Information Privacy Concern About Peer Disclosure in Online Social Networks

Jin Chen, Jerry Wenjie Ping, Yunjie (Calvin) Xu, and Bernard C. Y. Tan

***Abstract*—In online social networks, because one's private information can be co-owned and disclosed by peers, a new type of privacy concern, i.e., information privacy concern about peer disclosure (IPCPD), looms large. Should a member of an online social network be offered decision control to veto ex-ante the disclosure of his/her information by peers? There has been no theoretical research on the effectiveness of decisional control to alleviate such a privacy concern. Drawing on the communication privacy management perspective and the impression management theory, this study proposes a three-way interaction effect among three important antecedents of IPCPD: 1) decisional control; 2) image discrepancy (i.e., the degree to which the disclosed information portrays an unfavorable image of the disclosed person); and 3) social network overlap between the disclosed person and the discloser. Our experimental study reveals significant findings. When image discrepancy is low, decisional control is helpful only when the social network overlap between the disclosed one and the discloser is low. When image discrepancy is high, decisional control is helpful only when the social network overlap between the disclosed one and the discloser is high. This study contributes to a theory of privacy concern about peer disclosure in the context of online social networks.**

***Index Terms*—Decisional control, image discrepancy, information privacy concern, online social networks, peer disclosure, social network overlap.**

I. Introduction

With the large amount of information disclosure in online social networks, scholars have paid increasing attention to the dark side of information disclosure, e.g., divulgation of private information [1], [2]. Members of online social networks have generated large volumes of information about themselves (i.e., self-disclosure) as well as about others (i.e., peer disclosure) [3], [4]. Members express greater privacy concerns about peer disclosure than about self-disclosure because they do not always have control over peer disclosure [2], [5]. Peer disclosure, the disclosure of one's private information by peers in online social networks, can potentially raise severe privacy challenges [2]. Indeed, in online social networks, peers often possess intimate details of their friends and these details can be disseminated very quickly [2], [6]. For instance, it has been reported that unexpected disclosures by peers have jeopardized members' personal life, affected their promotion, or hurt the public image of a company [2], [7]. As a result, information privacy concern about peer disclosure looms large in online social networks.

Prior research on information privacy in the domains of information systems, sociology, psychology, and law, has mainly focused on how to alleviate consumers' privacy concern about the usage of their information by online firms in the context of e-commerce transactions [8]–[18]. Recently, researchers have started to examine members' privacy concern in the context of online social interactions, and have shown that members' privacy concern over self-disclosure negatively affects their intention to continue the use of a social networking website [19], [20]. While highlighting the importance of privacy concern, these studies have not addressed the issue of members' privacy concern due to peer disclosure. Some studies, despite acknowledging peers as a new source of privacy leakage, have restricted their focus to the adoption of privacy control techniques (e.g., [6]), yet have not explained when and why such techniques can alleviate members' privacy concern about peer disclosure (e.g., [3], [21]). So far, there has been no systematic research on the antecedents of privacy concern about peer disclosure, and, more importantly, when privacy control techniques would be more effective in alleviating such privacy concern in online social networks.

To address this critical gap in the literature, we examine prominent antecedents of privacy concern due to peer disclosure in online social networks and explore their interactive effects. We define information privacy concern about peer disclosure (IPCPD) as the extent to which a member of an online social network is concerned that his/her private information might be disclosed by peers in the online social network. Our research model is built on the perspective of communication privacy management [22] and the theory of impression management [23]. The perspective of communication privacy management sheds light on IPCPD by explaining why members desire control over the decision to disclose (or not) their private information coowned by peers [22]. It explains the effect of decisional control on IPCPD when people manage coowned private information. Complementing the communication privacy

Manuscript received September 29, 2013; revised August 8, 2014 and February 27, 2015; accepted May 3, 2015. Date of publication June 1, 2015; date of current version July 15, 2015. This work was supported by the National Natural Science Foundation of China under Grant 71302041, Grant 71172038, and Grant 71232008; by the Ministry of Education Project of Youth Fund of Humanities and Social Sciences under Grant 13YJC630008; by the Fundamental Research Funds for the Central Universities under Grant WN1323005; by the Shanghai Pujiang Program under Grant 13PJC021; and by the Program for Professor of Special Appointment (Eastern Scholar) at Shanghai Institutions of Higher Learning. Review of this manuscript was arranged by Department Editor T. Ravichandran. *(Corresponding author: Yunjie Xu.)*

J. Chen is with the School of Business, East China University of Science and Technology, Shanghai 200237, China (e-mail: jinchen@ecust.edu.cn).

J. W. Ping is with Standard Chartered Bank, Marina Bay Financial Centre, 018981 Singapore (e-mail: pingwenjie@gmail.com).

Y. Xu is with the Department of Information Management and Information Systems, School of Management, Fudan University, Shanghai 200433, China (e-mail: yunjiexu@fudan.edu.cn).

B. C. Y. Tan is with the Department of Information Systems, School of Computing, National University of Singapore, 117418 Singapore (e-mail: btan@comp.nus.edu.sg).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TEM.2015.2432117

0018-9391 © 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

management perspective, the impression management theory offers insights into contextual factors that could further explain how much members appreciate the value of decisional control over coowned private information [23]. It suggests that depending on different situations, members may consciously attempt to maintain their desired social image in the eyes of a certain audience [23]–[25]. Considering the "what" (i.e., what information is revealed) and the "whom" (i.e., to whom the information is revealed) aspects of the impression management theory [26]–[28], we focus on two such contextual factors: image discrepancy between one's desired image and the one portrayed by the disclosed information, and social network overlap between the disclosed one and the disclosing peer. The latter variable describes the relationship between the disclosed and the audience. Because the same information about a person may create different images in the eyes of distinct audience, the two aspects (i.e., "what" and "whom"), if isolated, could only represent an incomplete view of a privacy situation. As such, we expect the effect of decisional control on IPCP to be contingent upon the combination of image discrepancy and social network overlap. Therefore, this study posits a three-way interaction among decisional control, image discrepancy, and social network overlap. In doing so, this study offers a new theory of IPCPD that differs from traditional privacy research on self-disclosure in e-commerce contexts.

II. Theoretical Foundation

A. Communication Privacy Management

According to the communication privacy management perspective [22], [29], people often coown their private information with others (e.g., family members, friends) in social interactions. Unlike previous privacy research focusing on individuals managing their own privacy, the communication privacy management perspective suggests that besides the focal person, informed others are also critical to one's information privacy [22]. In this perspective, the disclosure of one's private information is composed of the decisions and actions of all coowners. As such, managing one's information privacy in social interactions is to construct a collective boundary around one's private information [22]. Ideally, this boundary would guide coowners in deciding who should have access to what information and the extent to which the information should be protected from those outside the boundary [30].

The collective boundary of one's information privacy could be defined based on privacy rules that are idiosyncratic and vary greatly from person to person [22]. Negotiating a set of rules among coowners is necessary for the management of the collective boundary [30]. If coowners do not establish or enact such common rules, or if any of them misuses such common rules, information privacy violation (e.g., inappropriate peer disclosure) happens [22]. Hence, with regard to coowned private information, control over the collective decision of disclosure is important to ward off potential vulnerability to information privacy violation [22].

Building upon this perspective, we investigate the issue of peer disclosure of coowned private information in online social networks. With the emergence of online social networks, people increasingly coown and comanage their private information in a public cyber space [6], [31]. Although common privacy rules are critical in such contexts, members seldom explicitly negotiate such rules. These rules are often tacit, a norm that everyone shall automatically know and observe. The lack of explicit rules is also due to high negotiation costs [30] because privacy is a "continually changing process which reflects a momentary ideal level of interpersonal contact" [32, p. 12]. The "momentary ideal level" of privacy varies for different situations. It is too costly for a person to specify all situations and negotiate *a priori* rules with coowners. Without common privacy rules, coowners are inclined to employ their personal rules even when handling another's private information [22]. As such, this often leads to privacy violations through peer disclosure in online social networks.

Given the fast speed and broad scope of information dissemination in online social networks, the optimal strategy is to exert control over peer disclosure [2], [4]. Previous research on self-disclosure has found that availability of control techniques alleviates information privacy concern [20]. Similarly, we posit that controls help alleviate IPCPD in online social networks. In particular, among various types of controls examined [33], decisional control is the most relevant when coowners could also be disclosure decision makers [22]. *Decisional control* is defined as the availability of technical options to stop the disclosure of private information which could potentially cause privacy violation [34], [35]. With the options provided, decisional control is akin to *a priori* negotiation of privacy rules among coowners of private information [6]. Enhanced decisional control can improve the comanagement of private information and alleviate IPCPD as it reduces the probability of inappropriate peer disclosure by giving the focal user an opportunity to make a discreet decision on a particular disclosure instance [22]. Hence, members of online social networks will have a lower level of IPCPD if they perceive a higher level of decisional control over peer disclosure.

B. Impression Management Theory

The impression management theory [23], [36] sheds light on the process whereby people attempt to manage the image others form about them [23]. In particular, one's desired image is how one wants to be perceived by audience [23], [37]. Conveying the right image to the right audience increases the likelihood that one would get desired interpersonal outcomes (e.g., be liked by others) and avoid undesired outcomes (e.g., be disliked by others) [23]. Recent studies on online self-disclosure suggest that the same process of impression management takes place in online settings as in offline settings [38]–[41]. Due to the affordances and constraints of computer-mediated communication, information disclosure is the essential tool to establish and maintain one's impression in online social networks [24], [25], [38]–[46]. For example, Scott [47] and Utz [48] found that Facebook members build profiles to form impressions and increase popularity. By means of self-disclosure, an individual controls "the information exchanged to ensure that what is desirable to her/his image (face supporting) is expressed and what

is damaging (face threatening) is kept private" [49, p. 118]. Despite the increasing research that applied this theory to explain online self-disclosure, little research has examined online peer disclosure [4], [50]. Nevertheless, the literature on offline peer disclosure suggests that losing decisional control over information pertaining to one's image due to peer disclosure is tantamount to a deprivation of control over one's image in front of the audience [37], [51]. Hence, it is reasonable to adopt the impression management theory in the context of this study.

