Networked Privacy Management in Facebook: A Mixed-Methods and Multinational Study

Hichang Cho
Communications and New Media
National University of Singapore
Singapore
cnmch@nus.edu.sg

Anna Filippova
Communications and New Media
National University of Singapore
Singapore
annaf@u.nus.edu

ABSTRACT
Users of social network services (SNSs) have to cope with a new set of privacy challenges because personal information on an SNS is often co-owned and co-managed by various distributed social ties. Using a multi-methods and multinational approach, we investigated Facebook users' privacy behavior by focusing on how they co-manage private information. Our findings from focus-group interviews (n = 28) and online surveys (n = 299) suggest that Facebook users primarily apply four different practices of privacy management: collaborative strategies, corrective strategies, preventive strategies, and information control. The four dimensions of privacy management display selective relationships with theoretical antecedents (e.g., self-efficacy, collective-efficacy, attitudes, privacy concern), indicating that each behavior is motivated by a different combination of conditions. Implications for research and practice are discussed.

Author Keywords
Privacy; Social network service; Networked privacy management; Collaborative privacy practice; Social computing

ACM Classification Keywords
H.5.3. Group and Organization Interfaces: Collaborative computing, Computer-support cooperative work

INTRODUCTION
Traditionally, the concept of privacy has been defined as personal control or autonomy with which individuals "determine when, how, and to what extent information about them is communicated to others" [39:7]. Likewise, most research on privacy has focused on how the level of privacy control is determined by individual-level variables or personal processes. These include self-efficacy beliefs [30], privacy concerns [9], personality traits [19], privacy calculus [35], and heuristics [6]. However, researchers have claimed that privacy is an inherently social issue [1, 22] that should be characterized as a group property managed through a dynamic and recursive process whereby individuals, groups, and organizations constantly negotiate interpersonal and information boundaries [35]. In this broader conceptualization, privacy-related decision making and behavior are not only influenced by an individual's predispositions, perceptions, and beliefs, but also by interpersonal and group-level factors and dynamics [26]. Consequently, there has been a call for researchers to revisit privacy issues and impacts by looking beyond individual-level factors towards interpersonal and group settings in which multiple stakeholders co-own and co-manage the privacy of information [31, 38].

This call is particularly relevant in the context of social network services (or SNSs). SNS users must cope with a new set of privacy challenges because personal data is not only easily permeable but also often co-owned and co-managed by various distributed social ties. Hence, it is suggested that privacy management strategies in a social media environment differ from those in traditional settings *"because of [a]change of agency (from the self to a group), [the] inclusion of interpersonal privacy decision making, and […] co-management of shared information"* [43:1093].

However, there has been little empirical and theoretical work examining the collaborative and collective aspects of privacy management in SNSs [38, 43]. This study seeks to contribute to privacy research in at least two important ways. First, we suggest a new conceptualization and operationalization of networked privacy management in SNSs. Specifically, we focus on a set of interpersonal actions and decisions that individuals make to maintain the privacy of the shared information on SNSs. Though past research has uncovered several types of collaborative privacy management strategies, most findings are based on qualitative and explorative studies using small samples [18, 41], or focused primarily on technological mechanisms [35, 40]. By conducting a multi-methods and multi-country study involving a more varied population, this study supplements and advances previous research on networked privacy.

Second, we specify the relationships between networked privacy management and key privacy-related beliefs and behavior in a research model. Whereas previous studies focused on identifying behavioral patterns or dimensions of

CSCW '16, February 27-March 02, 2016, San Francisco, CA, USA
 ISBN 978-1-4503-3592-8/16/02…$15.00
DOI: http://dx.doi.org/10.1145/2818048.2819996

networked privacy management [18, 40, 41], we take a step further to examine how these novel types of behavioral strategies are linked to other theoretical constructs central to privacy such as privacy self-efficacy beliefs, collective-efficacy beliefs, and privacy concerns. This will allow us to identify (a) under what conditions people apply different types of strategies; and (b) possible reasons why people do or do not enact collaborative privacy management strategies.

To do this we conducted a mixed-methods, multinational study. Using focus-group interviews (n = 28), we discovered key behavioral strategies related to collaborative privacy management. We then administered two online surveys in the U.S. (n = 146) and Singapore (n =153) to (a) explore the underlying dimensionality of networked privacy management; (b) describe the extent to which SNS users engage in different coping strategies; and (c) specify the ways in which this relatively unexplored privacy behavior (i.e., networked privacy management) is linked to theoretical constructs of privacy.

RELATED WORK

Theoretical and Conceptual Work on Collective Privacy Management

While personal process is central to many analyses of privacy, researchers have also argued that privacy goes beyond what is under individual control [26]. Altman [1:10] defines privacy as "an interpersonal boundary-control process, which paces and regulates interaction with others." Whereas traditional approaches understand privacy as a state of social withdrawal (e.g., "right to be left alone") [39], Altman instead sees it as a dialectic and dynamic process that involves both approach and avoidance of social contact—both the opening and the closing of the self to others. This dialectic boundary control is inherently governed by social and communication processes to the extent that privacy is under continuous negotiation and management between parties. As such, a proper understanding of privacy must include the interplay of people, their social world, and the physical environment [2]. An analysis of privacy should be applied not only at the individual but also at group levels in order to reveal how people regulate social interactions through a process of interpersonal boundary regulation.

Petronio's [27, 28] theory of communication privacy management (CPM) is built on Altman's dialectic conception of privacy. A central argument of CPM theory is that privacy rules and norms are developed through interpersonal boundary management and collaborative negotiations. This is particularly important in a networked environment, such as SNSs—once individuals disclose their personal information, it moves to a shared domain where collectives (i.e., data subjects and data recipients) manage mutually-held privacy boundaries [27]. For instance, Facebook users often share content that may interact with others' identities, such as tagging an image or linking to a friends' personal profile. This, in turn, entails joint responsibility for co-owners of the shared information to keep the information safe and private. Hence, users must negotiate a number of rules determining the opening and closing of the interpersonal privacy boundary and commit to mutually holding or coordinating these rules [41].

