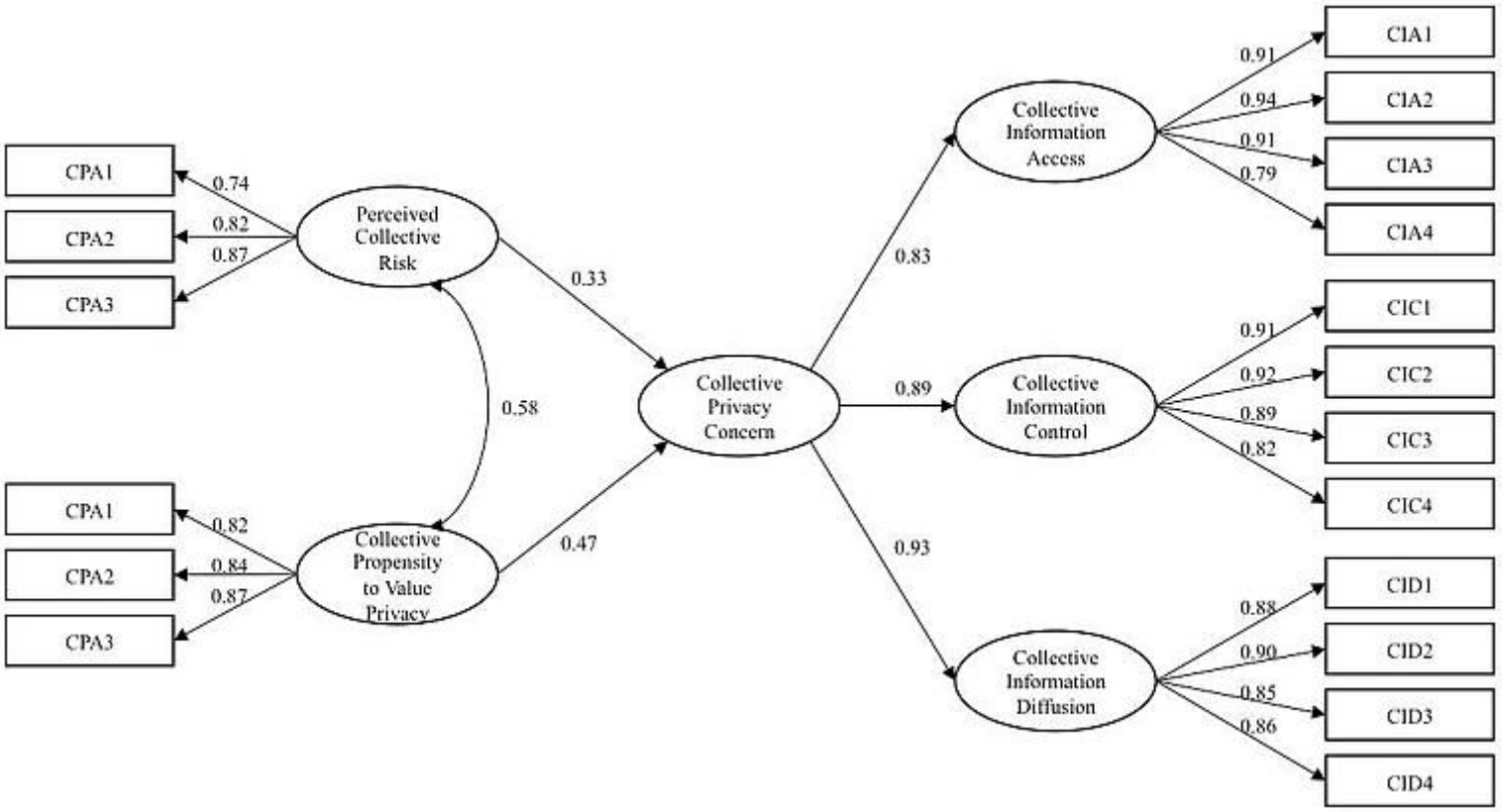

Figure 2. The second-order factor model of SNSCPC within its nomological network.