Impression management theory suggests that although people regularly try to gauge the image others form of them, they do not always conduct impression management at a conscious level [52], [53]. It has identified three central forces that determine impression motivation: the goal relevance of impressions, the value of desired goals, and the discrepancy between desired and current image [23]. First, the goal relevance of impressions refers to how relevant the impressions people make are to the fulfilment of their goals [23], [54]. An individual would be more motivated to manage impressions if any of the three factors increases: publicity of one's behavior (i.e., the size of audience), one's dependence on the audience, and the contact one expects to have with the audience [23]. Second, the value of desired goals refers to the importance of people's desired goals [23], [54]. An individual's impression motivation would increase as a function of the availability of desired resources and the characteristics of the audience. For example, "people are more motivated to manage their impressions for people who are powerful, of high status, attractive, or liable than for those who are less so" [23, p. 39]. Third, the discrepancy between desired and current image also motivates people's impression management [23], [54]. People have a latitude of images that they would like to project. Only when they believed that the image others have of them falls outside this latitude, they would be prompted to conduct impression management [23].

The former two goal-related factors (i.e., goal relevance of impressions and value of desired goals) both revolve around the dimension of audience and suggest that individuals' goals and their impression motivation thereof vary to the audience. If they are more dependent on the audience for valued outcomes, their impression management efforts are likely to increase [55]. To complement this audience dimension, the third factor (i.e., discrepancy between desired and current image) speaks to the image itself. In summary, impression motivation is a function of both the audience and the image discrepancy.

Similarly, in online social networks, one's desire for effective controls to manage online impression may vary depending on the audience and the image discrepancy. For example, when making the "right" impression to a specific audience is a salient decision, such as when a person tries to make a first impression in front of new friends online so as to extend his/her social network or when the perceived image is out of the comfort latitude in front of existing friends, the person would expend more effort to manage the impression. In such cases, a deprivation of decisional control would escalate the person's privacy concern. In contrast, when the active impression management makes no difference, such as when what others think of a person does not matter much, or when the resultant image is within the comfort latitude, the person may be oblivious of the decisional control. By and large, the impression management theory implies that the relationship between decisional control and IPCPD depends on situational factors.

III. Model and Hypotheses

Drawing on the two guiding theories, this study examines the contingent effect of decisional control on IPCPD. In particular, we identify two contextual factors: image discrepancy and social network overlap. In this study, "the disclosed" refers to the person whose information is revealed, "the discloser" refers to the peer who discloses the information, and "the disclosee" refers to the audience who receives the information.

A. Effect of Decisional Control Contingent on "What" and "Whom"

Communication privacy management perspective [22] suggests a generally alleviating effect of decisional control on IPCPD. However, according to the impression management theory, this relationship may be contingent on contextual factors [23]. The privacy literature attests to this observation in suggesting that people prefer different control strategies for information privacy in accordance with the circumstance [32]. Thus, it is important to investigate the contextual factors that moderate the effect of decisional control on IPCPD.

Impression management theory further implies that the contextual factors have to do with two major aspects: the "what" (i.e., what information is disclosed) and the "whom" (i.e., to whom the information is disclosed) aspects of the situation [23]. The "whom" and "what" aspects of situations have also been mentioned, but not explicitly established in the privacy literature. For example, Parker [26] states that privacy concern results from losing control over "who" can see "what" parts of us. Laufer and Wolfer [28] argue that privacy involves control over access to the "what" aspect of a person with regard to the interpersonal situation (i.e., "whom"). Similarly, Westin [27] regards information privacy as the claim of individuals to determine "what" about them is to be communicated to "whom." Therefore, since its inception, the privacy literature has emphasized the importance of the nature of disclosed information (i.e., "what") and the disclosee (i.e., "whom"). However, the privacy literature has not articulated the key factors that pertain to the "what" and the "whom" aspects of situations. To address this research gap, we draw on the impression management theory to identify contextual factors and examine how these contextual factors moderate the effect of decisional control on IPCPD.

B. Image Discrepancy—The Aspect of "What"

Impression management theory suggests that image discrepancy between one's desired and current social image is a critical factor pertaining to the "what" aspect of a situation [23]. *Image discrepancy* is defined as the degree of inconsistency between the desired image one would like others to have of oneself and the actual image one believes others have [23], [37]. The prior literature further suggests that image discrepancy arises when "individuals proactively seek to move to a more desirable self-conceptualization" or "they are reacting to a loss in their status

that is due to transgressions" [54, p. 88]. While the first cause of image discrepancy (i.e., one's own ambition) is often seen in self-disclosure, the second cause—transgression, referring to an act that violates a shared moral or legal code [54], [56]—is more related to peer disclosure. Indeed, in online social networks, peer disclosure is a common case of transgression and a major cause of image discrepancy [2]. The disclosed might face a loss in social image due to peer disclosure. Prior research argues that when people think that others hold a less positive impression of them than they desire, as in the case of a loss in social image, they have a higher motivation to repair their image [23], [57]. In online social networks, when information that can cause a larger image discrepancy is divulged, the disclosed would also have a higher motivation to manage the impression.

C. Social Network Overlap—The Aspect of "Whom"

Impression management theory also implies that one's relationship with an audience speaks to the "whom" aspect of the situation, as reflected in the two impression motives—goal relevance of impressions and value of desired goals [23]. Prior studies on offline social interactions found that when a person was more dependent on others for valued outcomes, the person would be more motivated to engage in impression management [55]. In online social interactions, people also tend to be sensitive to the audience of the disclosure [58]. Their privacy concern can vary greatly from one audience to another [29]. However, unlike the case of self-disclosure where members roughly know who are connected with them and allowed to see the information, in the case of peer disclosure, they may not know who are in the network of the discloser and have access to the information [2], [6], [21]. In other words, they are not conscious of all potential audience and their relationships with the audience. A member resorts to the *social network overlap* between himself/herself and the discloser to gauge who would be the audience. Social network overlap is defined as the extent to which the disclosed and the discloser share common friends [59], [60]. When there is a high social network overlap, the disclosed would expect most of the audience to be also his/her friends who might be able to make sense or even take the advantage of the disclosed information. Otherwise, the audience would most likely be strangers.

D. Three-Way Interaction

Given the complexity of social interactions determined by both aspects (i.e., the "what" and the "whom"), this study examines a three-way interaction among decisional control, image discrepancy, and social network overlap.

1) Low Image Discrepancy: In low image discrepancy situations, the image being released through peer disclosure does not deviate greatly from one's desired image. Members of online social networks have a desire to maximize the size of their networks. Given no severe image damage, they are not concerned about the loss of existing friends. Instead, they would limit their attention to how to maximize the gain of new friends. Prior research suggests that finding and connecting with new friends has been the primary way of enlarging one's social network [61]. Members of online social networks are interested in making friends with valuable others not yet known to them, so as to "reap the rewards of establishing new relationships" [44, p. 226]. For this reason, the disclosed can maximize his/her social network through maximizing the gain of new friends, and would focus on strangers rather than existing friends.

With a high social network overlap, many disclosees who receive the information from the discloser are also friends of the disclosed. On the one hand, focusing on existing friends can hardly help to enlarge one's social network (i.e., no gain). On the other hand, as friends already have formed an image of the disclosed based on the earlier impression management efforts of the disclosed, the information would not change the image of the disclosed due to low discrepancy (i.e., no loss). Considering that there is no gain or loss, the disclosed would have a lower motivation to engage in impression management through decisional control [23]. Therefore, the impact of decisional control on IPCPD is likely to be weak.

In contrast, with a low social network overlap, many disclosees are strangers to the disclosed. Focusing on these strangers can help to maximize the gain of new friends. This is because these strangers, with connections to the discloser, are not "complete strangers" in a traditional sense, but "friends of a friend." They may share many similarities with the disclosed (e.g., from the same university) and, thus, are very likely to enter the friend circle of the disclosed in the future [2]. As suggested by the impression management theory, in front of strangers with whom they may have future interdependence, people usually desire to project a very positive image instead of a neutral one, because "you only get one chance to make a first impression" [62, p. 635]. However, as these strangers do not have a prior image of the disclosed, the revealed information would be used to form the first impression of the disclosed [52]. Even though the information may not deviate from one's normal image, the disclosed would be more selective in what to disclose in front of strangers in order to have a favourable first impression [23]. This is especially the case in online social networks where people have many latent interactions with strangers (e.g., names mentioned by common friends) [63] who may later become someone important to them [2]. Prior studies found that people even tend to misrepresent themselves in online social networks to attract strangers [43], [44]. Considering that focusing on these strangers can maximize the gain of new friends, the impact of decisional control on IPCPD is likely to be strong.

H1: When image discrepancy is low, there is an interaction effect between social network overlap and decisional control, such that:

H1a: when social network overlap is low, high decisional control results in lower IPCPD than does low decisional control;

H1b: when social network overlap is high, high decisional control does not result in lower IPCPD than does low decisional control.