CPM theory extends Altman's original proposal of privacy regulation by specifying how decisions and rules of boundary regulation are made through three main processes: rule development, boundary coordination, and boundary turbulence. *Rule development* determines to whom it is appropriate to tell what pieces of information. Privacy rule choices are derived from decision criteria such as motivators, risk-benefit ratio, situational needs, gender, privacy orientations, and cultural values [28]. *Boundary coordination* refers to the process of developing and applying privacy ownership and permeability rules. For instance, some information may be expected to be permeable (and potentially shared and re-shared within the social medium; e.g., retweets), while other content is strictly non-permeable. Thirdly, *boundary turbulence* occurs when co-owners of information fail to negotiate or maintain interpersonal boundaries to manage personal disclosures. When it occurs, people seek to resolve these problems and restore coordination. SNS users often experience a form of boundary turbulence. For instance, Facebook friend requests from parents [5, 16] or co-workers [10] can cause a possible privacy dilemma because accepting such requests leads to context collapse [34]. This may prompt users to reassess and recalibrate the adequate functioning of the current privacy management rules. Overall, CPM argues that people depend on a rule-driven boundary system to manage privacy. The result is collective control of the flow of private information among multiple members [22].

The notion of contextual integrity [24] also addresses interpersonal- and group-level privacy management. A central tenet of this framework is that context-relative information norms regulate the flow of certain types of information from an actor to others according to particular transmission principles. In other words, privacy is a collective-level property to the extent that norms of appropriateness and norms of distribution are collectively shared, understood, and practiced by multiple actors situated in a specific context.

Overall, the aforementioned theoretical perspectives have extended narrower theories of privacy that emphasize personal control by incorporating social and communicative processes involved in privacy management. However, these theories are stated in general terms, and as with many theories, there is a need to explicate theoretical terms and concepts in order to advance research on privacy as a collective property [18].

Previous Research on Networked Privacy Management

Despite the need for studying privacy in group and collaborative settings, limited CSCW studies to date have examined empirically group-level collaborative privacy practices [4, 23]. Recently, a growing number of studies have examined collaborative aspects of privacy management in the context of SNSs since social media provides ample opportunities to study collaborative privacy management [38, 42]. In general, previous research has focused primarily on two areas: (a) designing technological mechanisms to support interpersonal/collaborative privacy practices [3, 13, 32, 33]; and (b) identifying various behavioral strategies that SNS users enact for the co-management of networked privacy [40, 41].

Behavioral Coping Strategies

Several studies have uncovered behavioral strategies SNS users employ to cope with privacy challenges. Most studies have focused on personal-level actions and processes: how an individual user employs various privacy settings or privacy-enhancing mechanisms available in SNSs [20, 35, 40]. For instance, previous studies have suggested that Facebook users change privacy settings when they have prior experience of privacy invasion [8], but most people keep the default privacy settings [11, 21].

Users employ a variety of mental and behavioral coping strategies in addition to technical strategies. Self-censorship is prevalent among SNS users to the extent that many SNS users decide not to post personal content on SNSs [18]. Users also adapt their disclosure behavior by only posting information that is suitable for the public, which is called the "common denominator" approach [12]. SNS users also actively manage information privacy by deleting content from one's profile or wall [41].

Studies have also discovered diverse sets of interpersonal coping mechanisms. Consistent with Altman's notion of privacy [2], SNS users engage in various ways to dynamically regulate interpersonal boundaries. For instance, they segregate their interaction with different audiences using a "friends only" profile [35]. Users also create multiple profiles on SNSs to prevent different social circles from overlapping (i.e., context collapse) [34].

Lampinen and colleagues [18] suggested a more comprehensive framework of privacy management strategies, distinguishing between behavioral versus mental, individual versus collaborative, and preventive versus corrective strategies. While people develop a wide variety of behavioral strategies, they rarely enact them. Instead, SNS users rely largely on mental strategies, such as information control or simply trusting others to be considerate of privacy protection, and expect that their privacy efforts will be reciprocated by their friends [18].

Wisniewski and colleagues [41] suggested that privacy management on Facebook is more than just information control or changing privacy settings because effective privacy management requires a constant regulation of interpersonal boundaries, such as choosing who to friend or unfriend. More importantly, they distinguished between *technology-supported boundary mechanisms*, behaviors supported through SNS interface controls, and *coping mechanisms*, which are an individual's response outside of these confines. They argue that people are more likely to apply coping mechanisms rather than technological mechanisms.

PRESENT STUDY

Though previous studies have proposed several ways to conceptualize networked privacy management in SNSs, most studies are qualitative and explorative using small samples. As such, there has been a call for more quantitative studies with a systematic metric that affords comparing findings across studies [25], or to generalize findings to a larger population [18]. A few studies have adopted a quantitative approach and examined underlying reasons why users adopt or reject coping mechanisms, but they have focused on the adoption of certain technological mechanisms, such as a friends-only profile [35], advanced privacy settings of Facebook [9, 40], and privacy enhancing technology [33]. While technological mechanisms are an important aspect of privacy management, privacy behavior on SNSs is not limited to "privacy settings" [9] or technology-supported mechanisms [41]. In fact, SNS users use various strategies that they devise outside explicit boundary-regulation interface features [41]. For instance, prior work suggests that collaborative privacy management is potentially multidimensional because they include at least a few more mechanisms, such as mental strategies [18] and coping strategies [41]. Hence, research has yet to empirically examine how and why individuals in varying contexts or conditions develop and apply different types of strategies to cope with the challenges associated with networked privacy management.

To address this gap in prior research, the present study takes a multi-methods and multinational approach. Using a qualitative study (focus group interviews: FGI) and findings from prior research, we identify several privacy strategies that Facebook users apply to co-manage their privacy when using Facebook. Drawing on the behavioral themes uncovered in this preliminary work, we develop a new survey instrument and test its reliability, validity, and dimensionality using survey data collected in two countries (see the below method section for details). Finally, we explore the conditions in which people develop and apply different privacy strategies. In doing so, we aim to provide a more complete understanding of networked privacy by addressing the following research questions.

RQ1: How do SNS users co-own and co-manage shared information, and what are their privacy practices (via technological, behavioral, and mental mechanisms)?

a. What is the underlying dimensionality of networked privacy management strategies?

b. *What types of coping mechanisms do people most commonly adopt or reject?*

RQ2: Why do people develop and apply different coping mechanisms? Under what conditions are people likely to enact different types of networked privacy management?