Discussion and Conclusion

This paper aims at empirically substantiating the notion of collective privacy concerns, and developing and validating an instrument to measure SNS users' concerns over collective privacy. Our study yielded both theoretical and practical implications for reconceptualizing the notion of privacy concerns.

Capturing the Collective and Social Aspects of Privacy Concern

The booming popularity of SNSs has brought an additional dimension to the complexity of privacy risks. According to Zittrain (2008), early threats to people's online information privacy came mostly from data stored in government or corporate databases, which he calls Privacy 1.0; yet, with the rise of SNSs, we have transitioned into an era of Privacy 2.0, where the data is generated and shared by individuals, and the "generativity" of SNSs breeds a new generation of privacy problems. Xu (2012) has further extended the notion of Privacy 2.0 to indicate that it is not simply user-generated data that have caused the possible privacy breaches; rather, the networked nature of such user data from users and their social ties, and the uncoordinated actions of individuals (both in terms of information sharing and information management), lead to the new privacy challenges. In the context of SNSs, keeping data safe and private has become a shared responsibility between users and social connections (Xu, 2012). That means, even if some user adopts tight privacy settings or is cautious about his or her own information disclosure, private information could still be leaked or misused because of friends' ignorance of privacy and security. The ubiquity of SNSs has increased the scope of privacy threats, emerging as a result of dysfunctional coordination and fostering the awareness of collective privacy risks among SNS users. Until now, few studies have made systematic attempts to specify privacy concerns from such a collective perspective. This study serves as an attempt to fill this gap in the privacy research by examining SNS users' collective privacy concerns and furthering privacy research beyond the scope of privacy as an individualistic concept.

Drawing on the CPM theory (Petronio, 2002) and an extensive review of the empirical studies of SNS-related privacy concerns, we constructed an instrument and empirically tested the three-dimensional measurement of SNSCPC scale. Exploratory and confirmatory factor analyses have revealed three factors—*collective information control, access*, and *diffusion*—as key dimensions of SNSCPC. Further analysis confirmed the three-dimensional conceptualization of SNSCPC. The superiority of the model fit statistics of the second-order SNSCPC scale imply that SNS users are concerned with all three aspects of their privacy, and the three dimensions are interdependent in the construction and measurement of individuals' collective privacy concerns. Finally, the scale of SNSCPC shows robust results in structural equation models with perceived risk and privacy values as antecedents, confirming prior findings in privacy research and indicating applicability of the propositions at the collective level as well.

Differentiating the Individualistic and the Social Aspects of Privacy Concern

Despite the proliferation of research with an individualistic approach to examining privacy concerns, conceptualization and measurement of individuals' concerns over socially constructed, collectively managed private information is lacking. More fundamentally, little empirical evidence exists to show that the two differ and co-reside in individuals' privacy perceptions. Our study has provided preliminary proof that individuals hold privacy concerns at these different levels. More specifically, the test of the discriminant validity of SNSCPC confirmed that SNS users' personal privacy concerns and collective privacy concerns are related, but distinct, constructs. The two constructs encompass conceptually corresponding factors that operate at individual and collective levels. Furthermore, the nomological validity test results showing significant relationships between collective-level antecedents and collective privacy concerns indicated that individuals' collective privacy concerns were strongly influenced by social and group factors such as the collective's susceptibility to privacy risk and collective privacy norms. Such findings confirmed the theoretical proposition that users perceive the construction and the management of collective privacy as collaborative processes, and their concern over potential threats to the collective privacy is influenced by the collective norm, preference, and power to regulate the collective privacy boundary.