2) High Image Discrepancy: In the situations of high image discrepancy, the information being disclosed by a peer deviates much from one's desired image. As there is severe image damage, people are largely concerned about the loss of existing friends with whom they have made a previous relational

investment and with whom they expect to have frequent future contact [37]. While they may be still concerned about not being able to get new friends, they would focus more on how to minimize the decrease in their existing social networks due to loss aversion. Prior research suggests that the effort put into managing friends can alleviate the loss of social networks and associated vested benefits [23], [64]. For this reason, the disclosed would try to minimize the loss of existing friends and would focus more on friends than on strangers.

With a high social network overlap, many disclosees who receive the information from the discloser are friends of the disclosed. Being friends, these disclosees not only have formed an image of the disclosed, but also have substantial interdependence with the disclosed [2]. If friends accepted the negative image of the disclosed, all the earlier efforts that the disclosed expended in impression management to get desired outcomes would be wasted. In contrast, focusing on friends and maintaining a good impression in front of them can help to minimize the loss of existing friends [23]. Considering the potential loss of existing friends, the disclosed would be highly motivated to engage in impression management through decisional control [23], so as to protect the desired image built up among friends over time. Hence, the impact of decisional control on IPCPD is likely to be strong.

In contrast, with a low social network overlap, many disclosees are strangers to the disclosed. On the one hand, focusing on strangers can hardly help to minimize the loss of existing friends (i.e., no gain). On the other hand, although the disclosed may also try to minimize the loss of potential new friends, he/she may not be able to find effective ways to revamp severe image damage in front of strangers due to the lack of connections with them. Under such circumstances, as the impression management theory suggests, the disclosed may feel "incapable of changing the perceptions others have of them . . . " [37, p. 693] (i.e., no ways to minimize loss). Thus, his/her impression management motivation would not be high [23], [37]. These arguments suggest that the effect of decisional control would be weaker in the case of high image discrepancy and low social network overlap.

H2: When image discrepancy is high, there is an interaction effect between social network overlap and decisional control, such that:

H2a: when social network overlap is low, high decisional control does not result in lower IPCPD than does low decisional control;

H2b: when social network overlap is high, high decisional control results in lower IPCPD than does low decisional control.

The hypotheses are summarized in Fig. 1. To control for other confounding factors, this study includes several control variables that may impact IPCPD, including privacy disposition [20], past privacy violation experience [15], and information sensitivity [8], [15], [65], [66].

IV. Methodology

This study employed a laboratory experiment. An experiment allows us to control extraneous variables so that causal relationships could be properly assessed [67]. While a field experiment is advantageous in establishing the generalizability and external validity of findings, a laboratory experiment is an appropriate choice for this study because a field experiment of peer disclosure in real online social networks raises many ethical concerns. A 2(decisional control: low versus high) $\times$ 2(image discrepancy: low versus high) $\times$ 2(social network overlap: low versus high) between subject factorial design was adopted.

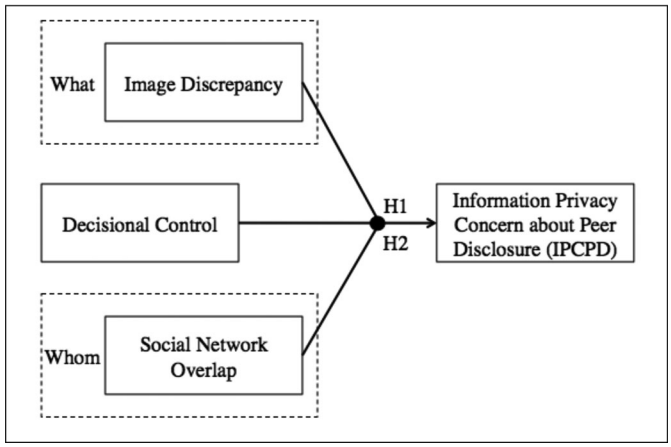

Fig. 1. Research model.

A. Vignettes

Like previous studies on information privacy (e.g., [68] and [69]), vignettes were used in the laboratory experiment. Vignettes are short scenarios in written or pictorial form to elicit perceptions, opinions, beliefs, and attitudes toward typical situations [70]. A focus group discussion with active participants of online social networks was conducted in order to design suitable scenarios. In these scenarios, a student subject assumed the role of the disclosed. Among two student association campaigns held concurrently, he/she attended and voted only for one (see Appendix B for details). Both association leaders were his/her friends. Nevertheless, a picture of his/her participation in one campaign was uploaded by a peer to a popular online social network. This peer disclosure led to privacy concerns for the disclosed.

B. Manipulations

Photo tagging, the act of using a user name as a tagging keyword to link a photo to the profile of a member [2], was chosen as the technical context to implement a decisional control because it is a prevalent activity in many social networking websites [71]. Second, the visibility of the picture [3], the identifiability of the tagged person [2], and the searchability of tags suggest that tagging is a good example of peer disclosure. Although a picture without tagging may also divulge private information, the effect of a picture with tagging will be much stronger due to the identifiability and searchability of tags, compared with pure image recognition. Third, tagging is an IT-enabled technique on which social networking websites can impose a decisional control in order to grant members tools for information privacy protection.

Decisional control was manipulated at two levels (i.e., low versus high). Several past studies have operationalized this variable as decisional choices available to people (e.g., [33], [34], [72], [73]). Under the condition of low decisional control in this study, subjects were told that their peers could freely tag their photo and link it to their profile without their consent. They could, at best, remove the tag linked to their profile after the photo had been posted. Under the condition of high decisional control, subjects were told that peers could tag their photo and link it to their profile only with their consent. Thus, they could choose to withhold their consent and not let the tagging happen. They were also able to remove the tag and link even after having given their consent. Compared to the condition of low decisional control, the condition of high decisional control gave subjects more decisional choices. The manipulation of decisional control was checked using three items (see Appendix A).

Image discrepancy was manipulated at two levels (i.e., low versus high) by varying the discrepancy between one's desired image and the one implied by the disclosed information. Under the condition of low image discrepancy, subjects were told that they did not care much about the friendship with the leader of the association that they did not attend and vote for. Instead, they cared about the relationship with the leader of the one that they attended and voted for. In contrast, under the condition of high image discrepancy, subjects were told that they cared very much about the relationships with both leaders, but had voted for only one. This situation was expected to cause a larger impact on the public image of the subjects (i.e., loyalty to friend). The manipulation of image discrepancy was checked using three items (see Appendix A).

Social network overlap was manipulated at two levels (i.e., low versus high). Prior research suggested two ways to operationalize it: absolute number of mutual friends and proportion of mutual friends [60], [74]. The latter can control for the size of friendship network which varies among people and was adopted in this study. A pilot study involving 34 active participants in online social networks showed that their proportion of mutual friends with peers ranged from slightly below 5% to slightly above 65%. Thus, under the condition of low social network overlap, subjects were told that 5% of their friends in the online social network were also friends of the discloser. Under the condition of high social network overlap, this figure was 65%. The manipulation of social network overlap was checked using three items (see Appendix A).

C. Procedure and Subjects

A pilot study involving 22 active participants of online social networks was conducted to obtain feedback to improve the design of our experimental process and instrument. They affirmed that the manipulations for decisional control, image discrepancy, and social network overlap make sense based on their own experience online. Moreover, as suggested by Perdue and Summer [75], a pretest using a separate subject pool is required to check all the manipulations before the main experiment. It helps to rule out the confounding effects of manipulation questions on the targeted dependent variables. Thus, a pretest involving 20 active participants was conducted for manipulation checks. The settings of the pretest, including experiment procedure, instrument, and subject types, were exactly the same as the main experiment. After making sure that all the manipulations checks were successful, we proceeded with the main experiment.

In the main experiment, a simulated Facebook website was created. Facebook was chosen because it is the most popular online social network with more than 890 million active participants globally [76]. Subjects were asked to play the role of the disclosed on the simulated Facebook website. Given that they might have prior knowledge about privacy settings on the actual Facebook website, subjects were explicitly told that the Facebook website used in this study had newly designed privacy settings that could be different from the actual one.

A total of 144 undergraduate students from a large university participated in the main experiment. Student subjects were used because active members of online social networks are often young people [21] who have a college affiliation [2]. The objective of the study was not revealed to subjects until they had finished the study. Subjects were randomly assigned to one of the eight scenarios. The experimental procedure had three parts. First, subjects completed a questionnaire on demographic variables and online social network experience. Second, subjects read their respective scenario in the context of the simulated Facebook website, and answered three content-related questions that served as comprehension checks to filter out nonserious ones (see Appendix A). Third, subjects evaluated their IPCPD and control variables. To motivate serious participation, a token payment was offered upon the completion of the main experiment.

D. Measurements

Wherever possible, tested items were adapted from past studies (see Appendix A). The manipulation check items measuring decisional control were taken from Hui and Bateson [77]; items for image discrepancy were developed based on Bolino [57] and Roberts [37]; and items for social network overlap were adapted from Sprecher [78]. The items measuring IPCPD were adapted from the instrument for privacy concern developed by Xu [68] and Xu *et al.* [20].

V. Data Analysis

The responses of 139 subjects who passed all comprehension checks were used for data analysis. They were registered members of Facebook. Table I reports their demographics. Nonparametric tests revealed no significant difference in demographic variables across the eight scenarios. All statistical analyses were carried out at the 5% level of statistical significance.