RQ1 is explorative/descriptive whereas RQ2 is prescriptive/predictive. In order to address RQ2, we develop a research model (see figure 1). The model includes several theoretical constructs central to privacy research such as attitudes, self-efficacy, and privacy concern, which have been found to have significant relationships with privacy behavior. Specifically, numerous studies have confirmed that privacy concern is a key factor that determines privacy behavior [9], but the degree to which people engage in privacy protection behavior is also determined by their self-efficacy beliefs that they have the sufficient resources and skills to carry out the action [30]. Hence, we predict that privacy concern (H1) and self-efficacy beliefs (H3) will have a positive association with networked privacy management. Information sharing is an essential motivation for many SNS users [15]. People are less likely to employ privacy-enhancing behavior when the perceived benefit of personal disclosure outweighs its perceived risk [8]. Hence, users who have favorable attitudes toward information sharing are less likely to engage in privacy management strategies (H2) because these privacy protection behaviors may hinder them from sharing their information with a large audience.

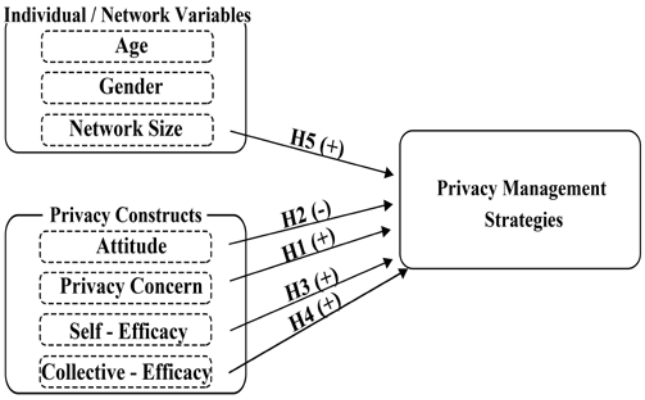

Figure 1. Research Model

We also add variables that were relatively unexplored in previous privacy research (e.g., collective efficacy, ego-network size) because collective behavior, such as collaborative privacy management, should be influenced by constructs related to group- and network-level properties. For a successful collective action (e.g., collaborative privacy management) to occur, individual control alone is not sufficient because the action requires a group effort and collective support [29]. Hence, we predict that users are more likely to engage in networked privacy management when they are confident that their network ties are competent, cohesive, and trustful (i.e., high collective-efficacy; H4). Finally, given that a large network size leads to context collapse and information leakage [35], we predict that ego-network size should be positively associated with privacy management strategies (H5). Figure 1 depicts the research model tested in this study.

FOCUS GROUP INTERVIEWS

Method

Recruitment

We invited students of a large university in Singapore to participate in our focus group study. A total of 28 participants were recruited through a combination of department-wide e-mails and advertisements placed in the "News" section of the University's e-learning platform. All participants received a small token of appreciation in the form of a book voucher. We only conducted focus group interviews in Singapore because previous studies [18, 41] already conducted similar focus groups in the U.S or Finland, which provided useful findings related to our research. Hence, we focused on the Singapore sample and assumed that previous research could complement the findings of the present study.

Procedure

We conducted five focus groups with 28 participants over the course of one week in June 2014. Each focus group was one hour long and emphasized, when possible, diversity in gender and age. In total, we spoke with 10 female and 18 male participants between the ages of 19 and 27, with 20 undergraduate participants and eight post-graduate participants.

At the beginning of the focus group, participants were informed about the purpose of the study: to learn about user opinions and behaviors with respect to privacy on Facebook. The groups were asked a series of questions regarding their own past and typical behavior on Facebook, such as the type of content they most commonly used Facebook for. Following this, the groups were asked to reflect on how they selected privacy settings for the various pieces of information they share, especially when the content also involved their peers. We further asked participants to recall specific examples of privacy violations and how they were managed.

Two facilitators were present at each focus group, with one leading the discussion and the other taking hand-written notes about participant speech turn-taking to help in transcribing the discussion.

Analysis

In our subsequent analysis, we used an inductive and grounded approach to examine prevalent privacy management strategies. Both facilitators at the focus groups performed the analysis in consultation with one another. First, transcripts of focus group audio recordings and facilitator notes were open coded to identify, group by group, unique privacy management strategies. Our units of analysis were individual phrases or parts of phrases from

each participant. These strategies were grouped into conceptually similar categories. We iterated this process across focus groups, identifying conceptually similar themes. Initial themes emerged concerning group strategies, personal strategies, boundary violations, trust, ownership, transparency, reasons to use Facebook, and platform limitations. For this analysis, we focused our attention at group and personal strategies to identify common sub-groups of strategies. Four overall themes emerged, discussed below.

Results (Theme extraction)

In this study we were specifically interested in how users managed the privacy of information that is produced collaboratively: either content that is uploaded by others involving the participant or content uploaded by the participant that also involves others. We found that our participants used four distinct sets of privacy management strategies.

Corrective Strategies

Participants across all five groups reported the use of existing privacy management features such as untagging, timeline review, or asking peers to remove content. These features allow users to control the visibility of unwanted content posted about them by others after the content has been published. Thus we label them as corrective strategies related to content management.

Participants reported untagging themselves mainly from content that was irrelevant (P6, 12) or did not present them in the best light, such as photos in which they appear "unglam" [unattractive] (P12, 18, 21). Asking to remove content appeared to be a feature reserved for more serious transgressions of privacy, such as being linked to a potential misdemeanor (P7), or when comments elicited by the content shared were judged "embarrassing" and "irritating" (P12, P14). As such, this strategy was used comparatively rarely. As P14 explains, timeline review and the ability to untag oneself alleviate the need for users to ask peers to remove content explicitly.

Participants indicated awareness that untagging does not remove content from general circulation on Facebook, as well as a hesitation to request for content removal except in serious circumstances. Thus they also employed preventative measures together with corrective strategies, as described below.

Preventive Strategies

Controlling the friend's network, rather than attempting to control the visibility of shared content, was another privacy management strategy that emerged. Specifically, this approach aims to prevent information leakage by constraining the audience. For instance, several participants reported using the friend lists feature to create distinct groups they share content with to avoid context collapse (P4, P18, P28). Specifically, P4 noted the necessity of creating "isolated friend lists" with no overlap in membership to prevent information leakage between different groups of friends or between friends, family, and coworkers. Similarly, respondents also used secret groups to share content between distinct subgroups of friends, because the very nature of a secret group ensures content cannot be shared outside of this limited network (P4, 7, 9, 11, 19, 20, 25).

Some participants recognized that using different friend lists involves significant cognitive overhead. Instead, they preferred to cull their overall friend list on a regular basis, because removing loose ties and maintaining a smaller number of friends reduces the overall load of controlling access (P9, 10, 20, 21, 25, 28). Likewise, participants also refrained from accepting friend requests from individuals that may make it more difficult to manage sharing content in the future, such as family and coworkers (P4, 5, 12, 21, 25, 28).