Application of the SNSCPC Scale

The SNSCPC scale, with its three dimensions, is deeply rooted in the highly social environment of online social networks. Privacy researchers and website designers will be able to utilize the SNSCPC scales to capture a user's privacy concerns in such contexts and to examine how different aspects of privacy concerns affect user adoption and user experience of the sites. For our data collection, we asked our participants to report their frequency of using a variety of social networking sites and services, and found that several sites were among the frequently used. For instance, when rating the fifteen listed social networking sites and services, 59.4% of the participants self-reported as frequent users (who chose response options from "frequently" to "all the time") of Facebook, 52.7% as frequent users of Instagram, and 50.1% as frequent users of Twitter. Given our goal to capture the collective privacy concerns that are most salient to the participants, they were asked to think about their most frequently used SNS service and the social group with which they most frequently interacted while answering the survey questions. Thus, it is reasonable to expect that findings from this study reflect collective privacy concerns throughout a variety of online social networks and services. Still, the SNSCPC scale may not be readily applicable to all social networking sites or applications, and adaptions may be needed, especially with emerging services and contexts.

Before SNSs became widespread, information privacy usually focused on one Internet user at a time; if the user is worried about being identified or personal information being misused, they may be able to easily hide their online identity or remove personal information. However, when private information is co-created and disseminated throughout a network of users, personal and absolute control over private information is no longer a reality. Consequences of privacy breaches and data misuse are no longer affecting a single user, but could potentially reveal critical information concerning multiple associated users or a wider group. Therefore, we argue that concerns for information privacy in a SNS context are not only different, but also collective in nature. Compared to online consumer and ordinary Internet users, SNS users are more prone to privacy threats and intrusion at higher levels beyond their personal data management.

While more websites and Internet applications, from consumer websites to news portals, are integrating social features into their site designs and structures, SNSCPC may make an important contribution to the field of Privacy by Design. The findings from this study could yield practical implications for developing privacy-enhancing mechanisms and policies to mitigate different aspects of user concerns, especially in the collective sphere. Today's highly networked cyberspace calls for our attention in investigating and better understanding how social and group dynamics affect individuals' privacy behaviors and decision-making. Our paper is one of the first to provide empirical evidence on the notion of collective privacy. Future research can extend this work and further examine how individuals' concerns over collective privacy may differentiate in their effects from personal privacy concerns on shaping individuals' privacy management strategies and online activities such as information disclosures and socialization.

Limitation and Future Work

In generalizing the results of this study, we caution readers to note that the social norms and group characteristics vary in different social networking sites, applications, and services. As privacy notions are highly contextualized (Nissenbaum, 2004), we call for future research to further confirm the validity of SNSCPC in other emerging online social contexts. Privacy strategies and behaviors may also vary significantly as users transition from one site or application to another; therefore, the scale may be updated or expanded in accordance to such variation. At the same time, as the online environment becomes more and more social in general, e.g., e-commerce websites are integrating online social networking as part of their branding, advertising, and consumer engagement strategies, the SNSCPC scale may be applicable not only with use of SNSs and applications, but also in contexts where private information is co-constructed, co-owned, and co-managed. The scale's applicability and predictability need testing when utilized in these scenarios for understanding individuals' privacy concerns and consequent online behaviors from disclosure to purchase intentions. Second, future studies should test the scale with demographically diverse samples, as factors such as gender and age are likely to influence privacy perceptions (Fogel & Nehman, 2009; Walrave, Vanwesenbeeck, & Heirman, 2012). Researchers should also consider group factors and individual idiosyncrasies, e.g., cultural differences, technological competence, and generational differences, etc. Third, the nomological validity of the scale can be further examined in a network of other plausible antecedents and outcomes. Future research is needed to examine the associations between SNSCPC and constructs that are prominent in group dynamics, such as group cohesion, group norms, and social identity that may influence individuals' privacy decision-making in group structures. Other forms of empirical study designs such as experimental studies can utilize the instrument to measure actual user responses to various collective privacy threats in different social contexts and scenarios. Researchers can further investigate how personal and collective privacy concerns may differ and converge under various social and technological influences, producing different psychological and behavioral responses.

