Journal of the Association for Information Systems (2018) **19**(3), 124-151
doi: 10.17705/1jais.00487

RESEARCH PAPER

ISSN 1536-9323

Love at First Sight: The Interplay Between Privacy Dispositions and Privacy Calculus in Online Social Connectivity Management

Ben Choi[1], Yi Wu[2], Jie Yu[3], Lesley Land[4]

[1]Nanyang Technological University, Singapore, benchoi@ntu.edu.sg
[2]Tianjin University, China, yiwu@tju.edu.cn
[3]University of Nottingham Business School China, jie.yu@nottingham.edu.cn
[4]University of New South Wales, Australia, l.land@unsw.edu.au

Abstract

Privacy has become the key concern of many users when they are confronted with friend requests on online social networking websites. Nonetheless, users' responses to friend requests seem at times inconsistent with their concerns about potential privacy implications. They accept friend requests and expose their personal profiles to largely unfamiliar others even though they are aware of the risks involved. Drawing on impression formation theory and the privacy calculus perspective, this paper elucidates the intriguing roles of privacy risks and expected social capital gains in social connectivity management by examining the key types of social information that users consider and their behavioral responses to online friend requests. We conducted a scenario-based experiment with 141 subjects. Our results indicate that individuals utilize two key types of social information; namely, network mutuality and profile diagnosticity in evaluating privacy risks and expected social capital gains. In addition, we find that privacy risks and expected social capital gains powerfully predict the likelihood of no-action and the likelihood of accepting friend requests on online social networking websites. In sum, this study contributes to the information systems literature by integrating impression formation theory and the privacy calculus perspective to identify the key types of social information that influence privacy tradeoff and predict individuals' behavioral responses toward establishing new online social connections.

Keywords: online social connectivity management, privacy risks, expected social capital gains, network mutuality, profile diagnosticity

1 Introduction

In recent years, online social networks have become nearly as universal as the Internet itself—with Facebook having 1.94 billion active users (statista, 2017). Increasing evidence suggests that the development of new network relationships is one of the key motivators for using online social networks (e.g., Yan & Tan, 2014). For instance, on Facebook, a new social network connection (SNC) or friendship is formed when a user's (i.e., requester) friend request is accepted by the intended recipient (i.e., request responder) (Boyd & Heer, 2006). The request responder typically responds to the friend request based on an impression of the requester, which can be formed based on the personal and network information available on the requester's personal profile (Sunnafrank & Ramirez, 2004). Overall, the establishment of SNC is an important issue not just to service providers but also to users in developing new online relationships.

How online relationships are developed and maintained has been a salient topic in information systems (IS) research (e.g., Choi, Jiang, Xiao, & Kim, 2015; Jiang, Heng, & Choi, 2013; Kim, Chan, & Kankanhalli, 2012). However, prior research has mostly examined relationship maintenance in online environments such as online communities, discussion forums, and chat rooms. The unique characteristics of online social networks could engender both similarities and differences in establishing new relationships, in comparison to other online environments. Like other online relationships, online social networking relationships typically involve the exchange of personal information; while such exchanges are vital to developing meaningful relationships, they also threaten information privacy (Choi et al., 2015). Thus, regardless of the online environment where users initiate relationships, information privacy is expected to be a similarly prevalent concern (Acquisti, Brandimarte, & Loewenstein, 2015). However, establishing online social network connections also differs from initiating other online relationships in several ways. First, other online relationships often involve largely unknown others. For example, online chat rooms involve relationships among anonymous individuals (Mileham, 2007) who can only be identified through avatars and/or nicknames. In online social networks, however, prior to initiating the connection, individuals typically have access to some basic identity information, such as profile pictures, gender, and lists of friends (Ellison, Hancock, & Toma, 2012), which they can use to estimate the potential threat to their privacy. Second, in other online environments users typically develop and maintain similar relationship types, and the coexistence of multiple relationship types is generally uncommon. In contrast, researchers have identified the convergence of multiple relationship types as a major privacy challenge in online social networks (Ellison et al., 2012). Furthermore, in similarity to offline relationship development, online relationships generally advance with a gradual escalation of information exchange, which can be regulated to protect privacy (Jiang et al., 2013). However, concerning online social networks, since personal profiles may contain a chronological archive of personal information and past activities, establishing online social network connections can instantaneously expose a thorough account of individuals to unfamiliar others. Collectively, these unique privacy implications in establishing online social connections warrant careful investigation.

Past IS research has substantially advanced our understanding of individuals' technology usage concerning privacy (e.g., Choi et al., 2015; Jiang et al., 2013; Smith, Dinev, & Xu, 2011). While IS literature has explored several aspects of privacy-related behavior, it has focused primarily on usage behavior during online commercial transactions (e.g., Sutanto, Tan, & Fang, 2013; Tsai, Egelman, Cranor, & Aquisti, 2011). As a result, we know of little research that has focused on privacy-related behavior beyond the rim of commercial transactions. Therefore, the theoretical framing of our study will address the particular attributes of online social interactions. For example, in performing commercial transactions, individuals typically focus on completing purchases and hence pay attention to transaction specific information, such as aftersales services and payment options. However, in developing online social network connections, individuals are likely to look beyond a specific exchange and contemplate subsequent interactions. As a result, they can be motivated to consider a wide variety of social information, such as self-generated information (e.g., self-disclosure in personal profile), friend-generated information (e.g., comments), and system-generated information (e.g., number of friends) (e.g., Choi et al., 2015). The impact of such a rich range of social information on online social network connection establishment warrants careful investigation. Hence, our first research question is: *What are the key types of impression-related information that a request responder considers in establishing new online social network connections?*

Since assessing new online social network connections entails impression formation, impression formation theory (Fisk & Neuberg, 1990) offers a suitable overarching framework. This theory helps us identify key impression-related information considered in the process of forming impressions, and clarifies how the outcome of this process influences the development of social relationships. Specifically, drawing on impression formation theory, this study focuses on two key categories of social information: namely, category-based information and attribute-based information, which are both essential to forming impressions of the requester.

Privacy research has devoted much attention to assessing the costs and benefits associated with privacy (e.g., Jiang et al., 2013; Sutanto et al., 2013). Most of these studies have advanced the general understanding of privacy calculus, while focusing on the tradeoff between privacy risks and certain tangible benefits (e.g., Dinev & Hart, 2006; Xu, Teo, Tan, & Agarwal, 2010). It is important to note that past research has mainly focused on how two interactants develop relationships (e.g., Jiang et al., 2013). However, new social network connections involve not only dyadic relationships, but also potentially instigate social exchanges between two different social circles. Hence, the second research question is: *What are the specific privacy risks and benefits that a request responder evaluates in establishing new online social network connections?* To this end, this paper integrates past privacy research and the social network literature to investigate the request responder's cost-benefit evaluations related to establishing new online social network connections. In terms of cost evaluation, this paper draws on the privacy literature to explain how the request responder's privacy can be threatened by accepting a friend request. In terms of benefit evaluation, this paper relies on the social network literature to understand the impact of online social network connections on the social resources available to the request responder. Research in the interpersonal communication domain offers insight into the impact of cost-benefit evaluations. For example, Karl and Peluchette (2011) revealed that users were more inclined to reject friend requests when they were concerned about malicious usage of their profile information.

Past privacy research has also highlighted that in the process of evaluating a privacy calculus, individuals typically struggle with information overload and limited cognitive resources, and hence are vulnerable to evaluating information less carefully and becoming subject to heuristic and cognitive biases (Choi et al., 2015). Instead of carefully performing a privacy calculus evaluation, individuals might take mental shortcuts (e.g., dispositions) to bypass the cognitive challenges. Indeed, according to Dinev, McConnell, and Smith (2015), individuals' sensitivity to privacy (e.g., self-relevancy and motivation to protect) could cause differential impacts on behavioral reactions concerning the effects of a privacy tradeoff. For example, Smith et al. (2011) noted that certain individuals typically discounted the risk of disclosing personal information (e.g., identity theft) if the risk was invisible or spread over time, while focusing on the immediate benefits of disclosure (e.g., convenience of placing orders online). Collectively, emerging evidence hints at the role of privacy dispositions in shaping the intricate joint influence of perceived risk and benefit on privacy related behaviors. Hence, to better understand the interplay between individuals' privacy dispositions and privacy calculus, the third research question is*: What is the role of dispositional privacy concerns in shaping the impacts of privacy calculus on behavioral reactions?*

Finally, the traditional view of information privacy focuses on privacy issues associated with explicit self-disclosure (Jiang et al. 2013). Recent studies examining information privacy suggest that an individual's privacy calculus determines a range of response behaviors to protect privacy (e.g., Choi et al., 2015). However, while shedding light on privacy protective behaviors, the privacy literature offers limited insight into individuals' behavioral responses to establishing online social network connections. Thus, the fourth research question is: *What are the behavioral strategies that a request responder performs in response to new online social network connections?*

The remainder of the paper is organized as follows. Section 2 comprehensively reviews the previous literature and discusses the theoretical foundations of this paper. Section 3 discusses the research model and hypotheses. Sections 4 and 5 elaborate the research methodology and data analysis. This paper concludes with discussions of theoretical and practical contributions, limitations, and avenues for future research in Section 6.

2 Literature Review

In this section, we develop our theoretical perspective on online social network connection establishment. We begin by reviewing impression formation theory, which serves as the overarching framework of this research. We then turn to the literature on social relationship development to identify the key impression information that a responder considers in forming online social network connections. Furthermore, we discuss extant privacy research and the social network literature to understand the responder's cost-benefit evaluation.

2.1 Impression Formation Theory

Impression formation is a psychological process that describes how an individual attempts to evaluate another person in a social interaction. According to impression formation theory, the process of interpersonal evaluation begins when an interactant presents him/herself in a social interaction. The other individual typically attempts to process social information to develop an impression of the interactant. Depending on the individual's evaluations, positive impressions are typically met with positive responses, whereas negative impressions are often detrimental to relationship development. Past research examining relationship development has recognized that individuals often face a formidable array of social information used to form interpersonal impressions. The impression formation process is manageable only by selectively attending to certain types of social information.

Through selective attention, individuals might assign social information to cognitive categories, which are abstract representations of conceptually related information. Indeed, in their seminal works on impression formation theory, Fisk and Neuberg (1990) consider category-based information and attribute-based information as the key types of social information that individuals interpret in forming impressions. Specifically, they posit that interpersonal impression is jointly determined by category-based information processing and attribute-based information processing. In the following sections, we discuss these two key types of social information.

2.1.1 Category-Based Information

Category-based information refers to heuristic information that cues relationship categories in the initial stage of impression formation (Fisk & Neuberg, 1990). Past research examining social cognition suggests that individuals often focus on immediately available informational cues to categorize a target person. Once categorized, expectations associated with the category are activated and form the basis for the impression of the target person. Extant empirical research has considered a broad array of category-based information in impression development. For instance, Kunda and Thagard (1996) examined impression formation in social interactions and found that individuals typically stereotype other social interactants based on readily available information, such as skin color, appearance, and attire. Likewise, Freeman and Ambaby (2011) revealed that individuals often developed initial impressions of others based on apparent face and body cues, such as sex, race, and age.