Several participants highlighted that the use of preventative features described above is "mentally draining" (P5) and introduces a high cognitive overhead to interacting with the site. Instead, some participants indicated a preference for information control described in the following section.

Information Control

Addressing the complexities of corrective and preventive strategies related to content management and network management, respondents across the five groups indicated a shift in their own mental strategies as the third possible way to individually deal with managing networked privacy. Specifically, participants either self-censored or made peace with the public nature of information sharing on the platform.

Some participants noted that they self-censor content published concerning oneself and others—they only share content when it is appropriate for all audiences (P5, 8, 16, 21). For instance, P21 recalls that, before they post, "I think to myself – my boss is going to read this." Similarly, because P5 is always mentally aware that their friends' parents may be monitoring their Facebook feed, P5 avoids posting potentially inappropriate content about friends. Participants suggest that an implicit set of social norms exists between peers about what is appropriate to be shared and trust that "only appropriate photos will be posted on Facebook" (P16). Participants estimate that these norms are based on information peers share about themselves on Facebook (P25), as well as explicit coordination described in the following section.

Other participants choose instead to accept that all information published about themselves and others is a consequence of having a presence on an inherently public platform:

"Actually, Facebook is all about publicity. Like, whatever you post, you are ready for other people to view." (P12)

Some participants have internalized the necessity of sharing in the social media landscape. Tellingly, P15 remarks that "If you need privacy, just hide in a cave." This highlights the assumption that having a social media presence presumes life under public scrutiny:

While the information control approach errs on the side of caution when sharing information about others, the view of Facebook as a public platform assumes an almost post-privacy perspective in which there is no boundary between what happens in real life and what is published on social media. It should be noted that the focus groups diverged on this issue.

Collaborative Strategies

Aside from the implicit protection of others' information on Facebook as described above, participants also described the use of explicit coordination mechanisms to collectively manage each other's privacy.

Specifically, participants across all five groups reported discussing with their peers whether and which content (such as photos or check-ins) from a group event was appropriate to be published on Facebook (P2, 3, 4, 5, 7, 12, 19, 20, 21, 24). Participants reported discussions both before and after the event. Discussions also occurred face-to-face and virtually over instant message groups or inside secret Facebook groups. For instance, P20 recalls a friend requesting in advance that any photos from an outing be kept private because the friend had not informed others about being in town. Participants further suggest that the onus is on the person producing the content (e.g., taking photos) to ask for permission before uploading: "If you want to post something, let me know" (P11, 12).

Sometimes negotiations may even occur during the event:

"Usually, my friends and I QC [filter out] the 'unglam' [unattractive] photos; […] if we are at a gathering we will pass the phone around for everyone to determine if the photo is acceptable." (P24)

Participants also reported taking direct action to educate their peers when experiencing a privacy violation, seeing this happen to others, or foreseeing potential privacy issues in the future (P4, 9, 12, 21). For instance, a recent graduate who has just joined the teaching service advised her colleague to opt out of being searched for by name in order to avoid getting friend requests from students (P21).

SURVEY RESEARCH

Method

Data Collection & Sample

Drawing on key behavioral themes identified from the FGI and previous research [18, 41], we developed a total of 54 survey items to assess various aspects of networked privacy management. Aside from seven items adapted from a previous study [35], most items were newly developed due to the lack of a pre-validated scale related to networked privacy management. We pre-tested the survey items using a pilot survey with 27 students from the same university. We conducted preliminary explorative factor analyses (EFAs) employing varimax rotation. The goals of these analyses was to retain a set of items that would represent multiple aspects of networked privacy management and to extract the set of items to a manageable number that could be readily and easily employed in future research. We refined the survey instruments by removing items that displayed either low convergent validity (factor loadings <. 40 with parental factors) or discriminant validity (cross-loadings > .40) or that were overly redundant. The initial analyses resulted in a total of 28 items, which were employed in the final surveys.

The final version of the surveys was administered by a professional online research company (Qualtrics). We collected data from two countries, Singapore and the U.S., to ensure that behavioral themes uncovered from FGI can be applied to different countries and to examine patterns of networked privacy management across cultures. We chose Singapore and the U.S. as study sites because they represent Eastern and Western cultures, respectively. Both countries are economically developed, have well-established ICT infrastructures and services, have relatively high Facebook penetration, and have mainly English-speaking populations. These similarities help remove factors that can potentially confound cross-national comparisons. Participants were randomly selected from online panels recruited by Qualtrics. The panel is an opt-in, privacy-protected participant pool. It consists of over 20 million panelists (6 million members in North America and 6.4 million in Asia Pacific). The research company runs regular benchmarking surveys to ensure their panelists are representative of the larger population. Eligibility was restricted to Facebook users who are older than 18 (for U.S.-based participants) and 21(Singapore-based participants) and visited their Facebook page at least once every two weeks. A total of 307 (Singapore: 151, the U.S.: 156) respondents participated in the survey. We eliminated eight unreliable responses, resulting in 299 respondents in the final sample. The Singapore sample (n = 153) consisted of 75 (49.0%) females and 78 (51.0%) males, and the U.S. sample (n = 146) consisted of 73 (50%) females and 73 (50%) males. The mean age of the Singapore sample was 37.72 (SD = 10.61) and that of the U.S. sample was 44.59 (SD = 16.53). The majority of the Singapore sample (n = 92, 76.5%) and the U.S. sample 63% (n = 92, 63.0%) had more than 81 Facebook friends.

Measures

In addition to the 28 items developed to assess networked privacy management, we employed several pre-validated scales adapted from previous studies in order to assess potential antecedents of privacy strategies. A seven-point Likert-type scale was used for all measures. We assessed *privacy concerns* using a four item scale (e.g., "I am concerned that I disclose too much personal information

when using Facebook," Cronbach's α = .87) adapted from Xu and colleagues [44]. *Privacy self-efficacy* was assessed by a five item scale (e.g., "I feel confident adjusting the privacy settings on my Facebook account, α = .93) adapted from Lampe and colleagues [17]. *Attitudes* toward information sharing in an SNS was assessed by five items (e.g., "Sharing personal information on Facebook is wise," α = .83) adapted from Igbaria and colleagues [14]. *Collective efficacy* was assessed by seven items (e.g., "Friends in my social network look out for each other," α = .93) adapted from Sampson and colleagues [29]. Finally, we measured age, gender, and ego-network size (i.e., the number of Facebook friends) using a single-item scale.