A. Manipulation Checks

Manipulation checks were conducted using the pretest data ($N = 20$). As the three measures for decision control were highly correlated with one another (Cronbach's alpha = 0.89), these measures were averaged to create one indicator of decisional control. A *t*-test showed that subjects in the low decisional control treatment perceived a lower decisional control than did subjects in the high decisional control treatment ($t = -2.240$,

TABLE I
SUBJECT DEMOGRAPHICS ($N = 139$)

Demographics				
Age (years)	Mean	20.98	Std. Dev.	2.03
Gender	Male	64.7%	Female	35.3%
Time spent on online social networks per week (hours)	Mean	9.50	Std. Dev.	11.67
Experience with online social networks (Likert scale 1 = none, 7 = Extensive)	Mean	5.04	Std. Dev.	1.21
Frequency of participation in online social networks	No more than once a month	0.7%	Once a fortnight	2.9%
			Once a week	3.6%
	Twice a week	10.1%	At least once a day	82.7%

TABLE II
DESCRIPTIVE STATISTICS FOR IPCPD[a]

	Low Image Discrepancy		High Image Discrepancy	
	Low Decisional Control	High Decisional Control	Low Decisional Control	High Decisional Control
Low Social Network Overlap	(5.765, 0.948) $N = 17$	(3.870, 1.861) $N = 18$	(4.941, 1.215) $N = 17$	(5.146,1.109) $N = 16$
High Social Network Overlap	(4.444, 1.126) $N = 18$	(4.167, 1.716) $N = 18$	(5.352, 1.006) $N = 18$	(4.392, 1.449) $N = 17$

[a] Mean and standard deviation in parentheses.

TABLE III
RESULTS OF ANCOVA FOR IPCPD (THE WHOLE SAMPLE, $N = 139$, $R^2 = 28.1\%$)

Variable	df	*F*	*p*	Power
Privacy Disposition	1	11.504	0.001**	0.92
Related Privacy Violation Experience	1	2.166	0.144	0.309
Information Sensitivity	1	48.488	0.000**	1.000
Image discrepancy (ID)	1	0.108	0.742	0.062
Social Network Overlap (SNO)	1	1.410	0.237	0.218
Decisional Control (DC)	1	10.063	0.002**	0.883
ID × SNO	1	0.012	0.911	0.051
ID × DC	1	2.738	0.100	0.376
SNO × DC	1	0.158	0.691	0.068
ID × SNO × DC	1	10.589	0.001**	0.898

$^{*}p < 0.05, ^{**}p < 0.01.$

TABLE IV
RESULTS OF ANCOVA FOR IPCPD (THE SUBSAMPLE OF LOW IMAGE DISCREPANCY TREATMENTS, $N = 71$, $R^2 = 58.1\%$)

Variable	df	*F*	*p*	Power
Privacy Disposition	1	15.719	0.000**	0.974
Related Privacy Violation Experience	1	1.055	0.308	0.173
Information Sensitivity	1	38.956	0.000**	1.000
Social Network Overlap (SNO)	1	0.288	0.593	0.083
Decisional Control (DC)	1	10.238	0.002**	0.883
SNO × DC	1	6.354	0.014*	0.699

$^{*}p < 0.05, ^{**}p < 0.01.$

$p < 0.05$). Items for image discrepancy also had a high reliability (Cronbach's alpha = 0.90) and were average for factor score. A *t*-test confirmed that subjects in the low image discrepancy treatment perceived a lower discrepancy of image compared to subjects in the high image discrepancy treatment ($t = -2.444$, $p < 0.05$). Similarly, items for social network overlap had a high reliability (Cronbach's alpha = 0.98). A *t*-test of factor score confirmed the success of manipulation ($t = -6.791$, $p < 0.001$).

B. Hypotheses Testing

With the main experiment data, IPCPD also demonstrated a high reliability (Cronbach's alpha = 0.885) [79]. Table II further provides descriptive statistics for IPCPD in each treatment.

The two hypotheses were tested using ANCOVA. The results showed a significant main effect for decisional control ($F = 10.063$, $p < 0.01$) and a significant three-way interaction involving the three independent variables ($F = 10.589$, $p < 0.01$) (see Table III). The interpretation of the three-way interaction should take precedence over that of the main effect [80].

To further explicate the three-way interaction, the dataset was split along image discrepancy. H1 was tested using the subsample of the low image discrepancy treatment. The results revealed a two-way interaction between social network overlap and decisional control ($F = 6.354$, $p < 0.05$) (see Table IV and Fig. 2). Under the condition of low social network overlap, the low decisional control treatment yielded a higher IPCPD than did the high decisional control treatment ($t = 3.824$, $p < 0.01$). In contrast, under the condition of high social network overlap, the low decisional control treatment did not yield a significantly higher IPCPD than did the high decisional control treatment ($t = 0.574$, $p = n.s$). Hence, H1 was supported.

H2 was tested using the subsample of the high image discrepancy treatments. The results revealed a two-way interaction between social network overlap and decisional control ($F = 4.295$, $p < 0.05$) (see Table V and Fig. 2). Under the condition of high social network overlap, the low decisional control treatment yielded a higher IPCPD than did the high decisional control treatment ($t = 2.287$, $p < 0.05$). In contrast, under the condition of low social network overlap, the low decisional control treatment did not yield a higher IPCPD than the high decisional control treatment ($t = -0.505$, $p = n.s.$). Therefore, H2 was also supported.

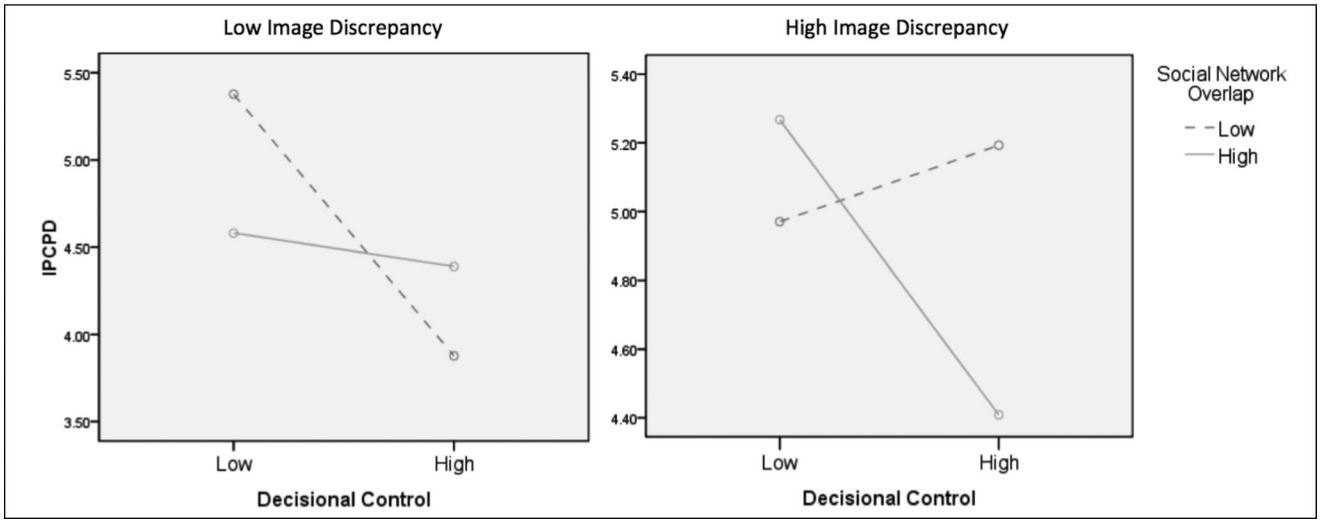

Fig. 2. Plotted three-way interaction based on results. Left panel: low image discrepancy treatments. Right panel: high image discrepancy treatments.

TABLE V
RESULTS OF ANCOVA FOR IPCPD (THE SUBSAMPLE OF HIGH IMAGE DISCREPANCY TREATMENTS, $N = 68$, $R^2 = 32.1\%$)

Variable	df	F	p	Power
Privacy Disposition	1	0.488	0.488	0.106
Related Privacy Violation Experience	1	1.400	0.241	0.214
Information Sensitivity	1	13.689	0.000**	0.954
Social Network Overlap (SNO)	1	0.858	0.358	0.149
Decisional Control (DC)	1	1.491	0.227	0.225
SNO × DC	1	4.295	0.042*	0.532

*$p < 0.05$, **$p < 0.01$.

VI. DISCUSSION AND IMPLICATIONS

An early conceptual development of this topic suggested that information privacy is a selective control [32]. People tend to choose different control strategies depending on their circumstances. Subsequent research examined control strategies people may choose in various contexts of commercial transactions (e.g., [68], [81]). This study extends this body of work to the context of online social networks. In particular, our results show that the effect of decisional control on IPCPD is contingent upon the combination of image discrepancy and social network overlap pertaining to the "what" and the "whom" aspects of a peer disclosure situation. Specifically, when the expected audience is mostly made up of friends, people tend to overlook decisional control if the image discrepancy is low. When the expected audience is mostly made up of strangers, they tend to overlook the value of decisional control when the image discrepancy is high. In contrast, people tend to value decisional control when there is a major image discrepancy in front of friends, or a minor image discrepancy in front of strangers.

A. Theoretical Contributions

This study makes valuable contributions to the information privacy literature. First, by developing a new concept—IPCPD in the emerging context of online social networks, it extends the theoretical body on information privacy into the new context of peer disclosure of coowned private information. Investigation in this context is particularly important given the prevalence and unique characteristics of online social networking [2]. Calls have been made to advance new theories on collective privacy management in online social networks [1], [12]. For example, Smith *et al.* suggested, "social networking websites such as Facebook and Twitter offer dynamic examples in which information boundaries are created in groups of various sizes and relationship levels... A set of studies that considers the factors associated with different boundaries regarding disclosure within and across online groups... could be of great interest in this domain" [12, p. 1007]. Xu and Bélanger [46, p. 372] also cautioned the contextual nature of privacy in social media "because of its change of agency (from the self to a group), its inclusion of interactional and interpersonal privacy decision making, and its collective domain where the user and her social ties share responsibilities for keeping their shared data safe and private." Our theorization of IPCPD in the context of online social networks heeds these calls and opens up fertile terrain for new research efforts in this direction.