Hayes and Barnes-Holmes (2004) posit that category-based information triggers social categorization by invoking relational frames stored in memory. Relational frames are a set of cognitions about a relationship group, such as stereotypes and relationship schema (Weinstein, Wilson, Drake, & Kellum, 2008). Researchers suggest that category-based information facilitates sense-making by providing mechanisms for comprehending relational communications. For example, in a vignette study, Solomon, Dillard, and Andersen (2002) examined the role of heuristic information in elucidating social interactions. Specifically, the authors found that heuristic information that implied social interactions with similar others (e.g., common social circles) triggered a relational frame for close relationships, whereas heuristic information that implied interactions with dissimilar others (e.g., distinct social circles) activated the relational frame for distant relationships. Furthermore, individuals interpreted relational approaches (i.e., friend requests) based on the activated relational frame. With the relational frame for close relationship activated, relational approaches were typically thought to be friendly. Conversely, if the relational frame for distant relationship triggered, individuals considered relational approaches with prudence.

2.1.2 Attribute-Based Information

Whereas category-based information facilitates impression formation through relationship categories, attribute-based information refers to other noticeable information specific to the requester that requires more elaborate processing beyond initial relationship categorization, and activates individualization in social information processing (Fisk & Neuberg, 1990). Unlike category-based information, which is often readily available, attribute-based information is typically acquired only through observation and careful diagnosis. For instance, in the earlier mentioned study, Kunda and Thagard (1996) found that individuals carefully synthesized attribute-based information by observing others' behaviors in developing impressions. More importantly, initial stereotypes that individuals formulated using immediately available category-based information shaped how they subsequently interpreted attribute-based information to form impressions.

By considering others' specific attributes systematically, individuals are more likely to develop a deep understanding of others. For example, Spears and Lea (1992) noted that specific attribute-based information was essential in forming impressions of idiosyncratic others. Specifically, the author revealed that attribute-based information helped emphasize interpersonal distinctions in the online environment, and hence independently accentuated others' identity. Tanis and Postmes (2003) examined how profile content affects impression formation and found that the availability of profile pictures and a biography substantially reduced impression ambiguity. More importantly, it was found that the availability of attribute-based information led to a positive impression of the target. Overall, extant studies reveal the importance of rich attribute-based information in forming concrete interpersonal impressions.

Collectively, past research has thoroughly demonstrated the importance of both category-based information and attribute-based information in impression formation (see Appendix). It is worthy to note that category-based information is typically accessible and readily available, whereas attribute-based information is often available only through explicit deliberation. As a result, when category-based information is available up front, it often influences how individuals interpret attribute-based information to form impressions.

2.2 Privacy Calculus and Establishment of Online Social Network Connections

The conceptualization of privacy and the examination of privacy-related behavioral outcomes have long been a focus of information privacy research (e.g., Hong & Thong, 2013; Malhotra, Kim, & Agarwal, 2004), which has identified a myriad of determinants of privacy perceptions in both offline and online environments. In an interdisciplinary review of privacy-related research, Smith et al. (2011) integrated the major privacy perspectives to propose an integrative privacy-specific framework; namely, the antecedents-privacy concerns-outcomes (APCO) model. Specifically, the model posits that individuals' responses to external stimuli result in a deliberate privacy calculus that leads to fully informed privacy-related behaviors.

Within the APCO model, privacy antecedents are features of the privacy decision-making context (e.g., a friend request episode) that individuals consider in order to perform privacy calculus. While privacy antecedents might be explicated in different contextual factors, past privacy studies have demonstrated the importance of identity-related information in online social interactions. For example, Jiang et al. (2013) found that the anonymity of others was an important antecedent of individuals' privacy calculus in developing online relationships. Specifically, they found that the anonymity of others increased individuals' concerns about privacy and decreased their evaluation of social rewards. Essentially, in developing online social relationships, privacy antecedents subsume social information (e.g., identity-related information) that is vital to privacy calculus.

Privacy calculus is a psychological process that weighs the costs associated with privacy loss against the potential benefits derived through privacy exposure (Dinev et al., 2015). The central tenet of the privacy calculus perspective is that privacy transactions are evaluated in economic terms. Essentially, when individuals encounter a privacy situation, they perform a cost-benefit analysis to assess the outcomes they would face in return for exposing personal information, and then develop behavioral reactions accordingly (Hui, Teo, & Lee, 2007).

While past research has considered a variety of risks and gains, it has suggested that privacy risks and expected social capital gains are particularly relevant to individuals' behavior concerning their personal information in social settings. Privacy risks exemplify individuals' beliefs concerning the extent to which their privacy is open to exploitation (Xu, Dinev, & Hart, 2011). Typically, privacy risks have been regarded as a countervailing force to positive interpersonal evaluation when situational contingencies create feelings of uncertainty, discomfort, or anxiety (Luo, Li, Zhang, & Shim, 2010). Consistent with extant research, this study defines privacy risks as threats to personal information associated with the establishment of online social network connections. This type of privacy risk is particularly important because the establishment of online social network connections exposes individuals' private space to unforeseen dangers. For instance, in a study examining privacy calculus in online social networking, Dienlin and Metzger (2016) found that individuals evaluated risks to privacy against the perceived benefits of using Facebook in determining their disclosure and withdrawal behaviors. Likewise, Sun, Wang, Shen, and Zhang (2015) found that individuals' privacy could be threatened when they disclosed their location to online social network friends, which might consist of both well-known friends and largely-unknown acquaintances.

Whereas privacy risks represent the potential repercussions of establishing new social connections, expected social capital gains represent the relational benefits individuals expect in allowing access to private space. Expected social capital gains are defined as the estimated increase in relational support derived through relationship development (Coleman, 1988). Past research has regarded expected gains in social capital as the main enticement for individuals to engage in social interactions (e.g., Wang, Moon, Kwon, & Evans, 2010). By establishing social connections, individuals can draw on additional resources from others' social networks. These resources can take the form of useful information, personal relationships, or socioemotional support. Researchers have considered individuals' expectation of social capital gains to be an important component in their cost-benefit evaluation concerning online social networking. For instance, Ellison et al. (2012) revealed that social capital gains resulting from creating social connections were the most important benefits of online social networks.

While researchers believe privacy risks to be a prime inhibitor to online social networking, they have also found responder's expected social capital gains to be a major driver of developing social connections. On the one hand, researchers suggest that privacy risks motivate avoidance to social connections. For example, Posey and Ellis (2007) noted that users of online social networks were particularly prudent in establishing social relationships when they faced high privacy risks. On the other hand, social capital gains also entice responders to accept connections on online social networking websites. For instance, in a study on interpersonal connections, Ellison et al. (2012) noted that the development of social network connections was motivated by expected social capital gains, such as additional emotional support, and exposure to diverse ideas. Overall, privacy risks and expected social capital gains, which represent the two components in the responder's privacy calculus, are particularly important in determining responses to online social network requests.

2.3 Privacy Dispositions and Privacy Calculus

Past IS research has made significant progress in understanding individuals' concerns for privacy. In particular, the majority of extant studies has focused on dispositional privacy concerns, which refer to individuals' overall concerns about opportunistic behavior related to disclosing personal information in the online social networking environment (Smith, Milberg, & Burke, 1996). Despite the established understanding of dispositional privacy concerns, some evidence suggests that individuals' dispositional privacy concerns might not be entirely sufficient in explaining privacy-related behavior in a specific privacy calculus. Indeed, several scholars underscore the importance of considering transaction-specific privacy concerns in explaining individuals' privacy calculus. For example, Ackerman and Mainwaring (2005) suggest that individuals develop highly divergent privacy concerns in different privacy situations. The authors pointed out that while individuals might be extremely concerned about privacy on healthcare websites, they might be much less sensitive to privacy issues on online social networking websites.

Recent IS research has started to formally recognize the transactional aspect of privacy calculus. For instance, Xu, Teo, Tan, and Agarwal (2012) showed that individuals' dispositional privacy concerns reflect their inherent needs and attitudes toward maintaining privacy, whereas transaction-specific privacy perceptions focus on specific assessments of privacy weighing privacy needs against information disclosure during a transaction. In essence, dispositional privacy concerns reflect individuals' basic beliefs about privacy, which are typically stable across various encounters with technologies. Privacy calculus, however, focuses on how individuals evaluate privacy in a specific online exchange involving personal information. Hence, privacy calculus is typically context-specific and formed in accordance with each unique privacy encounter.

Overall, in the spirit of past privacy research, this paper considers privacy calculus in terms of individuals evaluating their privacy concerns prior to establishing new social network connections. Specifically, in terms of privacy calculus, privacy risks represent the cost evaluation and the expected social capital gains represent the benefit evaluation. In terms of privacy disposition, this study investigates the role of dispositional privacy concerns for shaping the impacts of privacy calculus on behavioral reactions toward establishing online social network connections.

3 Research Model and Hypothesis Development

The research model draws on impression formation theory as the overarching framework to explain individuals' behavioral reactions to establishing online social network connections (see Figure 1). Specifically, consistent with the theory, this study examines two types of social information; namely, category-based information and attribute-based information, as the antecedents of privacy calculus. Corresponding to the important role of category-based information in impression formation, *network mutuality* reflects how the responder's evaluation of a friend request activates relationship categories. Network mutuality refers to the degree to which the responder and the requester share common interpersonal connections (Rogers & Kincaid, 1981). Based on the influence of attribute-based information on impression formation, we examine the notion of a requester's *profile diagnosticity* to understand how profile information triggers individualization in interpersonal evaluation. *Profile diagnosticity* refers to how much detailed information is contained in the requester's profile.

We investigate the effects of these two independent variables on the responder's privacy calculus in terms of *perceived privacy risks* and *expected social capital gains* in establishing connections with the unfamiliar requester. Emerging privacy research has also revealed the distinction between privacy calculus and privacy dispositions. Therefore, this study focuses on *dispositional privacy concerns*, which underscores individuals' general belief associated with privacy challenges in online social networks, and examines how it moderates between individuals' privacy calculus and their behavioral responses.

Finally, we predict that privacy risks and expected social capital gains influence the privacy-related behaviors of no-action and acceptance concerning online social network connection management.

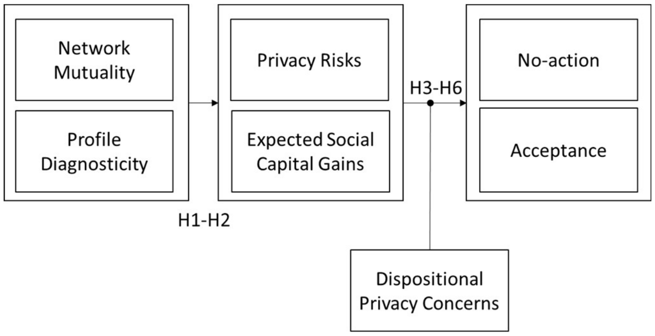


Figure 1. Research Model

3.1 Determinants of Privacy Risks

According to the principle of homophily, similarity in interpersonal connections increases ease of communication, improves predictability of behavior, and fosters trust and reciprocity between interactants (McPerson, Smith-Lovin, & Cook, 2001). A responder who overlaps social networks with a requester may be more likely to share a common perspective regarding relationship development, and such commonality would reduce the risks of developing connections. The social cohesion engendered by network mutuality would reduce the likelihood that a requester would engage in exploitive behavior, and hence would reduce the risks to the responder's privacy. For example, Ashleigh and Nandhakumar (2007) showed that individuals who shared highly interconnected social networks had significantly higher levels of confidence, respect, and commitment than those who shared less interconnected networks. Thus, we predict:

H1a: Compared to low network mutuality between requester and responder, high network mutuality leads to lower responder privacy risks.