While this research constitutes a step toward a better understanding of individuals' collective privacy concerns in SNSs, it raises many questions that need to be addressed in future research. As social networking increasingly becomes an integral component of more and more types of websites and online services, and as private information is gathered and computed more frequently on a collective rather than individual basis through emerging technologies such as Internet of Things and Big Data tools, collective privacy as an emerging concept may be researched from different angles and in different environments, such as e-commerce, collaborative learning, distributed work, etc. Researchers from different fields may propose new theoretical approaches than the CPM theory to study individuals' concerns and management of their collective privacy. We hope that the ideas and preliminary results put forth in this paper will motivate privacy researchers to move beyond the individual notion of privacy. Further, we hope this paper may serve as a starting point for empirical privacy research to adopt a multi-level approach in conceptualizing privacy and its implications in the process of social interactions, which remains a relatively unexplored area in our field.

Acknowledgements

This research was supported by the U.S. National Science Foundation under grant CNS- 0953749. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Privacy Enhancing Technologies*, 36-58. Springer Berlin Heidelberg.

Arbuckle, J. L. (2013). *IBM® SPSS® Amos™ 22 User's Guide*. Chicago, IL: IBM.

Bloustein, E.J. (1976). Group privacy: The right to huddle. *Rutgers Law Journal, 8*, 219-283.

Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationships. *Journal of Social and Personal Relationships, 6*, 131-158. http://dx.doi.org/10.1177/026540758900600201

Child, J. T., & Agyeman-Budu, E. A. (2010). Blogging privacy management rule development: The impact of self-monitoring skills, concern for appropriateness, and blogging frequency. *Computers in Human Behavior, 26*, 957-963. http://dx.doi.org/10.1016/j.chb.2010.02.009

Child, J. T., Pearson, J. C., & Petronio, S. (2009). Blogging, communication, and privacy management: Development of the blogging privacy management measure. *Journal of the American Society for Information Science and Technology, 60*, 2079-2094. http://dx.doi.org/10.1002/asi.21122

Child, J. T., & Petronio, S. (2011). Unpacking the paradoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the Internet. In K. B. Wright & L. M. Webb (Eds.), *Computer-mediated communication in personal relationships* (pp. 21-40). Peter Lang.

Choi, C. F., & Jiang, Z. (2013). Trading friendship for value: An investigation of collective privacy concerns in social application usage. In *Proceedings of Thirty Fourth International Conference on Information Systems (ICIS 2013)* (pp. 1-10). Milano, Italy.

Cronbach, L. J. (1971). Test validation. In R. L. Thomdike (Ed.), *Educational measurement* (pp. 443-507). Washington DC: American Council on Education.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*, 83-108. http://dx.doi.org/10.1111/j.1083-6101.2009.01494.x

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents – measurement validity and a regression model. *Behaviour & Information Technology, 23*, 413-422. http://dx.doi.org/10.1080/01449290410001715723

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. In *Proceedings of Americas Conference on Information Systems (AMCIS 2007)* (pp. 339-350). Keystone, CO.

Ellison, N. B., Steinfield, C., & Lampe, C. 2011. Connection strategies: Social capital implications of Facebook-enabled communication practices. *New Media & Society, 13*, 873-892. http://dx.doi.org/10.1177/1461444810385389

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12*, 1143-1168. http://dx.doi.org/10.1111/j.1083-6101.2007.00367.x

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*, 153-160. http://dx.doi.org/10.1016/j.chb.2008.08.006

Fong, P.W., Anwar, M., & Zhao, Z. (2009). A privacy preservation model for Facebook-style social network systems. *Computer Security–ESORICS 2009*, 303-320. Springer Berlin Heidelberg.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (pp. 71-80).

Hart, M., Johnson, R., & Stent, A. (2007). More content-less control: Access control in the Web 2.0. *IEEE Web* (2).