Second, this study develops a new theory of IPCPD by proposing a contingency model that unravels the complex interaction effects among three antecedents of IPCPD: decisional control, image discrepancy, and social network overlap. The contingency model of IPCPD is based predominantly on the communication privacy management perspective [43], which highlights the role of decisional control in one's management of IPCPD with others in a social network. However, the prior literature has overlooked that in such contexts, information privacy is an interpersonal concept which "presupposes the existence of others and the possibility of a relationship with them" [28, p. 33]. Thus, it is imperative to simultaneously examine the "what" and the "whom" aspects of the situation where the impression management theory offers a suitable theoretical lens. In this light, this study theoretically articulates and empirically demonstrates that the effect of decisional control is contingent on the combination of specific "what" and "whom" aspects—the nature of

information disclosed (i.e., image discrepancy) and the interpersonal relationship with the audience (i.e., social network overlap). The results suggest that people tend to value decisional control when image discrepancy and social network overlap are both high or both low. This finding provides more nuanced understanding of the contingent effect of decisional control on information privacy concern in online social networks.

Third, besides the contribution to the literature on peer disclosure, this study also adds to the traditional literature on online self-disclosure by extending the notion of privacy goals [46]. Past studies on online self-disclosure have largely focused on privacy goals related to the protection against monetary losses (e.g., against the disclosure of credit card information) [1]. Our study extends privacy goals to the management of a better social impression for desired social outcomes (e.g., maximizing the size of social networks, or minimize the decrease in existing social networks). Future research on self-disclosure can further extend the scope of privacy goals and investigate other types of social benefits and losses in information privacy management.

B. Practical Implications

The results of this study offer useful guidelines for practice. Many online social networks do not provide members with decisional control. Hence, peers are often able to disclose coowned private information without the consent of coowners. This study suggests that members value decisional control, although the valuation may vary in specific contexts.

There are two main broad categories of online social networks: those helping participants maintain their personal relationships (e.g., Facebook) and those helping participants maintain their professional relationships (e.g., LinkedIn). In the former, it is quite common for participants to share many friends with peers, and have large volumes of personal information disclosed by peers. Thus, participants in this type of online social networks tend to pay close attention to peer disclosure. Based on the results of this study, these participants are also likely to appreciate decisional control in high image discrepancy situations. However, this does not imply that decisional control is not useful in low image discrepancy contexts because participants make new friends in such networks. Attesting to our findings, Facebook recently provided decisional control to members by requiring their consent before peers could tag anything to their profiles.

In professional online social networks, it is quite common that peers may have many professional friends unknown to the disclosed. Members of such networks tend to pay close attention to peer disclosure even with low image discrepancy because a small failure of impression management may result in an unaffordable loss in professional networks [2]. Based on the results of this study, these participants are also likely to appreciate having a decisional control. In a situation where information of high image discrepancy is disclosed to strangers, the decisional control seems to have a low impact to alleviate privacy concern. Decisional control, however, should not be interpreted as of low value in this context. Platform providers should instead remind participants that there is a "second defense" of decisional control in their hands, which they can use to further manage their image in front of strangers.

In short, the results of this study cover the majority of scenarios confronting members of online social networks. The results suggest that it is worthwhile for operators of online social networks to find out the scenarios in which participants are particularly sensitive to privacy risks, and design effective decisional controls accordingly.

C. Limitations and Future Research

Our results have to be interpreted with due consideration to the limitations of this study. First, this study included only one attribute for the "what" and the "whom" aspects of information privacy. Future research can extend our study by proposing and testing other attributes. For example, Another attribute of the "what" aspect could be the information volume because people are concerned about the amount of information disclosed [15]. However, another attribute of the "whom" aspect could be the intimacy level between the disclosed and the disclosee [82] because close friends and acquaintances may have different rights of entry into one's personal space [83].

Second, this study used laboratory experiments where scenarios were presented to subjects in the form of vignettes. Although care has been taken to design the vignettes, these hypothetical situations are a simplification of real-life situations. While post hoc interviews with subjects revealed that they found the scenarios realistic, with appropriate attention to ethical issues, future studies can verify the results of this study using quasi-experiments involving real-life scenarios.

Third, in this study, the manipulation of decisional control is built upon photo tagging of online social network websites. As more and more privacy protection functionalities will become available in online social networks, there will be more decisional controls at user's disposal. For example, Facebook has changed its policy to allow members to remove themselves from search results [84]. Such decisional control allows members to adjust the extent to which their information can be searched by friends and strangers. Other ways of operationalization of decisional control would help to increase the experimental convergent validity of this construct.

VII. Conclusion

Global membership in online social networks will continue to grow steadily in the years ahead. The volume of coowned private information that could potentially leak through peer disclosure is likely to increase significantly in the years ahead. Given that the disclosure of such information might have severe consequences for members, scholars and practitioners need to continue searching for effective ways for people to protect their coowned information. Just as it is meaningful to conduct information privacy research in commercial situations where "I talk about myself," it is now equally meaningful to conduct information privacy research involving online social networks where "others talk about me."

To this end, this study draws on the tenets of the communication privacy management perspective and the impression

Dependent Variable	Item Description	Source
IPCPD	(7-point Likert scale, 1 = strongly disagree, 7 = strongly agree) IPCPD1: It bothers me when Wynne* discloses my personal information on this website. IPCPD2: I am concerned that on this website, Wynne can disclose too much of my personal information. IPCPD3: I am concerned that this website may not take measures to prevent Wynne's disclosure of my personal information.	Adapted from [20, 68]
Manipulation Check	**Item Description**	**Source**
Decisional Control (DC)	(7-point Likert scale, 1 = strongly disagree, 7 = strongly agree) DC1: I have much choice in stopping Wynne's disclosure of my personal information on this website. DC2: I have adequate opportunity in preventing Wynne from disclosing my personal information on this website. DC3: I have sufficient options to keep Wynne back from disclosing my personal information on this website.	Adapted from [77]
Image Discrepancy (ID)	(7-point Likert scale, 1 = strongly disagree, 7 = strongly agree) ID1: The information about me disclosed by Wynne would establish an image of me that deviates a lot from what I desire. ID2: I do not want people to perceive me as the kind of person indicated by the information disclosed by Wynne. ID3: I want to build up an image of me that is different from what Wynne disclosed.	Self-developed based on [37, 57]
Social Network Overlap (SNO)	(7-point Likert scale, 1 = strongly disagree, 7 = strongly agree) SNO1: On this website, the overlap between my friends and Wynne's friends is high. SNO2: On this website, a lot of my friends are also Wynne's friends. SNO3: On this website, my network of friends overlaps largely with Wynne's.	Adapted from [78]
Comprehension Check	**Item Description**	**Source**
Decisional Control	Which of the following sentences is TRUE according to your scenario? (Multiple choice question.) (a) On this website, if I tag a photo to a friend, the tag will be immediately shown. (b) On this website, if I tag a photo to a friend, the tag will not be shown until this friend approves the tag.	Self-developed
Image Discrepancy	Which of the following sentences is TRUE according to your scenario? (Multiple choice question.) (a) I do not cherish my friendship with Taylor**. (b) I cherish my friendship with Taylor very much.	Self-developed
Social Network Overlap	On this website, what is the percentage of your friends who are also Wynne' friends? (Multiple choice question.) (a) 5%; (b) 65%.	Self-developed
Control Variables	**Item Description**	**Source**
Privacy Disposition	Please select your privacy setting for your mostly used social networking site. (Multiple choice question.) (a) I do not know how to customize my privacy settings. (b) I know how to customize my privacy settings, but I leave my information available to everyone (i.e., friends and strangers). (c) I customize my privacy settings such that all my information is only available to my friends. (d) I customize my privacy settings such that some of my sensitive information is only available to specific friends.	Self-developed
Related Privacy Violation Experience	How many times did your feel uncomfortable when your friends shared information about you? ___ time(s) (Can be 0 if none).	Adapted from [15]
Information Sensitivity	(7-point Likert scale, 1 = strongly disagree, 7 = strongly agree) My information disclosed by Wynne is very sensitive to me.	Adapted from [15]

* Wynne is the name of the discloser in the scenarios. **Taylor is the name of one possible disclosee in the scenarios.

management theory, and proposes a contingency model to explain the effectiveness of decisional control. We found that decisional control is particularly important to alleviate privacy concerns of peer disclosure when the image discrepancy implied by the disclosed information and the social network overlap between the disclosed and discloser are both high or both low. Our findings suggest that decisional control is generally an important privacy protection tool in online social networks. Moreover, our findings reveal that the importance of decisional control stems from different contextual situations specified by the "what" and the "whom" aspects of information privacy.

APPENDIX A
MEASUREMENT ITEMS

See Appendix table top of the page.

APPENDIX B
ILLUSTRATIONS OF SCENARIOS

Subjects were shown a newly designed Facebook website with their respective scenarios. Manipulations are shown below with screenshots of the website.

Introduction (Same for all Treatments)

You will now be presented with a scenario. When you read the scenario, imagine that you are the character in the scenario. In the scenario, we have designed a new privacy setting for Facebook, which is different from the current privacy setting on Facebook. Imagine that you are using Facebook with this new privacy setting.

Decisional Control Description (Treatment Difference are Bolded and Underlined)

Low Decisional Control

On this newly designed Facebook, tagging is a function that lets you put tags on a piece of information to annotate who is involved in that information. For example, if a friend of yours Wynne tags you in a photo on Facebook, **the tag will be immediately shown in that photo. Your name will also be shown with the tag. Wynne's friends will be instantly notified on their Facebook pages that Wynne has tagged you in the photo. At the same time, you will be notified that Wynne has tagged you in a photo**.