In addition to network mutuality, we expect privacy risks to be influenced by requester's *profile diagnosticity*. By establishing profile connectivity, the responder initiates, develops, and maintains an interpersonal relationship with the requester. Researchers have noted the importance of personal profiles in the initial stage of relationship development. For example, Ellison et al. (2012) examined the importance of personal profiles on online dating websites. They found that comprehensive profile information served as a concrete psychological contract, which ensured that social interactions would take shape in mutually agreed upon and equitable manner. In sum, when a requester's profile diagnosticity is high, the responder may develop a rich understanding of the requester, reducing privacy risks with regards to establishing social network connection. Therefore, we posit:

H1b: Compared to low requester profile diagnosticity, high requester profile diagnosticity leads to lower responder privacy risks.

Relational framing theory (RFT) suggests that individuals extract relational meaning from social information based on relational frames, which can be triggered by social category cues (Dillard, Kinney, & Cruz, 1996). For example, Solomon et al. (2002) examined the effects of relational frames on social interactions and found that individuals' general attachment orientations influenced their interpretation of specific exchange in social episodes. Accordingly, we postulate an interaction effect of network mutuality and requester's profile diagnosticity on privacy risks. When network mutuality is high, a relational frame for close relationships is activated, which not only suppresses the responder's uncertainty in interpretation but also converges his/her focus in terms of social similarity with the requester—that is, the responder is likely to perceive the requester as someone who shares common interpersonal connections. Thus, in the high network mutuality condition, the responder might conveniently construct his/her impression of the requester based on network mutuality and be less motivated to consider specific profile information (Gawronski, Ehrenberg, Banse, Zukova, & Klauer, 2003). In particular, in evaluating privacy risks, the responder might focus on the high commonality in online social networks and expect the requester to be similar to the responder's friends in regulating and protecting privacy (Petronio, 2012). Furthermore, through high network mutuality, the responder might conjecture some social assurance that the requester is aware of the potential social repercussion for violating the responder's privacy. In sum, when network mutuality is high, the effect of requester's profile diagnosticity on perceived privacy risks is likely diminished.

On the contrary, low network mutuality suggests less commonality in interpersonal relationships, which activates a relational frame for distant relationships (Dillard, Kinney, & Cruz, 1996). With the influence of this relational frame, the responder is likely to become more prudent in forming impressions of the requester. Such prudence motivates the responder to adopt a careful approach in which he or she considers all of the attribute-based information available in the requester's personal profile. Further, the relational frame for distant relationships tends to be less informative and concrete (Bless, Schwarz, & Wieland, 1996). As a result, low network mutuality does not provide a sufficient basis for finalizing the responder's impression of the requester. Thus, in low network mutuality condition, attribute-based information available in personal profiles is essential to the responder's assessment of privacy risks. Compared to low requester profile diagnosticity, high requester profile diagnosticity connotes a more informative profile, and hence reduces privacy risks with regards to establishing social network connections. Specifically, low network mutuality connotes a lack of social assurance, and the responder is likely to be aware of the uncertainty concerning privacy in establishing a social network connection. In the case of low requester's profile diagnosticity, the requester not only lacks indirect social assurance, but is also deprived of extensive personal information about the requester. As a result, the requester is likely to be anxious about privacy concerning that online social network connection. In contrast, high requester profile diagnosticity implies that extensive information about the requester is available. The requester might develop a more concrete understanding about the requester's attitude toward protecting the responder's privacy. Thus, drawing on RFT, we predict the following interaction effect:

H1c: There is an interaction effect on privacy risks between network mutuality and requester profile diagnosticity—i.e., in comparison to the low network mutuality condition, the high network mutuality condition reduces the effect of requester profile diagnosticity on privacy risks.

3.2 Determinants of Expected Social Capital Gains

In addition to evaluating privacy risks, category-based information is important to the responder's assessment of expected social capital gains in establishing social network connections. In online social networks, network mutuality is a concise representation of similarity in social networks as well as commonality in interpersonal relationships. In general, most responders would prefer to develop relationships with those of high network mutuality. Research on interpersonal relationships has consistently uncovered strong links between network mutuality and liking, which is also termed the similarity effect. Further, researchers have also noted that high network mutuality induces perceptual biases, which cause individuals to overestimate the degree of interpersonal similarity (Montoya, Horton, & Kirchner, 2008). More importantly, according to the network cohesion perspective (Cohen & Hoberman, 1983), high network mutuality is indicative of a high degree of network cohesion, which suggests a highly collegial environment in which the responder might obtain socioemotional support. Therefore, compared to low network mutuality, the responder would expect larger social capital gains through establishing online social network connections with a requester of high network mutuality. Thus, we hypothesize:

H2a: Higher network mutuality leads to higher expected social capital gains.

From a social penetration perspective, when an unfamiliar requester reveals him/herself through self-disclosure, the responder is better able to understand the requester and predict future behaviors (Srull & Wyer, 1989). When a relationship is initiated in offline contexts, the responder's impression is typically formed based on direct assessment of attribute-based information, such as appearance and nonverbal cues (Tidwell & Walther, 2002). In online social networks, the lack of physical presence limits attribute-based information to the requester's self-disclosure in personal profiles. As a result, the responder must rely heavily on the requester's diagnostic profile in assessing expected social capital gains. To illustrate, when profile diagnosticity is low, the requester presents very limited personal information. As a result, the responder likely has access to limited personal information, such as gender, birthday, and profile photos. In contrast, when profile diagnosticity is high, the requester reveals a rich range of personal information, such as multiple photo albums, educational background, and professional experiences. An abundance of personal information is essential to developing a thorough understanding of the requester's social status, affiliations, and latent relationships. Accordingly, high requester profile diagnosticity is capable of inducing expectations of large social capital gains in establishing social network connections. For instance, Walther, Van Der Heide, Kim, Westerman, and Tong (2008) found that when profiles were highly comprehensive, individuals typically expected the online connection to be socially rewarding. On the contrary, when there were many missing details in profiles, individuals were less likely to expect a socially rewarding relationship. Thus, we predict:

H2b: Higher requester profile diagnosticity leads to higher expected social capital gains.

RFT highlights the importance of category-based information in forming individuals' perception of benefits (Dillard et al., 1996). Within the framework of RFT, when individuals perceive relationship commonality with others, a relational frame for close relationships is activated, which dominates their evaluation of relationship development, and hence reduces their focus on attribute-based information (Gawronski et al., 2003). However, if individuals perceive difference in social connections, a relational frame for distant relationships is activated, which emphasizes prudence in developing relationships. Hence, individuals are likely to pay attention to attribute-based information. Specifically, when network mutuality is low, the responder will not expect a high degree of interpersonal similarity. As a result, the responder is more likely to rely on profile diagnosticity to evaluate the expected social capital gains in establishing social network connection. In the case of low profile diagnosticity, the responder is not likely to find insightful information about the requester, and hence it will be difficult, if not impossible, to estimate the potential social capital gains. In contrast, in the case of high profile diagnosticity, the responder will be able to draw on a rich profile of information (i.e., social status, professional affiliations, and latent relationships) of the requester to vividly establish the potential of social capital gains.

According to RFT, therefore, when network mutuality is high, the responder feels assured that the requester would have common interests and share mutual understanding in developing relationships, thereby reducing the responder's reliance on profile information in assessing social capital gains. In particular, high network mutuality is indicative of network cohesion, which implies a high likelihood of obtaining socioemotional support. Since the responder might draw on immediately available network mutuality information in evaluating expected social capital gains, the role of profile diagnosticity is likely less prevalent compared with low network mutuality. Thus, we propose:

H2c: There is an interaction effect on expected social capital gains between network mutuality and requester profile diagnosticity—i.e., in comparison to the low network mutuality condition, the high network mutuality condition reduces the effect of requester profile diagnosticity on expected social capital gains.

3.3 Privacy Calculus and Behavioral Responses

Extending impression formation theory, this paper draws on Choi et al.'s (2015) classification to focus on two types of behavioral response to social network connection establishment; namely, no-action and acceptance. Whereas no-action represents a passive response to social network connection requests, acceptance subsumes the responder's active responses in either agreement or disagreement (i.e., rejection). No-action refers to the responder's adoption of the inaction strategy. Through performing no-action, the responder demonstrates disinterest in establishing a new social network connection with the unfamiliar requester. In contrast, acceptance is an active response that facilitates the development of online social connectivity by formally establishing the network connection between the two personal profiles. It is worthy to note that acceptance is typically the opposite of rejection, which allows the responder to dissociate from the requester in online social networking environments.

3.3.1 Privacy Risks and Behavioral Responses

Privacy risks highlight not just the probability of threats to privacy but also underscore the severity of the threat. No-action is not an effective behavioral strategy to address privacy risks because no-action maintains the responder's exposure and expresses the responder's tolerance to potential privacy implications (Choi et al., 2015). It is important to note that, while no-action toward friend requests does not further expose the responder to the requester, it might subject the responder to future harassment if the requester continues to make repetitive friend requests. Hence, privacy risks provide strong reasons for the responder to avoid no-action.

Accepting a friend request can be risky because it represents the responder's willingness to expose him/herself to the requester in online social networks. Much research suggests that in online social networks, relationship acceptance can be impeded by the responder's perceptions of privacy risks in establishing social network connections. For example, Ellison et al. (2012) found that when individuals expected high privacy risks in establishing profile connections, they were more reserved toward friend requests. Hence, privacy risks are expected to reduce approach behavior. In sum, we hypothesize:

H3a: Privacy risks will reduce the likelihood of no-action.

H3b: Privacy risks will reduce the likelihood of acceptance.

3.3.2 Expected Social Capital Gains and Behavioral Responses

According to the principle of economics, when individuals expect to gain from an exchange, they will be motivated to take explicit actions to realize the expected gains. Hence, when a responder expects social capital gains from establishing a new social network connection, he/she is likely to be enticed to act favorably toward the friend request. Therefore, the responder who expects social capital gains will be less likely to take no-action.

A number of studies suggest that expected social capital gains significantly influence friend request acceptance. For example, Tong, Van Der Heide, Langwell, and Walther (2008) investigated relationship development in online social networks and found that the social resource gains that individuals expected from forming social ties with others increased their willingness to sustain interpersonal connections. These findings imply that the responder's gains in social capital may induce acceptance in response to a friend request. Collectively, we posit:

H4a: Expected social capital gains will reduce the likelihood of no-action.

H4b: Expected social capital gains will increase the likelihood of acceptance.

3.4 The Interplay Between Dispositional Privacy Concerns and Privacy Calculus

Past privacy research suggests that the underlying mechanics of privacy calculus on behavioral responses can be influenced by loss aversion, which subsumes individuals' stronger preference for avoiding losses than for acquiring gains (Tversky & Kahneman, 1991). The risk literature has produced substantial evidence on the inverse relationship between judgment of risks and judgment of benefits. The central tenant of the literature focuses on the cognitive biases, which suggest that individuals might discount the potential for benefits when the risk potential is high. Accordingly, when individuals are confronted with high risks in evaluating an uncertain issue, pressure toward avoiding risks would lead them to discount the potential benefits. Similarly, when evaluating a request for establishing a new social network connection when privacy risks are high, the responder will likely focus on the high privacy risks and overlook the potential social capital gains. Therefore, we hypothesize:

H5a: The effect of expected social capital gains on no-action is stronger when privacy risks are low than when privacy risks are high.