Hoadley, M. C., Xu, H., Lee, J., & 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*, 50-60. http://dx.doi.org/10.1016/j.elerap.2009.05.001

Houghton, D.J., & Joinson, A. N. (2010). Privacy, social network sites, and social relations. *Journal of Technology in Human Services, 28*, 74-94. http://dx.doi.org/10.1080/15228831003770775

Hu, L.T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal, 6*(1), 1-55.

Jin, S. A. A. (2012). "To disclose or not to disclose, that is the question": A structural equation modeling approach to communication privacy management in e-health. *Computers in Human Behavior, 28*, 69-77. http://dx.doi.org/10.1016/j.chb.2011.08.012

Kane, G. C., Alavi, M., Labianca, G. J., & Borgatti, S. (2012). What's different about social media networks? A framework and research agenda. *MIS Quarterly, 38*, 274-304.

MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. *Psychological Methods, 1*, 130-149. http://dx.doi.org/10.1037/1082-989X.1.2.130

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in mis and behavioral research: Integrating new and existing techniques. *MIS Quarterly, 35*, 293-334.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Information Systems Research, 15*, 336-355. http://dx.doi.org/10.1287/isre.1040.0032

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119

Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory, 1*, 311-335. http://dx.doi.org/10.1111/j.1468-2885.1991.tb00023.x

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

Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation? *Journal of Family Theory & Review, 2*, 175-196. http://dx.doi.org/10.1111/j.1756-2589.2010.00052.x

Petronio, S., & Reierson, J. (2009). Regulating the privacy of confidentiality: Grasping the complexities through communication privacy management theory. In T. Afifi & W. Afifi (Eds.), *Uncertainty, information management, and disclosure decisions: Theories and applications* (pp. 365-383). Routledge.

Shi, P., Xu, H., & Chen, Y. (2013). Using contextual integrity to examine interpersonal information boundary on social network sites. In *Proceedings of the ACM Conference on Human Factors in Computing Systems* (CHI'13) (pp. 35-38). Paris, France.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*, 989-1015.

Smith, H. J., Milberg, J. S., & Burke, J. S. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*, 167-196. http://dx.doi.org/10.2307/249477

Squicciarini, C. A., Xu, H., & Zhang, X. (2011). CoPE: Enabling collaborative privacy management in online social networks. *Journal of the American Society for Information Science and Technology, 62*, 521-534.

Strater, K., & Lipford, H. R. (2008). Strategies and struggles with privacy in an online social networking community. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction* (pp. 111-119). British Computer Society.

Stutzman, F., & Kramer-Duffield, J. (2010). Friends only: Examining a privacy-enhancing behavior in Facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'10)* (pp. 1553-1562). ACM.

Swathi, G., Radharani, A., & Babu, K. M. (2014). Self-controlled privacy policy for online social networks using multi-party access control. *The International Journal of Computer Science Information and Engineering Technology, 4*(3).

Utz, S., & Krämer, N. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms*. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 3*(2), article 1.

Walrave, M., Vanwesenbeeck, I., & Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 6*(1), article 9.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193-220.

Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.

Xu, H. (2012). Reframing privacy 2.0 in online social network. *University of Pennsylvania Journal of Constitutional Law, 14*, 1077-1102.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*, 798-824.

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. In *Proceedings of 29th Annual International Conference on Information Systems (ICIS 2012)*, Orlando, FL.

Young, A. L., & Quan-Haase, A. (2009). Information revelation and internet privacy concerns on social network sites: A case study of Facebook. In *Proceedings of the Fourth International Conference on Communities and Technologies* (pp. 265-274). ACM.

Zittrain, J. (2008). Privacy 2.0. In *The University of Chicago Legal Forum, 2008*, 65-120.