If you do not like the tag, you can choose to **remove the tag. After the removal**, the tag will not be shown in the photo

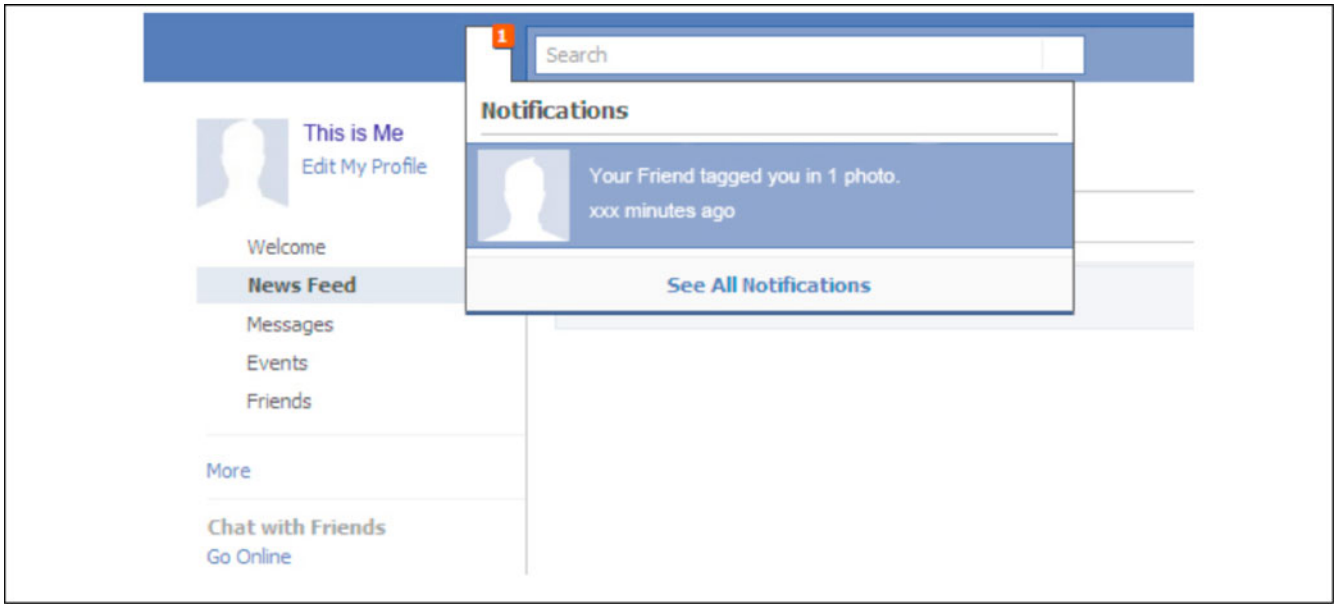

Fig. B1. Snapshot of notification for the low decisional control level.

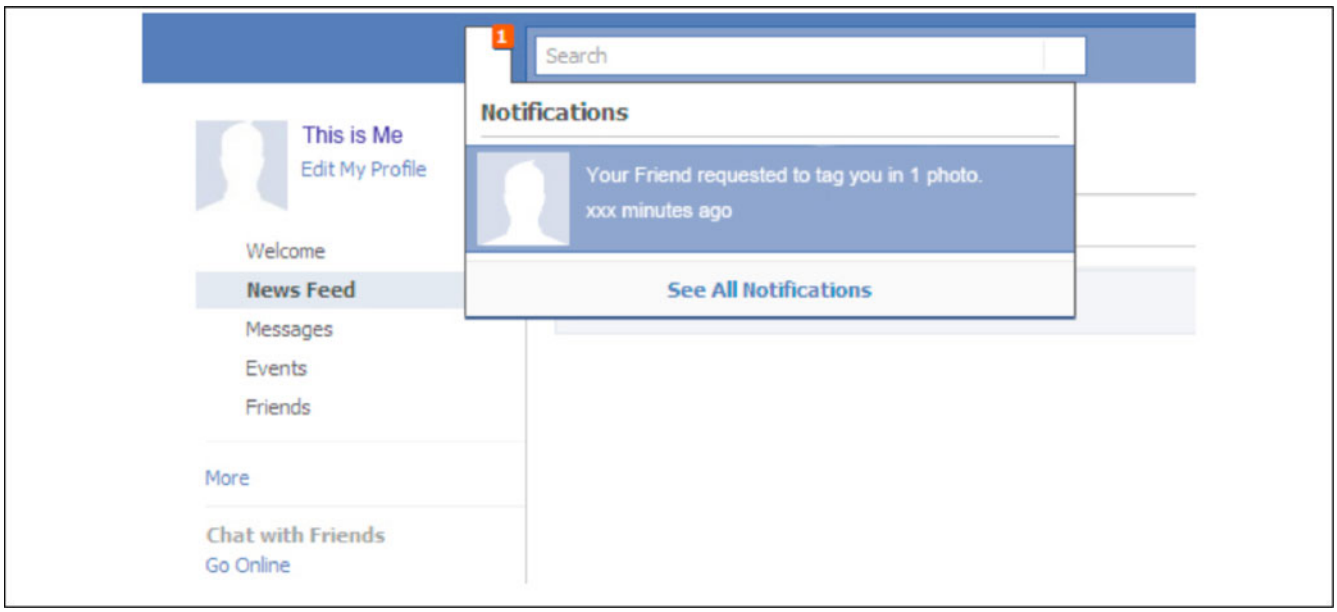

Fig. B2. Snapshot of notification for the high decisional control level.

anymore. None of Wynne's friends on Facebook will see the tag anymore. Your name will no longer be shown together with the tag either.

If you are comfortable with the tag, **you do not have to do anything. In this case, all Wynne's friends on Facebook will continue to see the tag in the photo and your name together with the tag.**

High Decisional Control

On this newly designed Facebook, tagging is a function that lets you put tags on a piece of information to annotate who is involved in that information. For example, if a friend of yours Wynne tags you in a photo on Facebook, **the system will send out a request for you to approve Wynne's tagging. Before your approval, the tag will NOT be shown in that photo. Your name will NOT be shown with the tag either. Wynne's friends will NOT be notified on their Facebook pages that Wynne tags you in the photo. Only you will be notified that Wynne has requested to tag you in a photo.**

If you do not like the tag, you can choose to **disapprove the tag. After the disapproval**, the tag will not be shown in the photo. None of Wynne's friends on Facebook will see the tag. Your name will not be shown together with the tag either.

If you are comfortable with the tag, **you can choose to approve the tag. After the approval, Wynne's friends will be instantly notified on their Facebook pages that Wynne**

has tagged you in the photo. They will see the tag in the photo and your name together with the tag.

Social Network Overlap Description (Low Social Network Overlap is 5%; High Social Network Overlap is 65%)

Wynne is one of your friends in real life. Consequently you and Wynne became friends on Facebook. [5% or 65%] of your friends on Facebook are also Wynne's friends on Facebook. That means, if you have 100 friends on Facebook, [5 or 65] friends of yours are also Wynne' friends on Facebook. These [5% or 65%] of your friends are called mutual friends of yours and Wynne's. All these mutual friends will be notified about the interaction between you and Wynne (e.g., they will be notified on their Facebook pages if Wynne tagged you in a photo).

Image Discrepancy Description (Treatment Difference are Bolded and Underlined)

Low Image Discrepancy

You joined two student sports associations at your university. Wynne was the leader of one association, while Taylor was the leader of another association. **You cherished your good friendship with Wynne. However, you did NOT care about your friendship with Taylor.**

Due to the economic crisis, your university wanted to cut budgets for all student associations. Associations of a same category (e.g., sports) had to demonstrate their excellence and compete on financial support from the university. Wynne's association and Taylor's association planned to hold their separate campaigns on one Saturday night. They both asked you to come for voting.

You would like to vote for both. However, according to the university rules, you could only vote for one association in a category. **Since you cherished your friendship with Wynne much more than that with Taylor,** you went to vote for Wynne's association. You did not tell this to Taylor or your friends in Taylor's association.

High Image Discrepancy

You joined two student sports associations at your university. Wynne was the leader of one association, while Taylor was the leader of another association. **You cherished your good friendships with both Wynne and Taylor.**

Due to the economic crisis, your university wanted to cut budgets for all student associations. Associations of a same category (e.g., sports) had to demonstrate their excellence and compete on financial support from the university. Wynne's association and Taylor's association planned to hold their separate campaigns on one Saturday night. They both asked you to come for voting.

You would like to vote for both. However, according to the university rules, you could only vote for one association in a category. **Although you cherished your good friendships with both Wynne and Taylor very much**, you went to vote for Wynne's association. You did not tell this to Taylor or your friends in Taylor's association.

Ending (treatment difference are bolded and underlined)

Under The Treatment of Low Decisional Control

The next day, you logged on to your Facebook account. You saw that Wynne had updated his status. Wynne wrote, "A big thank you to you all for voting for us!" Wynne uploaded photos of that night. **Wynne tagged you in one photo**. The photo showed that you were voting for Wynne's association. **The tag was shown** in the photo together with your name. **All Wynne's friends were notified of Wynne's tagging to you.**

Under The Treatment of High Decisional Control

The next day, you logged on to your Facebook account. You saw that Wynne had updated his status. Wynne wrote, "A big thank you to you all for voting for us!" Wynne uploaded photos of that night. **Wynne requested to tag you in one photo**. The photo showed that you were voting for Wynne's association. **The tag would be shown** in the photo together with your name **if being approved by you**. **You were notified of Wynne's request to tag you.**

REFERENCES

[1] F. Bélanger and R. E. Crossler, "Privacy in the digital age: A review of information privacy research in information systems," *MIS Qyart.*, vol. 35, pp. 1017–1041, 2011.