H5b: The effect of expected social capital gains on acceptance is stronger when privacy risks are low than when privacy risks are high.

Past IS research has largely assumed that privacy-related behaviors are enacted through deliberate, high-effort processing. However, according to the privacy literature, privacy-related behaviors could also be performed based on low-effort processing, which typifies simple and relatively automatic cognitive heuristics as well as mental shortcuts. While a number of complex factors determine the level of cognitive effort being expended, past privacy research has emphasized the importance of dispositional privacy concerns. For instance, in a study examining adoption of electronic health records, Angst and Agarwal (2009) found that dispositional privacy concerns caused a differential impact on the effects of argument-framing and issue involvement concerning intentions to opt-in. Specifically, individuals with strong dispositional privacy concerns were highly critical when evaluating information associated with the usage of electronic health records, whereas those with weak dispositional privacy concerns were largely indifferent toward the privacy implications.

Accordingly, we propose that dispositional privacy concerns moderate the impacts of privacy calculus on behavioral responses to social connectivity establishment. The notion of zero-value boundary in risk analysis (Grable, 2000) can explain the interactions between dispositional privacy concerns and privacy calculus. Specifically, according to the risk literature, if individuals have high risk propensity, they are willing to take chances with respect to the risk of loss and hence risks might be immaterial in the evaluation. To illustrate, most people understand the risk of financial losses in gambling, but gambling addicts may simply ignore the risk of loss.

Similarly, we expect low dispositional privacy concerns to moderate the impacts of privacy calculus on behavioral responses. Specifically, a responder with low dispositional privacy concerns is essentially insensitive toward privacy issues in using online social networks. Accordingly, that responder is likely to pay little attention to privacy risks and may ignore the possibility of losing privacy when establishing new social network connections. Following the logic of cognitive biases, given the lower emphasis on privacy risks, that responder will be less likely to discount the potential social capital gains in accepting the friend request. In essence, when a responder has low dispositional privacy concerns, the importance of privacy risks in the privacy calculus is diminished, and hence the effect of privacy risks in moderating the impact of expected social capital gains on behavioral responses is likely reduced.

In contrast, when a responder has high dispositional privacy concerns, the effect of privacy risks in moderating the impact of expected social capital gains on behavioral responses is expected to be amplified. Past privacy research has revealed individuals' variations in allocating different weight to the cost and benefit components in privacy calculus. These findings broadly pointed at the role of general privacy sensitivity in amplifying the impact of loss, which reduces the effect of benefits in influencing privacy-related behavior. In particular, high dispositional privacy concerns represent the responder's vulnerability to privacy issues and tendency to avoid risks. Accordingly, with high dispositional privacy concerns, the responder is likely to emphasize the importance of privacy risks. More importantly, since the highlighted pressure to avoid risk is likely to reduce the importance of benefits, we would expect the highlighted level of privacy risks to reduce the relevance of expected social capital gains in influencing the establishment of new social network connections. Collectively, we posit:

H6: Compared to low dispositional privacy concerns, high dispositional privacy concerns will strengthen the negative moderating influence of privacy risks concerning the impact of expected social capital gains on acceptance.

4 Research Methodology

We chose Facebook as the online social network platform for our study for two reasons: 1) Facebook facilitates establishment of social network connections by providing social information such as network mutuality and profile information; 2) Facebook's high popularity allows for a greater generalizability of findings.

4.1 Experimental Design

We conducted a laboratory experiment with a 2 (network mutuality: low vs. high) x 2 (profile diagnosticity: low vs. high) factorial design to test the proposed hypotheses. Network mutuality was manipulated by the number of shared friends the subject had in common with the requester. Recent research suggests that average Facebook users typically have about 17.5% of shared Facebook friends (Eldon, 2010). Accordingly, low network mutuality was represented as ≤5% of subjects' reported number of Facebook friends, whereas high network mutuality was represented as ≥30% of the number of reported Facebook friends.

We determined profile diagnosticity by manipulating the number of content items in the mock-up personal profile of the requester, mimicking actual Facebook layout. Evidence suggests that a typical Facebook user profile is about three years old, contains 1008 photos and 756 status updates, and has received 828 comments (Hampton, Goulet, Marlow, & Rainie, 2012; Koc & Gulyagci, 2013). Therefore, low profile diagnosticity was represented using an experimental profile that contained 50 photos, 38 updates, and 41 received comments. High profile diagnosticity was represented with a profile containing 1966 photos, 1474 updates, and 1615 received comments. To control for the potential effect of the content nature and sequence of content presentation, the experimental profile was dynamically populated with content items that were randomly selected from a common content pool. To improve the realism of the experiment, we developed the profile content based on actual Facebook profile content contributed by students from the same university as the experiment participants. The content was deidentified and revised to reflect the identity of a generic university student. The experiment involved a simulation of a Facebook friend request using a hypothetical scenario—such simulations have been broadly used in prior IS and privacy research (e.g., Choi et al. 2015).

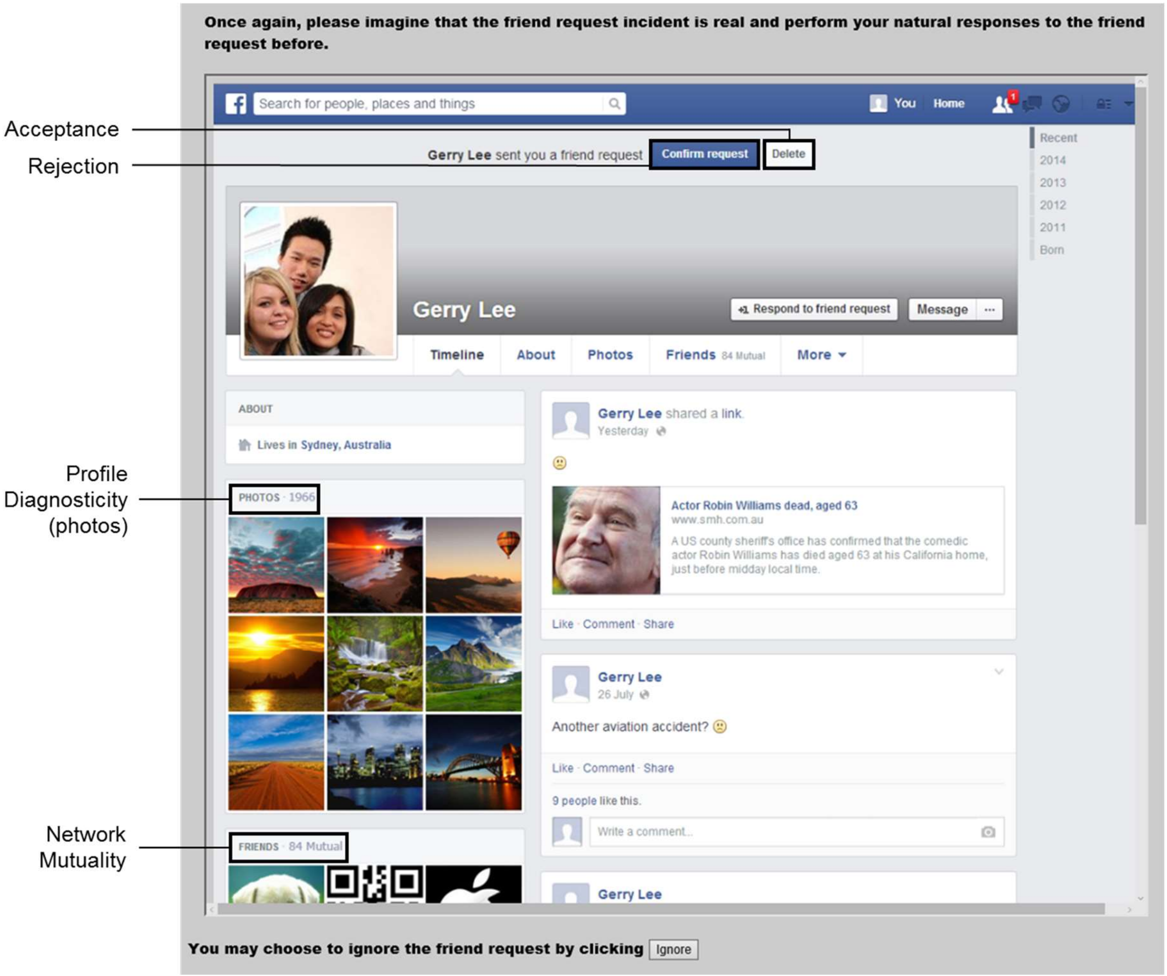
A pilot test was conducted with 20 subjects (five subjects in each experimental condition) to verify the experimental protocols. In the pilot test, subjects were randomly assigned to an experimental condition and presented with the hypothetical friend request scenario on Facebook that was sent to them by an unfamiliar requester who had low (or high) network mutuality with the subjects and had a profile with low (or high) diagnosticity. Subjects were asked to imagine that the scenario was real and review the profile carefully. Upon completing the questionnaire, subjects were shown a mock-up environment (see Figure 2) and could respond (i.e., accept) or not respond (i.e., no-action) to the friend request. Additionally, subjects were instructed to complete an online survey that contained measurement items (7-point Likert scales) to capture perceived realism and perceived relevance of the hypothetical scenario. Results suggest that the scenarios were highly realistic (mean = 6.12) and relevant to people like our subjects (mean = 5.78).

4.2 Main Experiment

Subjects were university students who had online social networking experience. One week prior to the experiment, subjects received an e-mail that instructed them to complete a prestudy survey. In this survey, subjects were asked to provide information about demographics, Internet experience, Facebook experience, and their number of Facebook friends. To verify subjects' Facebook usage, they were asked to provide their profile names, which the researchers used to contact them on Facebook.

We recruited 141 subjects to participate in the experiment. To enhance involvement, we asked subjects to log in to their actual Facebook accounts on a browser window. They were then randomly assigned to one of the four experimental conditions in an experimental Facebook environment that was modeled on the actual Facebook layout. On another browser window, we presented them with one of the four scenarios (i.e., varied across the two [low/high] categories of network mutuality and profile diagnosticity) where they received a friend request from an unfamiliar requester.

Subjects were told to imagine that the scenario was real (i.e., they received the friend request on their actual Facebook accounts) and read through it carefully. They were also encouraged to carefully evaluate the profile content of the requester (i.e., number of mutual friends, photos, postings, and comments) and spend as much time as they needed. Afterwards, they were instructed to complete a questionnaire that contained manipulation checks and measurements of the mediating variables. Upon completing the questionnaire, subjects were shown a mock-up environment (see Figure 2) and asked to respond (or not to respond) to the friend request. In terms of responding to the request, they could either reject or accept the request. After completing the responses in the mock-up environment, we debriefed the subjects and thanked them.



Once again, please imagine that the friend request incident is real and perform your natural responses to the friend request before.

Gerry Lee sent you a friend request

Gerry Lee shared a link.
Yesterday

Actor Robin Williams dead, aged 63
www.smh.com.au
A US county sheriff's office has confirmed that the comedic actor Robin Williams has died aged 63 at his California home, just before midday local time.

Gerry Lee
26 July
Another aviation accident?

9 people like this.

You may choose to ignore the friend request by clicking Ignore

Figure 2. Mock-Up Facebook Environment

5 Data Analysis

5.1 Subject Demographics and Background Analysis

Among the 141 subjects, 67 were females. The age of the subjects ranged from 19 to 24, with average Internet experience and average Facebook experience of 7.2 years and 3.9 years respectively. The average number of reported Facebook friends was 203.1. The average time a subject spent on completing the entire experiment was 25 minutes.