Correspondence to:
Dr. Heng Xu
College of Information Sciences and Technology
The Pennsylvania State University
316H IST Building
University Park, PA 16802

E-mail: hxu(at)ist.psu.edu

Appendices

Appendix A. Factor Intercorrelation

Factors	CIA	CIC	CID
Collective Information Access (CIA)	1.00		
Collective Information Control (CIC)	0.74	1.00	
Collective Information Diffusion (CID)	0.76	0.82	1.00

***Note**:* All factor intercorrelations are significantly different from zero ($p < 0.05$) and one ($p < 0.05$).

Appendix B. Model Comparison: Personal and Collective Privacy Concerns

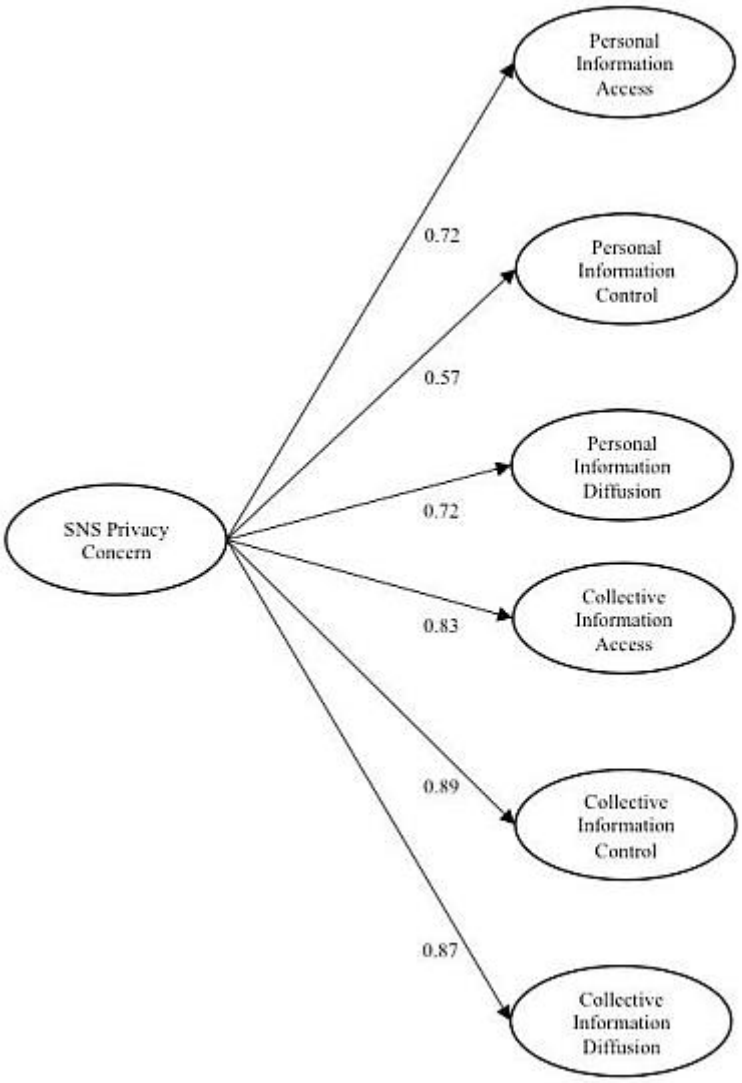

Figure B1. One-factor model. Model Fit Statistics: Chi-square = 925.60, DF = 244, CMIN/DF = 3.79, p < 0.001; CFI = 0.93; RMSEA = 0.08; SRMR = 0.09.