Results

We examined the dimensionality of collaborative privacy management and its relationships with other constructs using explorative factor analysis (EFA) and hierarchical regression analyses. Though confirmatory factor analysis (CFA) and structural equation modeling (SEM) could be alternative approaches, we deemed the former to be more appropriate for this study. CFA and SEM require specification of a model supported by theory or previous research [37]. To the best of our knowledge however, there is no *prior* measurement or theoretical model regarding networked privacy management. Given that this study is one of the first attempts to examine diverse sets of collaborative strategies using a quantitative approach, we chose EFA and regression analyses instead. Note that our intention was to *explore* the possible underlying factor structure of a set of observed variables without imposing a preconceived structure on the outcome.

To address RQ1, we examined the underlying dimensions of networked privacy management. The results of the initial EFAs suggested that eight original items lack convergent or discriminant validities: low factor loadings (< .40) with their parent factors or high cross-loadings (> .40) with other factors. Once those problematic items were removed from subsequent analyses, the results of the EFA suggested a four-factor structure model that is generally in line with the findings of the FGI. Table 1 shows the results of the final EFA model with varimax rotation. Note that we combined Singapore and the U.S. samples for the final factor model. We ran preliminary analyses for each country separately, and the results showed that the U.S. and Singapore samples exhibited similar patterns through factor loading for each item varied slightly across two samples. In order to make our subsequent analyses comparable across two samples, we chose to use the same set of factors for both samples.

The four factors that emerged from the EFA explained 67.65% of the variance. Most items displayed adequate face validity, convergent validity, and discriminant validity. Two items (i.e., "use of timeline feature" and "unfriending") displayed slightly low factor loadings (.52 and .58, respectively) with their parental factors, but we decided to keep them because FGI participants identified them as important strategies. The first factor is referred to as "*collaborative strategies*," which consists of behavioral items related to negotiation, interpersonal actions, and decision making related to collaborative privacy management. The second factor represents "*corrective strategies*," which refer to privacy actions that Facebook users enact when privacy is at risk, such as untagging, unfriending, requesting peers to remove contents. The third factor is "*preventive strategies*" through which users can limit their audience or control interpersonal/network boundaries. The fourth factor is "*information control*," which includes items related to self-censorship or the common denominator approach.

Items	Components			
	1	2	3	4
My friends and I negotiate a "rule of thumb" about sharing content concerning ourselves.	**.82**	.20	.26	-.01
My friends and I agree on a "rule of thumb" about sharing content concerning ourselves.	**.86**	.19	.22	.03
Prior to disclosing content, my friends and I discuss the appropriate privacy settings.	**.85**	.24	.23	.02
I ask for approval before disclosing content from those involved.	**.78**	.12	.17	.18
My friends ask for approval before uploading content concerning myself.	**.85**	.20	.12	.02
I discuss appropriate privacy settings with my friends before creating a Facebook group.	**.83**	.16	.26	.10
I educate my friends about privacy issues.	**.60**	.24	.18	.31
I untag myself from photos my friends uploaded.	.18	**.87**	.22	.03
I ask friends to remove content concerning myself.	.32	**.84**	.10	.02
I delete content posted about me by my friends.	.20	**.86**	.22	.01
I regularly unfriend individuals (remove individuals from my friends list).	.22	**.52**	.21	.21
I make use of friend lists to restrict the audience of my posts to certain individuals.	.19	.15	**.61**	.37
I prefer to share and circulate photos from gatherings with my friends through other communication channels such as email.	.20	.26	**.62**	-.02
I use secret groups to share content about my friends.	.16	.15	**.78**	-.03
I allow my Facebook friends to view only the mutual friends they share with me.	.30	.10	**.66**	.11
I use the timeline review function as a self-precautionary measure.	.26	.20	**.58**	.30
I only upload content about my friends that is suitable for public consumption.	.07	-.02	.11	**.78**
I will not post content concerning my Facebook friend(s) if I deem it to be potentially harmful.	.02	.06	-.03	**.83**
I only post information that I deem appropriate for public viewing.	.11	.09	.19	**.74**

Table 1. Results of explorative factor analysis

Table 2 reports internal consistency (Cronbach's α) and descriptive statistics for four different privacy management strategies. Cronbach's α for each variable was above (or very close to) the conventional cutoff (>.70), indicating adequate internal consistency for all measures.

As table 2 shows, the most commonly applied privacy strategy was *information control* followed by *preventive,*

collaborative, and *corrective* strategies. All mean scores were above the mid-point (3.5 for a seven-point Likert scale) except for corrective strategies (M US = 3.43), indicating that Facebook users utilized various privacy mechanisms to cope with privacy challenges in SNSs. The Singapore sample was more likely to enact *collaborative* and *preventive* strategies than the U.S. sample.

Behavioral Strategies	α	Mean (SD)			*Diff.*
		Singapore	US	All	
Collaborative	.94	4.19 (1.28)	3.81 (1.58)	4.01 (1.44)	t(*297*) = 2.32*
Corrective	.86	3.66 (1.25)	3.43 (1.49)	3.55 (1.37)	t(*297*) = 1.43
Information Control	.69	5.80 (.72)	5.72 (1.22)	5.76 (1.00)	t(*297*) = .71
Preventive	.77	4.82 (1.02)	4.09 (1.30)	4.47 (1.22)	t(*297*) = 5.35**

*p<.05, ** p <.01

Table 2. Descriptive statistics

To address RQ2 and H1-H5, we performed hierarchical regression analyses predicting four privacy management strategies as dependent variables. We entered predictor variables in a hierarchical manner: control variables (age, gender) were entered the first block, and predictor variables related to privacy in the second block. Table 3a and 3b reports the results of regression analyses.