No significant differences were found among subjects randomly assigned to each of the four experimental conditions with respect to age, gender, Internet experience, Facebook experience, and number of Facebook friends, indicating that subjects' demographics were quite homogeneous across different conditions.

5.2 Measurements

We conducted the manipulation check for network mutuality by asking responders to rate the extent to which they had common friends with the requester (see Table 1). On a seven-point Likert scale, responders in the low network mutuality condition reported a mean value of 2.03 for the extent of multiple social ties (standard deviation = 0.38) and responders in the high network mutuality condition reported a mean value of 5.51 for the extent of multiple social ties (standard deviation = 0.57). The difference was significant (t = -42.56, p <0.01), and hence the manipulation for network mutuality worked as anticipated.

We conducted the manipulation check for requester profile diagnosticity by asking responders to rate the extent to which the requester's personal profile provided detailed information about the person. On a seven-point Likert scale, responders in the low requester profile diagnosticity condition reported a mean value of 2.55 for the extent of profile detail (standard deviation = 0.50) and responders in the high requester profile diagnosticity condition reported a mean value of 5.54 for the extent of profile detail (standard deviation = 0.56). The difference was significant (*t* = -33.38, *p* <0.01), and hence the manipulation for requester profile diagnosticity worked as anticipated.

Table 1. Measurement Item

Network mutuality (NM), developed based on Choi et al. (2015)	
NM1	The requester and I are connected through multiple friends on Facebook.
NM2	The requester and I have many common friends on Facebook.
NM3	The requester and I have highly similar social circles on Facebook.
NM4	Many of my friends are friends of the requester on Facebook.
Profile diagnosticity (PD), developed based on Jiang and Benbasat (2004)	
PD1	The requester's profile is helpful for me to familiarize myself with him/her.
PD2	The requester's profile is helpful in influencing my overall evaluation of him/her.
PD3	The requester's profile is helpful in forming my judgment of him/her.
PD4	The requester's profile tells a lot about him/her.
Privacy risks (PR), adapted from Xu, Teo, Tan, and Agarwal (2010)	
PR1	Establishing profile connectivity with the requester would involve many unexpected problems.
PR2	It would be risky to establish profile connectivity with the requester.
PR3	There would like high potential for loss in establishing profile connectivity with the requester.
PR4	There would be too much uncertainty associated with establishing profile connectivity with the requester.
PR5	I would feel safe establishing profile connectivity with the requester. (r)
Expected social capital gains (ESCG), adapted from Lochner, Kawachi, and Kennedy (1999)	
ESCG1	Establishing profile connectivity with the requester would allow me to obtain additional socioemotional support from his/her social networks.
ESCG2	Establishing profile connectivity is an important way to acquire additional instrumental support from the requester's social networks.
ESCG3	I consider establishing profile connectivity with the requester as one way of acquainting myself to his/her social networks, so that I may garner additional informational support.
ESCG4	Establishing profile connectivity with the requester is an important way to allow me to rely on his/her social networks.
Dispositional privacy concerns, adapted from Smith et al. (1996)	
Collection	
DPC-C1	It usually bothers me when online social networking websites ask me for personal information.
DPC-C2	When online social networking websites ask me for personal information, I sometimes think twice before providing it.
DPC-C3	It bothers me to give personal information to unfamiliar others.
DPC-C4	I'm concerned that online social networking websites are collecting too much personal information about me.
Errors	
DPC-E1	All the personal information in computer database should be double-checked for accuracy—no matter how much this costs.
DPC-E2	Online social networking websites should take more steps to make sure that the personal information in their files is accurate.

Table 1. Measurement Item

DPC-E3	Online social networking websites should have better procedures to correct errors in personal information.
DPC-E4	Online social networking websites should devote more time and effort to verifying the accuracy of the personal information in their databases.
Unauthorized Access	
DPC-U1	Online social networking websites should devote more time and effort to preventing unauthorized access to personal information.
DPC-U2	Computer databases that contain personal information should be protected from unauthorized access no matter how much it costs.
DPC-U3	Online social networking websites should take more steps to make sure that unauthorized people cannot access personal information in their computers.
Secondary Use	
DPC-S1	Online social networking websites should not use personal information for any purpose, unless they have been authorized by the individuals who provided the information.
DPC-S2	When people give personal information to a company for some reasons, the company should never use the information for any other reason.
DPC-S3	Online social networking websites should never sell the personal information in their computer databases to other online social networking websites.
DPC-S4	Online social networking websites should never share personal information with other online social networking websites unless they have been authorized by the users who provided the information.
Note: (r) reverse item.	

We adapted five items measuring *privacy risks* (Cronbach's alpha = 0.89) from Xu et al. (2010) and we adapted four items measuring *expected social capital gains* (Cronbach's alpha = 0.91) from Lochner et al. (1999) (see Table 1). The Concerns for Information Privacy (CFIP) scales (Smith et al. 1996) were used to measure dispositional privacy concerns. The CFIP scales capture privacy concerns as a second-order variable with four first-order factors; namely, collection, error, unauthorized access, and secondary use. Following Chin (1998) and past IS research (e.g., Jiang et al. 2013), we computed four sets of factor scores based on the four first-order constructs. We then considered these four factor scores as indicator variables for dispositional privacy concerns (Cronbach's alpha = 0.95). Exploratory factor analysis shows that, in general, items load well on their intended factor and lightly on the other factors, thus indicating adequate construct validity (see Table 2).

Table 2. Rotated Factor-Item Loadings

	NM	PD	DPC	PR	ESCG
NM1	***0.92***	0.10	0.02	-0.23	0.15
NM2	***0.91***	0.04	0.08	-0.25	0.11
NM3	***0.87***	0.11	0.03	-0.28	0.18
NM4	***0.83***	0.14	0.07	-0.21	0.20
PD1	0.05	***0.91***	0.10	-0.11	0.25
PD2	0.06	***0.85***	0.11	-0.15	0.21
PD3	0.08	***0.87***	0.05	-0.19	0.26
PD4	0.10	***0.81***	0.14	-0.08	0.28
DPC-COL	0.23	0.25	***0.91***	-0.21	-0.02
DPC-ERR	0.14	0.21	***0.96***	-0.02	-0.09
DPC-UA	0.16	0.26	***0.96***	0.01	-0.11

Table 2. Rotated Factor-Item Loadings

DPC-SU	0.18	0.28	***0.95***	0.03	-0.08
PR1	-0.22	-0.24	-0.01	***0.75***	-0.24
PR2	-0.25	-0.29	-0.15	***0.81***	-0.18
PR3	-0.21	-0.22	0.03	***0.79***	-0.26
PR4	-0.20	-0.25	-0.03	***0.84***	-0.07
PR5	-0.26	-0.27	-0.05	***0.78***	-0.16
ESCG1	0.25	0.30	-0.13	-0.22	***0.82***
ESCG2	0.19	0.29	-0.06	-0.20	***0.85***
ESCG3	0.22	0.24	-0.02	-0.26	***0.84***
ESCG4	0.27	0.27	-0.11	-0.13	***0.88***

Notes:
NM = network mutuality; PD = profile diagnosticity; DPC = dispositional privacy concerns; COL = DPC-collection; ERR = DPC-errors; UA = DPC-unauthorized access; SU = DPC-secondary use; PR = privacy risks; ESCG = expected social capital gains.

Off-diagonal elements in Table 3 represent correlations of all latent variables, while the diagonal elements are the square roots of the average variances extracted (AVE) of the latent variables. Since the square roots of AVE of any latent variables are greater than the correlations shared between the latent variable and other latent variables, discriminant validity is deemed adequate.

Table 3. Internal Consistency and Discriminant Validity of Constructs

	CR	CA	M	NM	PD	DPC	PR	ESCG
NM	0.95	0.92	3.86	***0.90***				
PD	0.93	0.88	4.10	0.04	***0.93***			
DPC	0.96	0.95	4.98	0.20	0.24	***0.89***		
PR	0.93	0.89	4.16	-0.22	-0.26	-0.02	***0.88***	
ESCG	0.96	0.91	4.58	0.23	0.27	-0.05	-0.19	***0.93***

5.3 Results on Privacy Risks

We conducted multivariate analysis of variance (MANOVA) on both privacy risks and expected social capital gains. Results show that the treatment effects were significant (p <0.05); hence we also conducted analysis of variance (ANOVA) separately on the two dependent variables.

ANOVA with privacy risks as dependent variable reveals that higher network mutuality significantly leads to lower privacy risks (F [1, 137] = 85.81, p <0.01) (see Table 4 and 5). Furthermore, requester's profile diagnosticity was found to have a significant main effect on privacy risks (F [1, 137] = 28.03, p <0.01), meaning that compared to low requester's profile diagnosticity, high requester's profile diagnosticity reduces privacy risks. Hence, H1a and H1b are supported.

Simple main effect analysis reveals that 1) high requester profile diagnosticity is associated with significantly lower privacy risk than low requester profile diagnosticity under the low network mutuality condition (F [1, 69] = 41.61, p <0.01), and 2) low requester profile diagnosticity and high requester profile diagnosticity are not different from each other in affecting privacy risks under the high network mutuality condition (F [1, 68] = 1.12, p =0.16) (see Table 4 and 5; Figure 3). Therefore, H1c is supported.

Table 4. ANOVA Results on Privacy Risks

Source	Type III sum of squares	Df	Mean square	F	Sig.
Overall sample NM	85.81	1	85.81	101.90	.000
PD	28.03	1	28.03	33.28	.000
NM * PD	14.40	1	14.40	17.10	.000
Error	115.37	137	.84		
Total	2583.08	141			
NM=Low					
PD	41.61	1	41.61	36.71	.000
Error	78.21	69	1.13		
Total	1790.40	71			
NM=High					
PD	1.12	1	1.12	2.04	.158
Error	37.16	68	.55		
Total	792.68	70			

Notes: dependent variable: privacy risks; NM = network mutuality; PD = profile diagnosticity.

R squared = .529 (adjusted R squared = .518)

Table 5. Mean Values of Privacy Risks

	Low PD	High PD	Mean
Low NM	5.61	3.41	4.51
High NM	4.07	3.15	3.61
Mean	4.84	3.28	

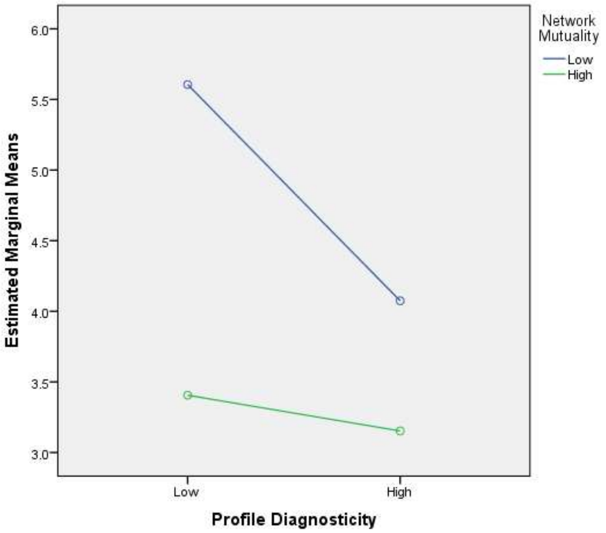


Figure 2. Mean Plot of Privacy Risks

5.4 Results on Capital Social Gains

ANOVA with expected social capital gains as dependent variable reveals that higher network mutuality significantly leads to higher expected social capital gains (F [1, 137] = 29.79, p <0.01) (see Table 6 and 7). Further, requester profile diagnosticity is found to have a significant main effect on expected social capital gains (F [1, 137] = 80.28, p <0.01), meaning that compared to low requester profile diagnosticity, high requester profile diagnosticity increases expected social capital gains (see Table 6 and 7; Figure 4). Hence, H2a and H2b are supported.