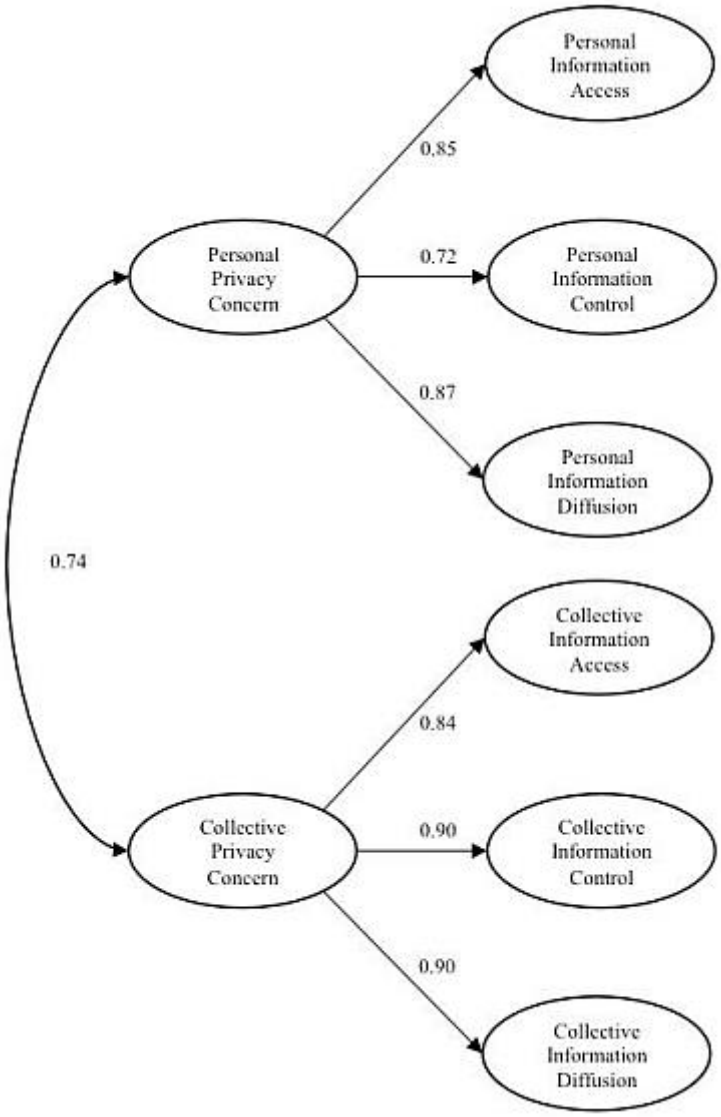

Figure B2. Two-factor model. Model Fit Statistics: Chi-square = 760.49, DF = 243, CMIN/DF = 3.13, $p < 0.001$; CFI = 0.95; RMSEA = 0.07; SRMR = 0.05.

Appendix C. Measurement of Perceived Risk and Propensity to Value Privacy

Factor	Collective-Level Measurement
Perceived Risk *(Adapted from the RISK scale in Xu et al., 2011)*	1. In general, it is risky for my friends and me to share our information and interaction on social networking sites. 2. It is likely that others will use what we post online inappropriately. 3. Sharing information and interactions on social networking sites will lead to many unexpected problems for my friends and me. Cronbach's Alpha = 0.85
Propensity to Value Privacy *(Adapted from the DTVP scale in Xu et al. 2011)*	1. As a group, we are very sensitive about the way social networking sites handle our information and interaction. 2. To my friends and me, it is the most important thing to keep our information privacy. 3. As a group, we tend to be very concerned about threats to our information privacy. Cronbach's Alpha = 0.88

About authors

Dr. **Haiyan Jia** is a post-doctoral scholar at the Pennsylvania State University in the College of Information Sciences and Technology. Her research interest primarily focuses on the social and psychological effects of communication technology ranging from Web to mobile apps to smart objects. Her current work investigates online privacy in social and collective contexts.

Dr. **Heng Xu** is an associate professor of Information Sciences and Technology at the Pennsylvania State University. Her research focus is on the interplay between social and technological issues associated with information privacy. She approaches privacy issues through a combination of empirical, theoretical, and technical research efforts. Her research projects have been dealing with individuals' information privacy concerns and behaviors, strategic management of organizational privacy and security practices, and design and empirical evaluations of privacy-enhancing technologies.