Block	Predictors	Standardized Beta			
		Collaborative	Corrective	Info. Control	Preventive
1	Age	.24*	.21*	-.03	.10
	Gender	-.09	-.01	-.06	-.11
2	Age	.20*	.23*	-.05	.08
	Gender	-.05	-.01	-.04	-.09
	Network Size	.14^	-.02	.15^	.21*
	Attitude	.07	-.08	-.15^	-.12
	Privacy Concern	.32***	.19*	.34***	.42***
	Self-efficacy	.17*	.09	.21**	.24**
	Collective-efficacy	.31***	-.19*	.20**	.09
Model 1: R^2		.01	.05	.01	.01
Model 2: R^2		.32	.13	.26	.30
F Change		13.65***	2.70*	9.28***	11.80***

^ p<.10, *p<.05, **p<.01, *** p<.001

Table 3a. Results of regression analyses predicting privacy management strategies (the Singapore sample)

Block	Predictors	Standardized Beta			
		Collaborative	Corrective	Info. Control	Preventive
1	Age	.06	-.01	.05	-.01
	Gender	-.08	.01	.17**	.06
2	Age	.06	.04	.11	.01
	Gender	-.13	-.09	.11	-.01
	Network Size	.10	.11	.16^	.00
	Attitude	.05	-.12	-.13	-.04
	Privacy Concern	.47***	.58***	.37***	.51***
	Self-efficacy	.16^	.19*	.25**	.15
	Collective-efficacy	.20*	-.07	.04	.05
Model 1: R^2		.01	.01	.04	.01
Model 2: R^2		.28	.36	.24	.26
F Change		13.13***	15.09***	7.33***	9.52***

^ p<.10, *p<.05, **p<.01, *** p<.001

Table 3b. Results of regression analyses predicting privacy management strategies (the U.S. sample)

The results showed that four dimensions of privacy management strategies had slightly different relationships with predictors. H1 predicted that privacy concern leads to networked privacy management. The results showed that *privacy concern* (H1) had a significant and positive association with all four strategies in both samples. The results suggest that privacy concern is a key factor that determines privacy behavior, lending support for H1. H2 predicted that favorable attitudes toward information sharing would have a negative association with networked privacy management. However, a*ttitudes* (H2) had only one marginally significant, negative relationship with information control (β [Sing.] = -.15, p =.052). Hence, H2 was not supported. H3 and H4 predicted that self-efficacy (H3) and collective efficacy (H4) would have a positive association with networked privacy management. *Self-efficacy* (H3) had a positive association with collaborative (β [Sing.] = .24, p <.01; β [US] = .16, p = .09), corrective (β [US] = .19, p <.05), information control (β [Sing.] = .21, p <.01; β [US] = .25, p <.01), and preventive strategies (β [Sing.] = .24, p <.01). *Collective efficacy* (H4) had a positive association with collaborative strategies (β [Sing.] = .31, p <.001; β [US] = .20, p <.05) and information control (β [Sing.] = .20, p <.01), but a negative association with corrective strategies (β [Sing.] = .17, p <.05). The results suggest that people are more likely to enact various, if not all, networked privacy management practices when they are confident that their network ties and they themselves have the capacity and resources to cope with the challenges of networked privacy management. Hence, H3 and H4 were

partially supported. Finally, *ego-network size* (H5) displayed a significant, positive association with preventive strategies ((β [Sing.] = .21, p <.05), indicating that Facebook users are more likely to engage in preventive privacy actions when their network size is larger, leading to potential information leakage. Network size also had a marginally significant association with information control (β [Sing.] = .15, p =.08; β [US] = .15, p =.07) and collaborative strategies (β [Sing.] = .14, p =.09). Hence, H5 was partially supported.

DISCUSSION

Several key findings emerged. First, there are mainly four dimensions of networked privacy management: collaborative strategies, corrective strategies, preventive strategies, and information control. Second, these behavioral strategies are associated with different sets of antecedents, indicating that users' enactment of different privacy strategies are motivated by somewhat distinct conditions. Third, privacy behavior in SNSs is essentially social and communicative given that (a) a significant portion of networked privacy management is based on an interpersonal process of communicating, agreeing, negotiating, and reaching mutual decisions; and (b) these actions are significantly associated with factors related to collective-level properties, such as collective efficacy and ego-network size.

Conceptualization and Operationalization of Networked Privacy Management

First, we specify the underlying dimensionality of networked privacy management, which enables several theoretical and practical contributions. From a research perspective, specifying the dimensionality of an unexplored construct is beneficial since this provides researchers with a better idea of how to conceptualize and operationalize the concept under investigation. The notion of networked privacy management is relatively new to privacy and CSCW researchers, requiring more scholarly discussion on conceptual explication [25, 38]. In this study, we contribute to the field by presenting a novel way of conceptualizing and operationalizing networked privacy management, which can be reassessed and reemployed in future studies of collaborative privacy practices. For instance, this study provides a newly developed metric that reflects different dimensions of networked privacy management. We also provide evidence of the validity of these measures. Using such a systematic or coherent measure is beneficial for researchers as this allows researchers to successfully communicate and compare findings across studies, which advances research on networked privacy.

From a practical perspective, a systemic metric with specific dimensions makes it easier for us to quickly comprehend users' overall behavioral patterns or to quantitatively examine the overall prevalence of different types of privacy practices using large samples. Knowing which type of privacy actions is employed most frequently or infrequently may provide useful insights or opportunities for designers and managers when deciding the user behavior to focus on. For instance, our findings show that Facebook users employ several technological mechanisms to manage networked privacy (e.g., untagging, unfriending, friend-only profile, secret group, and timeline review). However, we find that Facebook users in both countries also apply a wide variety of collaborative strategies to co-own and co-manage private information. These collaborative actions typically cannot be performed easily through an SNS itself, and SNS users involve alternative ways to coordinate interpersonal actions and decision-making related to networked privacy management. According to Lampinen and colleagues [18], this added layer of difficulty tends to push SNS users toward relying on mental strategies (trusting or being trustworthy). Indeed, we find that information control (M = 5.76, SD = 1.00) is the most commonly adopted behavioral strategy in both countries (see table 2), which may result in reduced information sharing and less effective use of SNSs.

Though prior research suggested that "many participants had never negotiated or even discussed shared rules of disclosure with their friends" [18:3222], our findings suggest that people actually engage in such collaborative privacy practices. However, Facebook provides a limited interface to support these explicit coordination mechanisms. The findings from the FGI and prior research show that this coordination mostly happens *outside* the SNS environment in that users find ways to use offline or private communication with their friends to perform these actions.

Overall, the findings suggest that many SNS users engage in a variety of mental and behavioral mechanisms in the absence of an effective system to support collaborative privacy management. Recently, researchers have proposed several prototypes to support collaborative privacy practices [3, 13, 32]. For instance, prior work has prototyped applications that help co-owners of shared content separately specify their own privacy preferences [32] and promote mutual awareness about privacy preferences among friends on the same network [3]. Our findings may complement this approach by highlighting key types of collaborative actions that people are likely to enact when coping with various privacy challenges in SNSs. Also, the survey instrument developed in this study can be a useful tool to assess users' privacy needs and behaviors when designing a new system for collaborative privacy management.