Simple main effect analysis reveals that 1) high requester profile diagnosticity is associated with significantly higher expected social capital gains than low requester's profile diagnosticity under the low network mutuality condition (F [1, 69] = 160.54, p <0.01), and 2) low requester profile diagnosticity and high requester profile diagnosticity are not different from each other in affecting expected social capital gains under the high network mutuality condition (F [1, 68] = .41, p =0.51). Therefore, H2c is supported.

Table 6. ANOVA Results on Expected Social Capital Gains

Source	Type III sum of squares	Df	Mean square	F	Sig.
Overall sample					
NM	29.79	1	29.79	33.32	.000
PD	71.77	1	71.77	80.28	.000
NM * PD	88.00	1	88.00	98.44	.000
Error	122.47	137	.89		
Total	3134.13	141			
NM=Low					
PD	160.54	1	160.54	184.19	.000
Error	60.14	69	.87		
Total	1358.69	71			
NM=High					
PD	.41	1	.41	.45	.506
Error	62.33	68	.92		
Total	1775.44	70			

Notes: dependent variable: privacy risks; NM = network mutuality; PD = profile diagnosticity.

R squared = .611 (adjusted R squared = .602)

Table 7. Mean Values of Expected Social Capital Gains

	Low PD	High PD	Mean
Low NM	2.52	5.53	4.03
High NM	5.02	4.87	4.95
Mean	3.77	5.20	

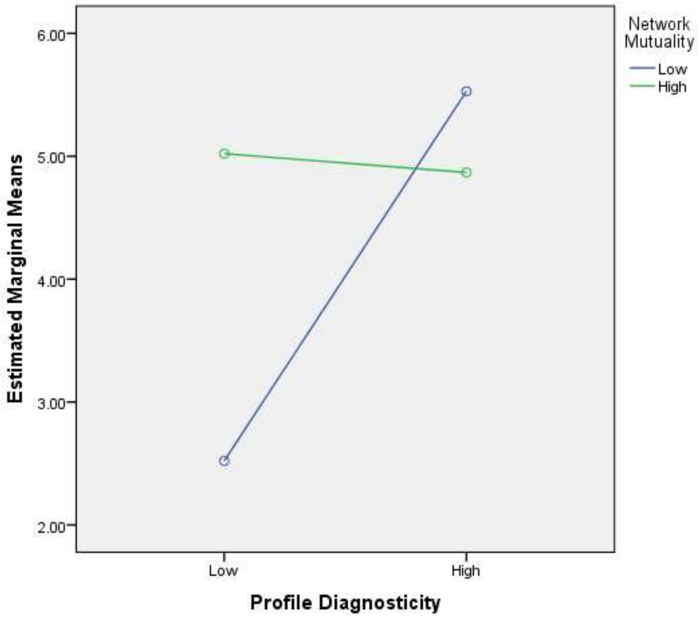


Figure 3. Mean Plot of Expected Social Capital Gains

5.5 Results on No-Action

A binary logistic regression was performed to test the effects of privacy risks, expected social capital gains, and dispositional privacy concerns on no-action. Overall, out of the 141 subjects, 64 chose no-action (77 subjects performed either acceptance or rejection). Before fitting the logistic regression models with no-action as outcome (see Table 8), we computed the standardized scores for privacy risks, expected social capital gains, and dispositional privacy concerns. The Cox & Snell Pseudo R^2 is 0.24, hence the binary logistic regression model predicts about 24% of no-action. As shown in Table 8, both privacy risks (β = -1.09, p <0.01) and expected social capital gains (β = -2.57, p <0.01) are found to have significant negative effects on no-action. Therefore, H3a and H4a are supported. Since the two-way interactions and three-way interactions are significant, further analysis was conducted to investigate the higher order interaction effects.

Table 8. Logistic Regression on No-Action (N = 141)

<table>
<tr><td colspan="8">Model Fit</td></tr>
<tr><td colspan="4">Likelihood ratio chi-square</td><td colspan="4">58.23</td></tr>
<tr><td colspan="4">Degrees of freedom</td><td colspan="4">5</td></tr>
<tr><td colspan="4">Significance</td><td colspan="4"><i>p</i> &lt;0.01</td></tr>
<tr><td colspan="4">Cox &amp; Snell pseudo R²</td><td colspan="4">0.24</td></tr>
<tr><td rowspan="2">Predictors</td><td rowspan="2">β</td><td rowspan="2">SE</td><td rowspan="2">Wald</td><td rowspan="2">Sig</td><td rowspan="2">OR</td><td colspan="2">95% CI</td></tr>
<tr><td>Lower</td><td>Upper</td></tr>
<tr><td>Estimate</td><td>2.65</td><td>4.56</td><td>5.32</td><td><i>p</i> &lt;0.01</td><td>2.85</td><td></td><td></td></tr>
<tr><td>ESCG</td><td>-2.57</td><td>0.22</td><td>6.71</td><td><i>p</i> &lt;0.01</td><td>2.79</td><td>-1.44</td><td>-1.05</td></tr>
<tr><td>PR</td><td>-1.09</td><td>0.36</td><td>5.10</td><td><i>p</i> &lt;0.01</td><td>2.61</td><td>-4.41</td><td>-2.02</td></tr>
<tr><td>DPC</td><td>-0.91</td><td>0.17</td><td>4.23</td><td><i>p</i> &lt;0.01</td><td>2.13</td><td>-3.12</td><td>-1.31</td></tr>
<tr><td>ESCG*PR</td><td>-2.49</td><td>0.44</td><td>9.93</td><td><i>p</i> &lt;0.01</td><td>3.23</td><td>-1.82</td><td>-1.43</td></tr>
<tr><td>ESCG*DPC</td><td>-0.80</td><td>0.13</td><td>5.28</td><td><i>p</i> &lt;0.01</td><td>2.86</td><td>-1.74</td><td>-1.05</td></tr>
</table>

PR*DPC	-0.94	0.19	3.29	*p <0.01*	1.98	-1.64	-1.01
ESCG*PR*DPC	-0.85	0.13	1.24	*p <0.05*	1.24	-1.35	-1.02
PR = Low							
ESCG	-1.89	0.29	10.29	*p <0.01*	5.48	-10.95	-1.16
DPC	-0.52	0.17	3.93	*p <0.01*	1.81	-1.82	-1.43
PR = High							
ESCG	-1.05	0.26	5.11	*p <0.01*	1.80	-1.94	-1.21
DPC	-0.44	0.15	8.83	*p <0.01*	1.91	-1.86	-1.48
DPC = Low							
ESCG*PR	-0.94	0.45	4.33	*p <0.05*	1.40	-1.59	-1.19
DPC = High							
ESCG*PR	-0.53	0.24	4.92	*p <0.05*	1.42	-1.57	-1.37

Following past research, to facilitate interpretation of the interaction effects, we performed median-split on privacy risks. Since the mean of privacy risks was 3.6, continuous scores that were less than or equal to 3.6 were coded as 0 (i.e., low privacy risks), whereas continuous scores that were greater than 3.6 were coded as 1 (i.e., high privacy risks). When privacy risks are low, for every unit change in expected social capital gains, the log odds of no-action reduces by -1.89. When privacy risks were high, the log odds of no-action reduced by -1.05. The results imply that compared to low privacy risks, with high privacy risks, expected social capital gains lead to less reduction in no-action likelihood. Therefore, H5a is supported.

5.6 Results on Acceptance

Since rejections and acceptance are opposite actions, we conducted a binary logistic regression (N = 77) to test how privacy risks, expected social capital gains, and dispositional privacy concerns affected acceptance.

Table 9 presents the result of the logistic regression analysis with acceptance as the outcome variable. The Cox & Snell Pseudo R^2 is 0.29, hence privacy risks, expected social capital gains, and dispositional privacy concerns predict about 29% of acceptance. As shown in Table 9, privacy risks (β = -1.78, *p* <0.01) were found to have a significant positive effect on acceptance, whereas expected social capital gains (β = 1.31, *p* <0.01) had a significant negative effect on acceptance. Therefore, H3b and H4b are supported. Since both the two-way interactions and three-way interactions are significant, we conducted further analysis to investigate the higher order interaction effects.

Table 9. Logistic Regression on Acceptance (N = 77)

Model Fit							
Likelihood ratio chi-square				32.97			
Degrees of freedom				5			
Significance				*p <0.01*			
Cox & Snell pseudo R^2				0.29			
Predictors	β	SE	Wald	Sig	OR	95% CI	
						Lower	Upper
Estimate							
ESCG	1.31	0.58	14.56	*p <0.01*	5.61	1.44	7.89
PR	-1.78	0.21	17.42	*p <0.01*	6.97	-9.00	-1.87
DPC	-1.60	0.32	10.01	*p <0.01*	5.51	-7.78	-1.54

ESCG*PR	1.43	0.32	7.54	*p <0.01*	2.23	1.34	1.88
ESCG*DPC	1.16	0.30	8.97	*p <0.01*	3.05	1.14	2.31
PR*DPC	-2.21	0.27	24.47	*p <0.01*	9.77	-12.45	-2.31
ESCG*PR*DPC	0.79	0.21	7.21	*p <0.05*	2.02	1.38	1.81
PR = Low							
ESCG	1.23	0.11	8.87	*p <0.01*	3.13	1.30	1.87
DPC	-1.29	0.21	9.45	*p <0.01*	3.07	-1.84	-1.03
PR = High							
ESCG	0.24	0.21	2.33	*p =0.11 (N.S.)*	1.00	0.49	0.97
DPC	-1.90	0.20	14.21	*p <0.01*	5.47	1.30	8.56
DPC = Low							
ESCG*PR	1.30	0.19	7.76	*p <0.01*	2.51	1.05	1.75
DPC = High							
ESCG*PR	0.07	0.26	2.01	*p =0.31 (N.S.)*	0.91	0.08	0.51

When privacy risk was low, for every one-unit change in expected social capital gains, the log odds of acceptance increased by 1.23. When privacy risks were high, the effect of expected social capital gains on acceptance was not significant (β = 0.24, *p* =0.11). The results imply that compared to low privacy risks, with high privacy risks, expected social capital gains lead to less increase in acceptance likelihood. Therefore, H5b is supported.

Furthermore, when dispositional privacy concerns were low, for every unit change in expected social capital gains and privacy risk collectively, the log odds of acceptance increased by 1.30. When dispositional privacy concerns were high, the joint effect of expected social capital gains and privacy risk on acceptance was not significant (β = 0.07, *p* =0.31). The results imply that compared to low dispositional privacy concerns, the interaction effect on acceptance between expected social capital gains and privacy risk is stronger when dispositional privacy concerns are high. Therefore, H6 is supported.