[2] D. Rosenblum, "What anyone can know: The privacy risks of social networking sites," *IEEE Security Privacy*, vol. 5, no. 3, pp. 40–49, May/Jun. 2007.

[3] J. Grimmelmann. (2008). *Facebook and the Social Dynamics of Privacy*. [Online]. Available: http://works.bepress.com/cgi/viewcontent.cgi?article = 1019&context = james_grimmelmann

[4] A. Lampinen, V. Lehtinen, A. Lehmuskallio, and S. Tamminen, "We're in it together: Interpersonal management of disclosure in social network services," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, Vancouver, BC, Canada, 2011, pp. 3217–3226.

[5] YouGov. (2007). What does your netrep say about you? [Online]. Available: http://www.rp-net.com/online/filelink/386/ETUDE% 20VIADEO_NetRep_2007.pdf

[6] A. C. Squicciarini, H. Xu, and X. Zhang, "Cope: Enabling collaborative privacy management in online social networks," *J. Am. Soc. Inf. Sci. Technol.*, vol. 62, pp. 521–534, 2011.

[7] H. Jones and J. H. Soltren. (2005). *Facebook: Threats to Privacy*. [Online]. Available: http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf

[8] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Inform. Syst. Res.*, vol. 15, pp. 336–355, Dec. 2004.

[9] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," *Inform. Syst. Res.*, vol. 17, pp. 61–80, 2006.

[10] J. B. Earp, A. I. Anton, L. Aiman-Smith, and W. H. Stufflebeam, "Examining internet privacy policies within the context of user privacy values," *IEEE Trans. Eng. Manage.*, vol. 52, no. 2, pp. 227–237, May 2005.

[11] M. W. Vail, J. B. Earp, and A. I. Anton, "An empirical study of consumer perceptions and comprehension of web site privacy policies," *IEEE Trans. Eng. Manage.*, vol. 55, no. 3, pp. 442–454, Aug. 2008.

[12] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: An interdisciplinary review," *MIS Quart.*, vol. 35, pp. 989–1015, 2011.

[13] P. B. Lowry, J. Cao, and A. Everard, "Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures," *J. Manage. Inf. Syst.*, vol. 27, pp. 163–200, 2011.

[14] N. F. Awad and M. S. Krishnan, "The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization," *MIS Quart.*, vol. 30, pp. 13–28, Mar. 2006.

[15] K.-L. Hui, H. H. Teo, and S.-Y. T. Lee, "The value of privacy assurance: An exploratory field experiment," *MIS Quart.*, vol. 31, pp. 19–33, 2007.

[16] C. V. Slyke, J. T. Shim, R. Johnson, and J. Jiang, "Concern for information privacy and online consumer purchasing," *J Assoc. Inf. Syst.*, vol. 7, pp. 415–444, Jun. 2006.

[17] P. A. Pavlou, H. Liang, and Y. Xue, "Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective," *MIS Quart.*, vol. 31, pp. 105–136, 2007.

[18] B. Mai, N. M. Menon, and S. Sarkar, "No free lunch: Price premium for privacy seal–bearing vendors," *J. Manage. Inf. Syst.*, vol. 27, pp. 189–212, 2010.

[19] N. K. Lankton, D. H. McKnight, and J. B. Thatcher, "The moderating effects of privacy restrictiveness and experience on trusting beliefs and habit: An empirical test of intention to continue using a social networking website," *IEEE Trans. Eng. Manage.*, vol. 59, no. 4, pp. 654–665, Oct. 2012.

[20] H. Xu, T. Dinev, H. J. Smith, and P. Hart, "Examining the formation of individual's privacy concerns: Toward an integrative view," in *Proc. 29th Int. Conf. Inform. Syst.*, Paris, France, 2008, pp. 1–16.

[21] D. Boyd, "Why youth love social network sites: The role of networked publics in teenage social life," in *Youth, Identity, and Digital Media*, D. Buckingham, Ed. Cambridge, MA, USA: MIT Press, 2008, pp. 119–142.

[22] S. Petronio, *Boundaries of Privacy: Dialectics of Disclosure*. Albany, NY, USA: State Univ. Press, 2002.

[23] M. R. Leary and R. M. Kowalski, "Impression management: A literature review and two-component model," *Psychol. Bull.*, vol. 107, pp. 34–47, 1990.

[24] D. Boyd and N. Ellison, "Social network sites, definition, history and scholarship," *J. Comput.-Mediated Commun.*, vol. 13, pp. 210–230, 2007.

[25] A. N. Joinson, "Looking at, looking up or keeping up with people?: Motives and use of Facebook," in *Proc. 26th Annu. SIGCHI Conf. Human Factors Comput. Syst.*, Florence, Italy, 2008, pp. 1–10.

[26] R. B. Parker, "A definition of privacy," *Rutgers Law Rev.*, vol. 27, pp. 275–296, 1974.

[27] A. F. Westin, *Privacy and Freedom*. Boston, MA: USA: Atheneum Press, 1967.

[28] R. S. Laufer and M. Wolfe, "Privacy as a concept and a social issue: A multidimensional development theory," *J. Social Issues*, vol. 33, pp. 22–42, 1977.

[29] I. Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Monterey, CA, USA: Brooks/Cole, 1975.

[30] S. Petronio, J. Sargent, L. Andea, P. Reganis, and D. Cichocki, "Family and friends as healthcare advocates: Dilemmas of confidentiality and privacy," *J. Social Pers. Relationships*, vol. 21, pp. 33–52, 2004.

[31] S. T. Margulis, "On the status and contribution of Westin's and Altman's theories of privacy," *J. Social Issues*, vol. 59, pp. 411–429, 2003.

[32] I. Altman, "Privacy: A conceptual analysis," *Environ. Behav.*, vol. 8, pp. 7–29, 1976.

[33] E. A. Skinner, "A guide to constructs of control," *J. Pers. Social Psychol.*, vol. 71, pp. 549–570, 1996.

[34] J. R. Averill, "Personal control over aversive stimuli and its relationship to stress," *Psychol. Bull.*, vol. 80, pp. 286–303, 1973.

[35] S. T. Fiske and S. E. Taylor, *Social Cognition*. New York, NY, USA: McGraw-Hill, 1991.

[36] E. Goffman, *The Presentation of Self in Everyday Life*. New York, NY, USA: Doubleday, 1959.

[37] L. M. Roberts, "Changing faces: Professional image construction in diverse organizational settings," *Acad. Manage. Rev.*, vol. 30, pp. 685–711, 2005.

[38] N. Ellison, R. Heino, and J. Gibbs, "Managing impressions online: Self-presentation processes in the online dating environment," *J. Comput.-Mediated Commun.*, vol. 11, pp. 415–441, 2006.

[39] C. Lampe, N. Ellison, and C. Steinfield, "A familiar face(book): Profile elements as signals in an online social network," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, San Jose, CA, USA, 2007, pp. 435–444.

[40] S. T. Tong, V. D. Heide, L. Langwell, and J. B. Walther, "Too much of a good thing? The relationship between number of friends and interpersonal impressions on Facebook," *J. Comput.-Mediated Commun.*, vol. 13, pp. 531–549, 2008.

[41] J. Rosenberg and N. Egbert, "Online impression management: Personality traits and concerns for secondary goals as predictors of self-presentation tactics on Facebook," *J. Comput.-Mediated Commun.*, vol. 17, pp. 1–18, 2011.

[42] J. T. Hancock and P. J. Dunham, "Impression formation in computer-mediated communication revisited: An analysis of the breadth and intensity of impressions," *Commun. Res.*, vol. 28, pp. 325–347, 2001.

[43] Z. J. Jiang, C. S. Heng, and B. C. F. Choi, "Privacy concerns and privacy-protective behavior in synchronous online social interactions," *Inform. Syst. Res.*, vol. 24, pp. 579–595, 2013.

[44] A. Chester and D. Bretherton, "Impression management and identity online," in *The Oxford Handbook of Internet Psychology*, A. N. Joinson, K. Y. A. McKenna, T. Postmes, and U. Reips, Eds. Oxford, U.K.: Oxford Univ. Press, 2007, pp. 223–236.

[45] N. C. Krämer and S. Winter, "Impression management 2.0: The relationship of self-esteem, extraversion, self-efficacy, and self-presentation within social networking sites," *J. Media Psychol.: Theories, Methods, Appl.*, vol. 20, pp. 106–116, 2008.

[46] H. Xu and F. Bélanger, "Information systems journal special issue on: Reframing privacy in a networked world," *Inform. Syst. J.*, vol. 23, pp. 371–375, 2013.

[47] G. G. Scott, "More than friends: Popularity on Facebook and its role in impression formation," *J. Comput.-Mediated Commun.*, vol. 19, pp. 358–372, 2014.

[48] S. Utz, "Show me your friends and I will tell you what type of person you are: How one's profile, number of friends, and type of friends influence impression formation on social network sites," *J. Comput.-Mediated Commun.*, vol. 15, pp. 314–335, 2010.

[49] J. C. Feaster, "Expanding the impression management model of communication channels: An information control scale," *J. Comput.-Mediated Commun.*, vol. 16, pp. 115–138, 2010.

[50] J. Chen, W. Ping, Y. Xu, and B. C. Y. Tan, "Am I afraid of my peers? Understanding the antecedents of information privacy concerns in the online social context," presented at the 30th International Conference on Information Systems (ICIS), Phoenix, AZ, USA, 2009.

[51] H. C. Kelman, "Privacy and research with human beings," *J. Social Issues*, vol. 33, pp. 169–195, 1977.