Antecedents of Networked Privacy Management

Second, we find that each set of privacy management strategies is associated with different sets of antecedents (see Tables 3a and 3b). A closer examination of these findings confirm that the observed relationships display theoretically reasonable patterns. For instance, collective efficacy has a *positive* association with collaborative management strategies. Consistent with prior research on efficacy beliefs, group-level efficacy beliefs play a

significant role when the target action requires active coordination and collaboration among multiple stakeholders [29]. In contrast, collective efficacy had a *negative* relationship with corrective strategies. It appears that when users have a high level of collective efficacy, they are less likely to rely on intrusive actions that might damage mutual trust between parties (e.g., asking peers to remove content concerning himself/herself). Collective efficacy has a *positive* association with information control, suggesting that people with high collective efficacy mutually commit to holding norms (e.g., being a trustworthy person by not sharing inappropriate content concerning each other). Meanwhile, collective efficacy does not have a significant relationship with preventive strategies. A possible reason is that limiting the audience or controlling others' access rights becomes less important when people perceive their network ties are cohesive and trustful. The selective relationships observed in this study further confirm the multidimensional nature of networked privacy management. As described above, a researcher can observe positive, negative, or non-significant associations depending on the type of privacy behavior that the researcher focuses on. If a study narrowly focuses on a certain dimension or uses a unidimensional measure of networked privacy management, the results can be vastly different or even misleading. Hence, we suggest that future studies should take into account the dimensionality of networked privacy management observed in this study. The multidimensional instruments developed in this study can be useful for capturing a more accurate picture about the relationship between networked privacy management and its antecedents or outcomes.

Third, the findings highlight facilitating or constraining conditions under which people are more likely to engage in privacy enhancing behaviors. Consistent with prior work, individual-level factors, such as privacy concerns and self-efficacy beliefs, have significant associations with privacy behavior. We also find that group or network related factors, such as collective-efficacy and ego-network size, have significant (or at least marginally significant) associations with certain dimensions of privacy behavior. Overall, the findings highlight that networked privacy management is essentially a social process or a group property influenced by a wide variety of factors including both individual- and group-related factors. Based on these findings, we encourage researchers and designers of privacy management systems to more broadly consider motives and practices of SNS users. From a research standpoint, future studies should examine the role of related variables such as group/collective efficacy, team potency, proxy efficacy, generalized reciprocity, peer norms, and descriptive norms when examining networked privacy management. This will provide a better understanding of how collaborative privacy actions and decisions are shaped through interpersonal and group-level dynamics and processes. From a practical perspective, the findings also provide useful insights about how to design or deploy privacy enhancing technologies or policies. For instance, people are likely to engage in collaborative privacy practices when collective efficacy beliefs are high. Hence, we suggest that designers should develop a privacy management system that makes others' privacy efforts and actions visible to each other. This will enhance mutual trust and collective-efficacy beliefs, which will increase the likelihood of more active and prolonged use of such a system.

Limitations and Directions for Future Studies

There are a few limitations of this present study that should shape the direction of future studies. First, we observed a few significant differences across two samples (e.g., the degree to which people engage in privacy management strategies). The cross-national differences observed in this study seem to suggest that future research should locate the sources of potential differences across cultures. We do not know whether national differences are due to differences in national cultures (e.g., individualistic versus collectivistic cultures), privacy regulations, or other socio-contextual ones. This would be an area for potential future research.

Related to this issue, this study chose only two sites (Singapore and the U.S.) for data collection. Though many studies have chosen two countries for cross-national comparisons of distributed groups [36] and privacy [7], a more comprehensive and accurate understanding about privacy behaviors across cultures can be gained when future studies employ diverse samples in different countries.

Participants in both FGI and online surveys are voluntary samples who are more likely to share their opinions and ideas with researchers. As such, they might have lower levels of privacy concerns than the general population. Though this is almost an unavoidable problem for any privacy research, our findings should be interpreted with some caution. We believe that this does not impose a significant threat to validity given that participants in our study have a fairly high level of privacy concerns ($M = 5.22$, $SD = 1.26$).

Facebook introduced new privacy settings in January 2015, a few months after we conducted FGI and online surveys. It would be worthwhile to check if users have become more or less proactive in applying the four different privacy management strategies identified in this study.

CONCLUSION

Taken together, the findings advance our understandings of privacy in a networked environment. Specifically, this study (a) reframes/conceptualizes privacy with an extended analytical focus on an interpersonal- and group-level aspects of privacy management, moving beyond an individual centric notion of privacy; (b) explores the underlying dimensions of networked privacy management using a newly developed metric, which can be reemployed in future privacy research; and (c) specifies the ways in which this underexplored privacy behavior is linked to

theoretical constructs central to privacy perceptions and beliefs. We hope to see continued efforts to complement and advance the findings presented in this study.

ACKNOWLEDGEMENTS

This research is supported by a grant from the National University of Singapore (R124-000-053-112).