5.7 Common Method Bias

Following the recommendation of Podsakoff, MacKenzie, Lee, and Podsakoff (2003) and past IS research (Jiang et al., 2013), we tested for possible common method bias by conducting confirmatory factor analysis (CFA) for two models. First, we estimated a six-factor model, which included six constructs in the research model with privacy concerns consisting of four first-order factors. Each of the 24 measurement items was restricted to being an indicator for the respective latent factor. Fit indices of the first model (α^2 [237] = 258.1) were as follows: α^2/df = 1.09, SRMR = 0.421, RMSEA = 0.012, NFI = 0.953, CFI = 0.992, GFI = 0.912, AGFI = 0.823, TLI = 0.990. Generally, these indices satisfied the recommended thresholds and hence indicate a good fit of the model to the data.

In the second model, in addition to the six factors examined in the first model, we conducted a CFA with one additional factor to represent the unmeasured common method. We allowed each of the 24 items to load on its respective theoretical factor construct, and all were allowed to load on the additional method factor, which was constrained to be uncorrelated with the other ten factors. The fit indices for the second model (α^2 [213] = 232.3) were largely identical to those of the first model (α^2/df = 1.09, SRMR = 0.422, RMSEA = 0.012, NFI = 0.951, CFI = 0.990, GFI = 0.911, AGFI = 0.821, TLI = 0.990). Furthermore, a chi-square test comparing the first model with the second model indicated that the difference between the two models was not significant (α^2 [24] = 25.8, p = 0.36, N.S.), suggesting that the common method bias was not a serious concern.

6 Discussion and Conclusion

6.1 Discussion of Results

The results are in support of our hypotheses. We seek to enrich the understanding of social connectivity regulation in online social networks by considering the effects of privacy risks as well as expected social capital gains associated with social connectivity. We establish that the responder's perceptions of both costs and benefits influence their behavioral responses to the establishment of social network connections. We also hope to achieve a more comprehensive understanding of social connectivity regulation by examining network mutuality and requester profile diagnosticity, which we derived based on the two main types of social information in interpersonal cognition—namely, category-based information and attribute-based information respectively. Our findings show that network mutuality and requester profile diagnosticity are important determinants of privacy risks and expected social capital gains in establishing social connectivity.

We also seek to explain the different roles of dispositional privacy concerns and privacy calculus in affecting individuals' behavioral responses (i.e., no-action and acceptance) to establishing online social network connections. We demonstrate that privacy risks moderate the impact of expected social capital gains on behavioral responses. More importantly, we enhance the information privacy literature by clarifying the distinct roles of dispositional privacy concerns. Our findings reveal that dispositional privacy concerns alter the different impacts of privacy calculus on behavioral responses.

6.2 Theoretical Contribution

This study enriches the privacy literature in several ways. First, past IS research examining privacy issues in online social networks has devoted little attention to social connectivity regulation. This lack of attention to the establishment of social connections is somewhat surprising since a prime reason for individuals to adopt online social networks is to establish, develop, and maintain social connections. On the basis of the privacy calculus perspective, we identify privacy risks and expected social capital gains, as the cost and benefit elements of a privacy calculus, whereby individuals consider the privacy threats and social benefits in establishing social connectivity. Our findings show that privacy risks and expected social capital gains are indeed important determinants of individuals' responses to requests for social network connections. To the best of our knowledge, our study is the first to employ the notion of privacy calculus to understand distinct behavioral responses to establishing social connectivity.

Second, we contribute to the IS literature by providing evidence on the importance of impression formation in regulating social connectivity. While past studies have identified a myriad of factors pertinent to privacy perceptions, rarely have researchers examined the effects of social information processing on individuals' assessment of privacy threats and social benefits. Based on impression formation theory, this study identifies two important types of social information cues that influence privacy calculus; namely, network mutuality and requester's profile diagnosticity. Specifically, network mutuality is a type of social category-based information, which invokes relational frames to facilitate social categorization. Profile diagnosticity concerns the details of requester-specific information, which is essential for individualization in social information processing. Taken as a whole, we combine impression formation and privacy calculus and then show the efficacy of this integrative approach in the context of online social networks.

Third, to our best knowledge, this is one of the first studies to formally examine the interplay between dispositional privacy concerns and privacy calculus. Given the transactional nature of privacy calculus, it is surprising that past research has paid little attention to recognizing the difference. Drawing on Xu et al. (2012) and Li (2011), we proposed that privacy calculus and dispositional privacy concerns are independent concepts. Our findings show that privacy calculus is indeed distinct from dispositional privacy concerns. More importantly, our results reveal that the impacts of perceived benefits (i.e., expected social capital gains) on behavioral responses are moderated by individuals' judgment of risks (i.e., privacy risks).

6.3 Practical Contributions

Our findings have important implications for application designers as well as online social networks providers. Application designers for online social networks often provide mechanisms that address users' perception of privacy risks. While mechanisms that address privacy risks are somewhat common, few design efforts have been devoted to enhancing the appreciation of expected social capital gains. To this end, we advocate a design strategy that improves the recognition of expected social capital gains. As predicted by the proposed model, expected social capital gains are found to be enhanced by higher network mutuality and requester profile diagnosticity. While this result is largely consistent with conventional wisdom, a more interesting finding of this study is probably that the effect of profile diagnosticity on expected social capital gains is more pronounced in the low network mutuality condition than in the high network mutuality condition. This finding suggests that the richness of profile detail is crucial for relationship development between users who do not share a high degree of social commonality. This is because a rich profile provides vivid details about the requester, thereby reducing the responder's uncertainties and enhancing interpersonal understanding. Thus, it is important that application designers consider providing mechanisms that help enhance requester's profile diagnosticity, such as providing photo album previews and timeline abstracts in online social network platforms.

6.4 Limitations and Future Directions

This study examines the establishment of online social network connections between unfamiliar others. While we focus on a requester who shares some mutual friends with the request responder, we do not attempt to generalize the results to friend requests made from total strangers. In such a case, since the requester does not share any common friends with the responder, network mutuality may not come into play. Additionally, this study focuses on privacy risks and expected social capital gains as the cost and benefit components of privacy calculus. It is possible that individuals might consider other potential benefits in evaluating requests to establish online social network connections. For instance, individuals might accept connection requests to increase their social connection number as a means to signal their popularity (i.e., social enhancement). Additionally, they might accept new connection requests for entertainment value (e.g., thrill derived from the opportunity to interact with unfamiliar others). We encourage future studies to explore additional manifestation of privacy calculus pertinent to developing online social network connections.

It might also be worthy to note that our contributions may be limited by using a mock-up Facebook website. Although the mock-up website largely resembled the general layout and appearance of the website, the mock-up website may not entirely reflect the actual social networking environment. Despite this limitation, the mock-up environment allowed us to manipulate the experimental conditions, which would have otherwise been impossible in the actual environment. Since we used Facebook as the experimental environment, this study focused on network mutuality (which is readily available in a friend request) to represent category-based information, and used profile diagnosticity (which can be determined through explicit deliberation) to represent attribute-based information. It is possible that the two types of impression formation information might manifest differently in other contexts. Furthermore, some recent statistical evidence suggests that there may be more female than male users on Facebook. Caution should be taken in generalizing our findings to specific user types.

Furthermore, this study focuses on network mutuality as the social information cue for relationship category in forming impressions. It is important to note that other types of social information cues might also help activate relationship categories in developing impressions. For instance, when the requester and the responder are both fans of a football team, the relational frame for close relationships might be activated. Likewise, depending on the requester's marital status and professional affiliations, responders might assume vastly different relationship categories in impression development. To this end, we believe our research provides a robust theoretical framework that will help future studies explore other intriguing social information cues pertinent to online social networking.

It is also worthy of noting that online social networking websites have implemented a range of features whereby individuals can regulate the visibility of their social updates. For instance, on Facebook, users might explicitly exclude certain online friends from seeing their postings, and hence limit their privacy exposures. Furthermore, users might expect less privacy risks when their profile contains limited information. However, despite the availability of such privacy protection features and variation in profile content, evidence suggests that individuals largely ignore such visibility-regulation mechanisms and choose to continue using the default visibility settings, which typically expose individuals' existing disclosure and future disclosure (e.g., social updates, photos posting, and comments) to their online friends (Turner 2016). We encourage scholars to examine whether and how users adopt new privacy protection features, and how differences in profile content influence online social connectivity management. Lastly, this study identifies rejection and acceptance as the two key behavioral responses to online social network connection establishment. The recent introduction of visibility and audience management features by major social networking platforms could facilitate richer response behaviors. For instance, on Facebook, users might categorize friends into different types, which allows various levels of visibility concerning users' profile content. Likewise, Google+ allows users to classify friends into different social circles, which are assigned different levels of accessibility to users' profiles. Hence, it would be interesting for future research to examine how behavioral responses might manifest in such environments.

Acknowledgement

The authors wish to acknowledge the Nanyang Business School (Grant M4082100.010) and Science Foundation of Ministry of Education of China (Grant 17YJC630173) for financial support. The authors also appreciate the constructive comments provided to us by the review team. Yi Wu is the corresponding author of this paper.

References

Ackerman, M., & Mainwaring, S. (2005). Privacy issues and human-computer interaction. *Computer, 27* (5), 19-26.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science 347*(6221), 509-514.

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, 33(2), 339-370.

Ashleigh, M.J., & Nandhakumar, J. (2007). Trust and technologies: Implications for organizational work practices. *Decision Support Systems, 43*(2), 607-617.

Blair, I.V., Chapleau, K. M., & Judd, C. M. (2005). The use of Afrocentric features as cues for judgment in the presence of diagnostic information. *European Journal of Social Psychology, 35*(1), 59-68.

Bless, H., Schwarz, N., & Wieland, R. (1996). Mood and the impact of category membership and individuating information. *European Journal of Social Phycology, 26*(6), 935-959.

Boyd, d., & Heer, J. (2006). Profiles as conversation: Networked identity performance on Friendster. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 39*(3,) 59c-59c.

Chin, W.W. (1998). The Partial Least Squares Approach to Structural Equation Modeling. In G. A. Marcoulides (ed.), *Modern methods for business research* (pp. 295-336). Mahway, NJ: Lawrence Erlbaum.

Choi, B.C., Jiang, Z., Xiao, B., & Kim, S. (2015). Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding. *Information Systems Research, 26*(4), 675-694.

Chun, W.Y., & Kruglanski, A. W. (2006). The role of task demands and processing resources in the use of base-rate and individuating information. *Journal of Personality and Social Psychology*, *91*(2), 205-217

Cohen, S., & Hoberman, H. M. (1983). Positive events and social supports as buffers of life change stress. *Journal of Applied Social Psychology,13*(2), 99-125.

Coleman, J.S. (1988). Social capital in the creation of human capital, *American Journal of Sociology, 94*, 95-120.

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication, 21*(5), 368-383.

Dillard, J.P., Kinney, T. A., & Cruz, M. G. (1996). Influence, appraisals, and emotions in close relationships. *Communication Monographs, 63*(2), 105-130.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions, *Information Systems Research, 17*(1), 61-80.

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. *Information Systems Research, 26*(4), 639-655.

Eldon, E. (2010). Facebook tests new "subscribe to" option for friends and pages. Retrieved from http://www.adweek.com/digital/facebook-tests-new-subscribe-to-option-for-friends-and-pages.

Ellison, N.B., Hancock, J. T., & Toma, C. L. (2012). Profile as promise: A framework for conceptualizing veracity in online dating self-presentations. *New Media & Society,14*(1), 45-62.

Epley, N., & Kruger, J. (2005). When what you type isn't what they read: The perseverance of stereotypes and expectancies over e-mail. *Journal of Experimental Social Psychology, 41*(4), 414-422.