[52] A. H. Buss, *Self-Consciousness and Social Anxiety*. San Francisco, CA, USA: Freeman, 1980.

[53] E. Diener, "Deindividuation, self-awareness, and disinhibition," *J. Pers. Social Psychol.*, vol. 37, pp. 1160–1171, 1979.

[54] M. C. Blino, "Citizenship and impression management: Good soldiers or good actors?," *Acad. Manage. J.*, vol. 24, pp. 82–98, 1999.

[55] M. Hendricks and P. Brickman, "Effects of status and knowledgeability of audience on self-presentation," *Sociometry*, vol. 37, pp. 440–449, 1974.

[56] J. T. Tedeschi and C. A. Riordan, "Impression management and prosocial behavior following transgression," in *Impression Management Theory and Social Psychological Research*, J. T. Tedeschi, Ed. New York, NY, USA: Academic, 1981, pp. 223–244.

[57] M. C. Bolino, "Citizenship and impression management: Good soldiers or good actors?" *Acad. Manage. Rev.*, vol. 24, pp. 82–98, 1999.

[58] N. L. Collins and L. C. Miller, "Self-disclosure and liking: A meta-analytic review," *Psychol. Bull.*, vol. 116, pp. 457–475, 1994.

[59] S. Sprecher and D. Felmlee, "The influence of parents and friends on the quality and stability of romantic relationships: A three-wave longitudinal investigation," *J. Marriage Family*, vol. 54, pp. 888–900, 1992.

[60] R. M. Milardo, "Friendship networks in developing relationships: Converging and diverging social environments," *Social Psychol. Quart.*, vol. 45, pp. 162–172, 1982.

[61] K.-Y. Lin and H.-P. Lu, "Why people use social networking sites: An empirical study integrating network externalities and motivation theory," *Comput. Human Behav.*, vol. 27, pp. 1152–1161, 2011.

[62] K. D. Vohs, R. F. Baumeister, and N. J. Ciarocco, "Self-regulation and self-presentation: Regulatory resource depletion impairs impression management and effortful self-presentation depletes regulatory resources," *J. Pers. Social Psychol.*, vol. 88, pp. 632–657, 2005.

[63] J. Jiang, C. Wilson, X. Wang, P. Huang, W. Sha, Y. Dai, and B. Y. Zhao, "Understanding latent interactions in online social networks," in *Proc. ACM SIGCOMM Internet Meas. Conf.*, Melbourne, Australia, 2010, pp. 369–382.

[64] B. Major, W. Quinton, S. McCoy, and T. Schmader, "Reducing prejudice: The target's perspective," in *Reducing Prejudice and Discrimination*, S. Oskamp, Ed. Mahwah, NJ, USA: Lawrence Erlbaum Assoc., 2000, pp. 211–237.

[65] K. B. Sheehan and M. G. Hoy, "Dimensions of privacy concern among online consumers," *J. Public Policy Marketing*, vol. 19, pp. 62–73, 2000.

[66] J. Phelps, G. J. Nowak, and E. Ferrell, "Privacy concerns and consumer willingness to provide personal information," *J. Public Policy Marketing*, vol. 19, pp. 27–41, 2000.

[67] W. L. Neuman, *Social research Methods: Qualitative and Quantitative Approaches*, 6th ed., Englewood Cliffs, NJ, USA: Pearson, 2006.

[68] H. Xu, "The effects of self-construal and perceived control on privacy concerns," presented at the 28th Int. Conf. Inform. Syst., Montreal, QC, Canada, 2007.

[69] H. Sheng, F. F.-H. Nah, and K. Siau, "An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns," *J. Assoc. Inf. Syst.*, vol. 9, pp. 344–376, 2008.

[70] J. Finch, "The vignette technique in survey research," *Sociology*, vol. 21, pp. 105–114, 1987.

[71] TopTenREVIEWS. (2009). *Social Networking Websites Review Product Comparisons*. [Online]. Available: http://social-networking-websites-review.toptenreviews.com/
[72] N. Corah and J. Boffa, "Perceived control, self-observation, and response to aversive stimulation," *J. Pers. Social Psychol.*, vol. 16, pp. 1–4, 1970.
[73] P. Lewis and E. B. Blanchard, "Perception of choice and locus of control," *Psychol. Rep.*, vol. 28, pp. 67–70, 1971.
[74] C. R. Agnew, T. J. Loving, and S. M. Drigotas, "Substituting the forest for the trees: Social networks and the prediction of romantic relationship state and fate," *J. Pers. Social Psychol.*, vol. 81, pp. 1042–1057, 2001.
[75] B. C. Perdue and J. O. Summers, "Checking the success of manipulations in marketing experiments," *J. Marketing Res.*, vol. 23, pp. 317–326, 1986.
[76] Facebook. (2014). *Statistics*. [Online]. Available: https://newsroom.fb.com/company-info/
[77] M. K. Hui and J. E. G. Bateson, "Perceived control and the effects of crowding and consumer choice on the service experience," *J. Consumer Res.*, vol. 18, pp. 174–184, 1991.
[78] S. Sprecher and D. Felmlee, "Romantic partners' perceptions of social network attributes with the passage of time and relationship transitions," *Pers. Relationships*, vol. 7, pp. 325–340, 2000.
[79] J. Nunnally and I. Bernstein, *Psychometric Theory*. New York, NY, USA: McGraw-Hill, 1994.
[80] G. Keppel, *Design and Analysis: A Researcher's Handbook*. Eaglewood Cliffs, NJ, USA: Prentice-Hall, 1991.
[81] H. Xu and H. H. Teo, "Alleviating consumers' privacy concerns in location-based services: A psychological control perspective," in *Proc. 25th Int. Conf. Inform. Syst.*, Washington, DC, USA, 2004, pp. 793–806.
[82] D. J. Solove, *Understanding Privacy*. Cambridge, MA, USA: Harvard Univ. Press, 2008.
[83] I. Altman and D. A. Taylor, *Social Penetration: The Development of Interpersonal Relationships*. London, U.K.: Holt, Rinehart and Winston, 1973.
[84] J. Devitt. (2015). *Facebook Changing Privacy Settings in 2015*. [Online]. Available: http://www.indiesunlimited.com/2014/12/01/facebook-changing-privacy-settings-in-2015/

Jin Chen received the Ph.D. degree from the National University of Singapore, Singapore, in 2012.

She is currently an Assistant Professor in the Department of Management Science and Engineering, School of Business, East China University of Science and Technology, Shanghai, China. She has published her research work in international journals, such as *Information & Management*, the *European Journal of Information Systems*, the *International Journal of Electronic Commerce*, and *Electronic Markets*. Her works have also appeared at many intentional conferences, such as the International Conference on Information Systems, the European Conference on Information Systems, the Pacific Asia Conference on Information Systems, the Human-Computer Interaction International Conference, and the International Association for Chinese Management Research. Her research interests include information technology innovation and entrepreneurship in emerging markets, the impact of innovative information technologies, and information privacy in online social networks.

Jerry Wenjie Ping received the Bachelor's degree in computer science from Fudan University, Shanghai, China, in 2008, and the Ph.D. degree in information systems from the School of Computing, National University of Singapore, Singapore, in 2014.

He has published his work in the *Journal of the Association for Information Systems*. He has also presented and published his research work at conferences, such as the International Conference on Information Systems, the European Conference on Information Systems, and the Pacific Asia Conference on Information Systems. His research interests include the areas of information privacy and digital marketing on new interactive media platforms, such as mobile media, social media, and advergame platforms.

Yunjie (Calvin) Xu received the Ph.D. degree in management information systems from Syracuse University, New York, NY, USA, in 2002.

He is a Professor with the School of Management, Fudan University, Shanghai, China. His research interests include electronic commerce, knowledge management, and social media. His research publications appeared in various information systems journals, including the *Journal of Management Information Systems*, the *Journal of Association for Information Systems,* the *Journal of the American Society for Information Science and Technology,* the IEEE TRANSACTIONS ON PROFESSIONAL COMMUNICATION*,* the *Communication of the ACM,* the *International Journal of Electronic Commerce*, and the *Journal of Retailing, Decision Support Systems*.

Bernard C. Y. Tan received the Ph.D. degree from the National University of Singapore (NUS), Singapore, in 1995.

He has been a Visiting Scholar at Stanford University, Stanford, CA, USA, and the University of Georgia, Athens, GA, USA. He is Vice-Provost at NUS, where he was formerly the Head of the Department of Information Systems. He is Shaw Professor of Information Systems at NUS, where he received university awards for research and for teaching. He was the 15th President of the Association for Information Systems. His research work has been published in *ACM Transactions on Computer–Human Interaction*, *ACM Transactions on Information Systems*, *ACM Transactions on Internet Technology*, *ACM Transactions on Management Information Systems*, *Communications of the ACM*, *Decision Support Systems*, the *European Journal of Information Systems*, IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, IEEE TRANSACTIONS ON PROFESSIONAL COMMUNICATION, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS, *Information and Management*, *Information Systems Frontiers*, *Information Systems Research*, the *International Journal of Human–Computer Studies*, the *Journal of Global Information Management*, the *Journal of Management Information Systems*, the *Journal of the AIS*, the *Journal of the American Society for Information Science and Technology*, *Management Science,* and *MIS Quarterly*. His current research interests include social media, virtual communities, and Internet commerce.

He is a Fellow of the Association for Information Systems. He has served on the Editorial Boards of *MIS Quarterly* as a Senior Editor, the *Journal of the AIS* as a Senior Editor, the IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT as a Department Editor, *Management Science* as an Associate Editor, *ACM Transactions on Management Information Systems* as an Associate Editor, and the *Journal of Management Information Systems* as an Editorial Board Member.