REFERENCES

1. Irwin Altman. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.* Cole Publishing Company, Monterey, CA.
2. Irwin Altman, Anne Vinsel, and Barbara B. Brown. 1981. Dialectic conceptions in social psychology: An application to social penetration and privacy regulation. *Advances in Experimental Social Psychology* 14: 107–160.
3. Andrew Besmer, Heather Richter Lipford, Mohamed Shehab, and Gorrell Cheek. 2009. Social applications: exploring a more secure framework. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, 1-10.
4. Yunan Chen and Heng Xu. 2013. Privacy management in dynamic groups: Understanding information privacy in medical practices. In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work* (CSCW'13), 541–552.
5. Jeffrey T. Child and David A. Westermann. 2013. Let's be Facebook friends: Exploring parental Facebook friend requests from a communication privacy management (CPM) perspective. *Journal of Family Communication* 13, 1: 46–59.
6. Hichang Cho, Jae-Shin Lee, and Siyoung Chung. 2010. Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior* 26, 5: 987–995. http://doi.org/10.1016/j.chb.2010.02.012
7. Hichang Cho, Milagros Rivera-Sánchez, and Sun Sun Lim. 2009. A multinational study on online privacy: global concerns and local responses. *New Media & Society* 11, 3: 395–416.
8. Bernhard Debatin, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes. 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication* 15, 1: 83–108.
9. Nicole B. Ellison, Jessica Vitak, Charles Steinfield, Rebecca Gray, and Cliff Lampe. 2011. Negotiating privacy concerns and social capital needs in a social media environment. In *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, Sabine Trepte and Leonard Reinecke (eds.), Springer, 19–32.
10. Bethany D. Frampton and Jeffrey T. Child. 2013. Friend or not to friend: Coworker Facebook friend requests as an application of communication privacy management theory. *Computers in Human Behavior* 29, 6: 2257–2264.
11. Ralph Gross and Alessandro Acquisti. 2005. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 71–80.
12. Bernie Hogan. 2010. The Presentation of Self in the Age of Social Media: Distinguishing Performances and Exhibitions Online. *Bulletin of Science, Technology & Society* 30, 6: 377 –386. http://doi.org/10.1177/0270467610385893
13. Hongxin Hu, Gail-Joon Ahn, and Jan Jorgensen. 2011. Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. In *Proceedings of the 27th Annual Computer Security Applications Conference*, 103–112.
14. Magid Igbaria, Tor Guimaraes, and Gordon B. Davis. 1995. Testing the determinants of microcomputer usage via a structural equation model. *Journal of Management Information Systems*: 87–114.
15. Adam N. Joinson. 2008. Looking at, looking up or keeping up with people?: Motives and use of Facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI'08), 1027–1036.
16. Maggie Kanter, Tamara Afifi, and Stephanie Robbins. 2012. The impact of parents "friending" their young adult child on Facebook on perceptions of parental privacy invasions and parent–child relationship quality. *Journal of Communication* 62, 5: 900–917.
17. Cliff Lampe, Donghee Yvette Wohn, Jessica Vitak, Nicole B. Ellison, and Rick Wash. 2011. Student use of Facebook for organizing collaborative classroom activities. *International Journal of Computer-Supported Collaborative Learning* 6, 3: 329–347.
18. Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in it together: interpersonal management of disclosure in social network services. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI'11), 3217–3226.
19. Dale G. Larson and Robert L. Chastain. 1990. Self-concealment: Conceptualization, measurement, and health implications. *Journal of Social and Clinical Psychology* 9, 4: 439–455.
20. Kevin Lewis, Jason Kaufman, and Nicholas Christakis. 2008. The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication* 14, 1: 79–100.
21. Yabing Liu, Krishna P. Gummadi, Balachander Krishnamurthy, and Alan Mislove. 2011. Analyzing Facebook privacy settings: user expectations vs.

reality. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, 61–70.

22. Stephen T Margulis. 2003. On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues* 59, 2: 411–429.
23. Alison R. Murphy, Madhu C. Reddy, and Heng Xu. 2014. Privacy practices in collaborative environments: A Study of emergency department staff. In *Proceedings of the 2014 Conference on Computer Supported Cooperative Work & Social Computing* (CSCW'14), 269-282.
24. Helen Nissenbaum. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.
25. Xinru Page, Karen Tang, Fred Stutzman, and Airi Lampinen. 2013. Measuring networked social privacy. In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work Companion*, 315–320.
26. Leysia Palen and Paul Dourish. 2003. Unpacking privacy for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI'03), 129–136.
27. Sandra Petronio. 2002. *Boundaries of Privacy: Dialectics of Disclosure*. State University of New York Press.
28. Sandra Petronio. 2013. Brief status report on communication privacy management theory. *Journal of Family Communication* 13, 1: 6–14.
29. Robert J. Sampson, Stephen W. Raudenbush, and Felton Earls. 1997. Neighborhoods and violent crime: A multilevel study of collective efficacy. *Science* 277, 5328: 918–924.
30. Dong-Her Shih, Sheng-Fei Hsu, David C. Yen, and Chia-Chia Lin. 2012. Exploring the individual's behavior on self-disclosure online. *International Journal of Human-Computer Interaction* 28, 10: 627–645. http://doi.org/10.1080/10447318.2011.654198
31. H. Jeff Smith, Tamara Dinev, and Heng Xu. 2011. Information privacy research: An interdisciplinary review. *MIS Quarterly* 35, 4: 989–1016.
32. Anna Cinzia Squicciarini, Mohamed Shehab, and Federica Paci. 2009. Collective privacy management in social networks. In *Proceedings of the 18th International Conference on World Wide Web*, 521–530.
33. Anna C. Squicciarini, Heng Xu, and Xiaolong Luke Zhang. 2011. CoPE: Enabling collaborative privacy management in online social networks. *Journal of the American Society for Information Science and Technology* 62, 3: 521–534.
34. Frederic Stutzman and Woodrow Hartzog. 2012. Boundary regulation in social media. In *Proceedings of the 2012 Conference on Computer Supported Cooperative Work* (CSCW'12), 769–778.
35. Fred Stutzman and Jacob Kramer-Duffield. 2010. Friends only: examining a privacy-enhancing behavior in facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI'10), 1553–1562.
36. Bernard CY Tan, Kwok-Kee Wei, Richard T. Watson, Danial L. Clapper, and Ephraim R. Mclean. 1998. Computer-mediated communication and majority influence: Assessing the impact in an individualistic and a collectivistic culture. *Management Science* 44, 9: 1263–1278.
37. Jodie B. Ullman 2006. Structural equation modeling: Reviewing the basics and moving forward. *Journal of Personality Assessment* 87, 1: 35-50.
38. Jessica Vitak, Pamela Wisniewski, Xinru Page, et al. 2015. The Future of Networked Privacy: Challenges and Opportunities. In *Proceedings of the 2015 ACM Conference Companion on Computer Supported Cooperative Work & Social Computing* (CSCW'15), 267–272.
39. Alan F. Westin. 1967. *Privacy and Freedom.* Atheneum, New York, NY.
40. Pamela Wisniewski, Bart P. Knijnenburg, and H. Richter Lipford. 2014. Profiling Facebook users' privacy behaviors. In *SOUPS2014 Workshop on Privacy Personas and Segmentation*. 1-6.
41. Pamela Wisniewski, Heather Lipford, and David Wilson. 2012. Fighting for my space: Coping mechanisms for SNS boundary regulation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI'12), 609–618.
42. Ralf De Wolf, Koen Willaert, and Jo Pierson. 2014. Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior* 35: 444–454.
43. Heng Xu. 2011. Reframing privacy 2.0 in online social network. *University of Pennsylvania Journal of Constitutional Law* 14: 1077-1102.
44. Heng Xu, Tamara Dinev, H. Jeff Smith, and Paul Hart. 2008. Examining the formation of individual's privacy concerns: Toward an integrative view. In *International Conference on Information Systems (ICIS) 2008 Proceedings*, 1-16.