Fisk, S.T., & Neuberg, S. L. (1990). A continuum of impression formation, from category-based to individuating processes: Influences of information and motivation on attention and interpretation. *Advances in Experimental Social Psychology, 23*, 1-74.

Freeman, J.B., & Ambady, N. (2011). A dynamic interactive theory of person construal. *Psychological review, 118*(2), 247-279.

Gawronski, B., Ehrenberg, K., Banse, R., Zukova, J., & Klauer, K. C. (2003). It's in the mind of the beholder: The impact of stereotypic associations on category-based and individuating impression formation. *Journal of Experimental Social Psychology, 39*(1), 16-30.

Grable, J.E. (2000). Financial risk tolerance and additional factors that affect risk taking in everyday money matters. *Journal of Business and Psychology, 14*(4), 625-630.

Greenlees, I., Buscombe, R., Thelwell, R., Holder, T., & Rimmer, M. (2005). Impact of opponents' clothing and body language on impression formation and outcome expectations. *Journal of Sport and Exercise Psychology, 27*(1), 39-52.

Hampton, K. N., Goulet, L. S., Marlow, C., & Rainie, L. (2012). Why most facebook users get more than they give. Retrieved from http://www.pewinternet.org/2012/02/03/why-most-facebook-users-get-more-than-they-give.

Hayes, S.C., & Barnes-Holmes, D. (2004). Relational operants: Processes and implications: A response to Palmer's review of relational frame theory. *Journal of Experimental Analysis of Behavior, 82*(2), 13-224.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: an integrated conceptualization and four empirical studies. *MIS Quarterly, 37*(1), 275-298.

Hosoda, M., Stone-Romero, E. F., & Coats, G. (2003). The effects of physical attractiveness on job-related outcomes: A meta-analysis of experimental studies. *Personnel Psychology, 56*(2), 431-462.

Hui, K.L., Teo, H. H., & Lee, S.-Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly, 31*(1), 19-33.

Jiang, Z., & Benbasat, I. (2004). Virtual product experience: Effects of visual and functional control of products on perceived diagnosticity and flow in electronic shopping. *Journal of Management Information Systems*, 21(3), 111-147.

Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research, 24*(3), 579-595.

Karl, K. A., & Peluchette, J. V. (2011). "Friending" professors, parents and bosses: A Facebook connection conundrum. *Journal of Education for Business*, 86(4), 214-222.

Kim, H.-W., Chan, H.C., & Kankanhalli, A. (2012). What motivates people to purchase digital items on virtual community websites? The desire for online self-presentation. *Information Systems Research, 23*(4), 1232-1245.

Ko, S.J., Judd, C. M., & Stapel, D. A. (2009). Stereotyping based on voice in the presence of individuating information: Vocal femininity affects perceived competence but not warmth. *Personality and Social Psychology Bulletin, 35*(2), 198-211.

Koc, M., & Gulyagci, S. (2013). Facebook addiction among Turkish college students: The role of psychological health, demographic, and usage characteristics. *Cyberpsychology, Behavior, and Social Networking, 16*(4), 279-284.

Kunda, Z., & Thagard, P. (1996). Forming impressions from stereotypes, traits, and behaviors: A parallel-constraint-satisfaction theory. *Psychological Review,103*(2), 284-308.

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems, 28*(1), 453-496.

Lochner, K., Kawachi, I., & Kennedy, B. P. (1999). Social capital: A guide to its measurement. *Health & Place,5*(4), 259-270.

Luo, X., Li, H., Zhang, J., & Shim, J. P. (2010). Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision Support Systems, 49*(2), 222-234.

Malhotra, N.K., Kim, S. S., & Agarwal, J. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information System Research, 15*(4), 336-355.

McPerson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a feather: Homophily in social networks. *Annual Review of Sociology,27*, 415-444.

Mileham, B.L.A. (2007). Online infidelity in internet chat rooms: An ethnographic exploration. *Computers in Human Behavior,23*(1), 11-31.

Montoya, R. M., Horton, R. S., & Kirchner, J. (2008). Is actual similarity necessary for attraction? A meta-analysis of actual and perceived similarity. *Journal of Social and Personal Relationships, 25*(6), 889-922.

Park, J.-W., Kim, K.-H., & Kim, J. (2002). Acceptance of brand extensions: Interactive influences of product category similarity, typicality of claimed benefits, and brand relationship quality. *Advances in Consumer Research, 29*(1), 190-198.

Petronio, S. 2012. *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: SUNY.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N.P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879-903.

Posey, C., & Ellis, S. (2007). Understanding self-disclosure in electronic communities: An exploratory model of privacy risk beliefs, reciprocity, and trust. *AMICS 2007 Proceedings,* 1-11.

Rogers, E.M., & Kincaid, D. L. 1981. *Communication Networks*. New York, NY: The Free Press:

Smith, H.J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989-1016.

Smith, H.J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196.

Solomon, D.H., Dillard, J. P., & Andersen, J. W. (2002). Episode type, attachment orientation, and frame salience: Evidence for a theory of relational framing. *Human Communication Research, 28*(1), 136-152.

Spears, R. L. & M. Lea (1992). Social influence and the influence of the "social" in computer-mediated communciation. In M. Lea (ed.) *Contexts in Computer-Mediated Communication*. Hertfordshire, UK: Harvester Wheatsheaf.

Srull, T.K., & Wyer, R. S. J. (1989). Person memory and judgment. *Psychological Review* (96(1), 58-83.

statista. (2017). Number of monthly active Facebook users worldwide as of 4th quarter (millions). Retrieved from https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide.

Sun, Y., Wang, N., Shen, X.-L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior, 52*, 278-292.

Sunnafrank, M., & Ramirez, A. (2004). At first sight: Persistant relational effects of get-acquainted conversations. *Journal of Social and Personal Relationships, 21*(3), 361-379.

Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly, 37*(4), 1141-1164.

Tanis, M., & Postmes, T. (2003). Social cues and impression formation in CMC. *Journal of Communication, 53*(4), 676-693.

Tidwell, L.C., & Walther, J.B. (2002). Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations: Getting to know one another a bit at a time. *Human Communication Research, 28*(3), 317-348.

Tong, S.T., Van Der Heide, B., Langwell, L., & Walther, J. B. (2008). Too much of a good thing? The relationship between number of friends and interpersonal impressions on Facebook. *Journal of Computer-Mediated Communication, 13*(3), 531-549.

Tsai, J.Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254-268.

Turner, A. (2016). 5 facebook privacy settings you should check right now. Retrieved from http://mashable.com/2016/11/29/facebook-privacy-checkup/#DS_Z032NqqqA.

Tversky, A., & Kahneman, D. (1991). Loss aversion in riskless choice: A reference-dependent model. *The Quarterly Journal of Economics, 106*(4), 1039-1061.

Walther, J. B., Van Der Heide, B., Kim, S. Y., Westerman, D., & Tong, S. T. (2008). The role of friends' appearance and behavior on evaluations of individuals on Facebook: Are we known by the company we keep?. *Human Communication Research, 34*(1), 28-49.

Wang, S. S., Moon, S.-I., Kwon, K. H., Evans, C. A., & Stefanone, M. A. (2010). Face off: Implications of visual cues on initiating friendship on facebook. *Computers of Human Behavior, 26*(2), 226-234.

Weinstein, J. H., Wilson, K. G., Drake, C. E., & Kellum, K. K. (2008). A relational frame theory contribution to social categorization. *Behavior and Social Issues, 17*(1), 40-65.

Whitty, M. T., & Gavin, J. (2001). Age/sex/location: Uncovering the social cues in the development of online relationships. *CyberPsychology and Behavior, 4*, 623-630.

Wyer, N.A. (2010). You never get a second chance to make a first (implicit) impression: The role of elaboration in the formation and revision of implicit impressions. *Social Cognition, 28*(1), 1-19.

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

Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2010). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems, 26*(3), 135-174.

Xu, H., Teo, H.H., Tan, B. C. Y., & Agarwal, R. (2012). Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research, 23*(4), 1342-1363.

Yan, L., & Tan, Y. (2014). Feeling blue? Go online: An empirical study of social support among patients. *Information Systems Research, 25*(4), 690-709

.

Appendix

Key Impressions formation studies	Category-based information	Attribute-based information
Kunda and Thagard (1996)	Occupation stereotypes (i.e., accountant vs. construction worker)	Behaviors (i.e., unaggressive vs. aggressive)
Greenlees, Buscombe, Thelwell, Holder, and Rimmer (2005)	Apparel (i.e., tennis-specific vs. general sportswear)	Body languages (i.e., positive vs. negative)
Freeman and Ambady (2011)	Visual information (i.e., face and body cues)	Auditory input (i.e., voice cues)
Wyer (2010)	Physical appearance (i.e., visibly shaved head)	Behavioral evidence (i.e., behaviors in a party)
Epley and Kruger (2005)	Photograph appearance (i.e., Asian American vs. African American)	Communication (i.e., e-mail vs. voice)
Gawronski et al. (2003)	Gender (i.e., male vs. female)	Individual responsibility (i.e., domestic vs. work)
Park, Kim, and Kim (2002)	Category similarity (i.e., a new grocery food vs. a nonfood product)	Benefit typicality information (i.e., brand typicality vs. brand atypicality)
Ko, Judd, and Stapel (2009)	Applicant gender (i.e., female vs. male)	Resume content (i.e., feminine vs. masculine)
Hosoda, Stone-Romero, and Coats (2003)	Physical attractiveness (i.e., attractive vs. unattractive)	Job nature descriptions (i.e., feminine job vs. masculine job)
Blair, Chapleau, and Judd (2005)	Racial category (i.e., Afrocentric features)	Diagnostic information (i.e., aggressive responses vs. nonaggressive responses)
Chun and Kruglanski (2006)	Occupation types (i.e., engineers vs. nonengineers)	Individuating information (i.e., easy to process vs. difficult to process)

About the Authors

Ben Choi is an assistant professor in Information Technology and Operations Management at the Nanyang Technological University, Singapore. He was previously a faculty member at the University of New South Wales. Ben received his B.Sci. and PhD in information systems from National University of Singapore. He has been named Reviewer of the Year 2016 at *MIS Quarterly*. He has published multiple papers in premier information systems journals including, *Information Systems Research, Journal of Management Information Systems,* and *Journal of the Association for Information Systems.* His research interests focus on information privacy, mobile healthcare, and social media.

Yi Wu is an assistant professor in Information Management and Management Science at the Tianjin University, China. He obtained his PhD in information systems from National University of Singapore. He received his B.Eng. in information management at the Renmin University of China. His research focuses on employees' IT behaviors, e-healthcare and social media. His research work has appeared in journal outlets, such as *Journal of the Association for Information Systems, Information and Management,* and *Internet Research.*

Jie Yu is an Assistant Professor of information systems at the Nottingham University Business School China. He received his PhD in information systems from National University of Singapore. His papers have been published in *Journal of Management Information Systems, International Journal of Production Economics,* and *Expert Systems with Applications.* His current research interests are social media, Internet celebrity, and human-computer interactions.

Lesley Land is a senior lecturer of information systems at the UNSW Australia Business School, University of New South Wales, Australia. She has a B.Sc. from the University College London, an M.Sc. from Brunel University, and a PhD from UNSW. Her research interests include understanding the impact of IT (such as social media and organizational systems)—their benefits and/or abuse, and IT implementation issues (including project management).