Information Systems Research

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions

Zhenhui (Jack) Jiang, Cheng Suang Heng, Ben C. F. Choi

To cite this article:
Zhenhui (Jack) Jiang, Cheng Suang Heng, Ben C. F. Choi (2013) Research Note—Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. Information Systems Research 24(3):579-595. https://doi.org/10.1287/isre.1120.0441

Information Systems Research
Vol. 24, No. 3, September 2013, pp. 579–595
ISSN 1047-7047 (print) | ISSN 1526-5536 (online)

http://dx.doi.org/10.1287/isre.1120.0441

Research Note

Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions

Zhenhui (Jack) Jiang
Department of Information Systems, School of Computing, National University of Singapore, Singapore 117418; and National University of Singapore (Suzhou) Research Institute, Suzhou, People's Republic of China 215123, jiang@comp.nus.edu.sg

Cheng Suang Heng
Department of Information Systems, School of Computing, National University of Singapore, Singapore 117418, hengcs@comp.nus.edu.sg

Ben C. F. Choi
Australian School of Business, The University of New South Wales, Sydney, NSW 2052, Australia, ben.cf.choi@gmail.com

Privacy is of prime importance to many individuals when they attempt to develop online social relationships. Nonetheless, it has been observed that individuals' behavior is at times inconsistent with their privacy concerns, e.g., they disclose substantial private information in synchronous online social interactions, even though they are aware of the risks involved. Drawing on the hyperpersonal framework and the privacy calculus perspective, this paper elucidates the interesting roles of privacy concerns and social rewards in synchronous online social interactions by examining the causes and the behavioral strategies that individuals utilize to protect their privacy. An empirical study involving 251 respondents was conducted in online chat rooms. Our results indicate that individuals utilize both self-disclosure and misrepresentation to protect their privacy and that social rewards help explain why individuals may not behave in accordance with their privacy concerns. In addition, we find that perceived anonymity of others and perceived intrusiveness affect both privacy concerns and social rewards. Our findings also suggest that higher perceived anonymity of self decreases individuals' privacy concerns, and higher perceived media richness increases social rewards. Generally, this study contributes to the information systems literature by integrating the hyperpersonal framework and the privacy calculus perspective to identify antecedents of privacy trade-off and predict individuals' behavior in synchronous online social interactions.

Key words: synchronous online social interactions; privacy concerns; privacy-protective behavior; social rewards; self-disclosure; misrepresentation
History: Elena Karahanna, Senior Editor; Katherine Stewart, Associate Editor. This paper was received on October 17, 2009, and was with the authors 16 months for 3 revisions. Published online in *Articles in Advance* May 28, 2013.

1. Introduction

Transcending temporal and spatial barriers, online social interactions have revolutionized lives by offering more than a space in which to hang out. They enable individuals to share cultural artifacts, manage self-presentation, or receive feedback from peers. For example, it was reported that, in 2011, over 20% of Internet users had participated in various online social interactions, such as chat room conversations and instant messaging (Ofcom 2011). Through these synchronous exchanges of information, individuals seek to gain immediate socio-emotional support and satisfaction in the immense and borderless space of the Internet.

Despite the promising potential of engaging in online social interactions, a survey of 1,698 Internet users in the United States has revealed that about one-third (33%) of the users were concerned about the loss of personal privacy (Madden and Smith 2010), particularly in the context of synchronous online social interactions. As an incredible amount of information is being exchanged synchronously, an individual's privacy is subject to public scrutiny. The possibility of real-time monitoring and eavesdropping aggravates the problem, by exposing individuals to potential harassment and flaming, or even more extreme forms of aggravation such as stalking and sexual abuse. Unlike the asynchronous exchanges of information, individuals' privacy concerns can be exacerbated in synchronous online social interactions. In the asynchronous environment, individuals can rely on message editing, reprocessing, or third-party advice on privacy protection (Son and Kim 2008); however, in the synchronous environment, individuals are pressured to maintain the flow of information exchange

and hence would be motivated to engage in more immediate behavior. For instance, when there is a request for personal information, an individual has to make an immediate decision on privacy-related behavior, and whether or not to disclose private information, and how to disclose it, so as to better safeguard and protect oneself (Joinson et al. 2007).

It has, however, been observed that despite privacy concerns, individuals are very willing and forthcoming toward the sharing of personal and intimate information with others, including complete strangers. For example, in another survey of 1,623 Internet users in the United States, nearly 40% explicitly expressed concerns about their privacy. Ironically, among this group of respondents, a majority reported that they would still be likely to disclose private information, such as names, affiliations, private thoughts, or opinions in interaction with others online (Madden et al. 2007). Hence, it would be interesting to investigate why users' privacy behavior is at times inconsistent with their privacy concerns.

Indeed, information systems (IS) research has made some progress in understanding the determinants of individuals' privacy-related behavior. For instance, Hui et al. (2007) investigated mechanisms of privacy mitigations. They found that although privacy assurance mechanisms, such as privacy statements, reduced privacy concerns, economic incentives encouraged individuals' risk-taking behavior, e.g., disclosure of personal information to Internet merchants. Thus the researchers suggested that individuals performed a privacy calculus psychologically when confronting privacy loss. Likewise, in a study of user behavior on financial websites, Hann et al. (2007) found that users were willing to reveal their private information, such as household income and stocks portfolio, when they were compensated with sufficient monetary rewards. In essence, these studies suggest that an individual's privacy-protective behavior is jointly determined by both privacy concerns and some tangible benefits derived from surrendering personal information. Notwithstanding these findings, our understanding on the determinants of privacy-related behavior beyond commercial contexts remains incomplete. Hence, our first motivation is to investigate what drives individuals' privacy-protective behavior in the context of synchronous online social interactions. In particular, we propose that individuals derive certain intangible benefits from such interactions, which is referred to as social rewards in this paper, and that these intangible benefits can be just as compelling as privacy concerns in affecting behavior.

Our second motivation is to unravel the antecedents of privacy concerns and social rewards in the context of synchronous online social interactions. Given the contextual differences between social relationship development and commercial transactions (e.g., the former typically has no monetary compensation), our theoretical framing would need to embrace certain aspects of online social interactions. For example, in developing social relationships, either party can choose to remain anonymous or otherwise (Burgoon et al. 1989); whereas in online commercial transactions, individuals are usually aware of the identity of the seller. In addition, the interaction approach is expected to differ. In synchronous online social interactions, information is constantly being exchanged as the two interactants ask questions or provide answers in a to-and-fro manner. This exchange of information can be misconstrued as invasive and disrespectful if the other party keeps persisting (Peris et al. 2002). In contrast, in online commercial transactions, such negative pursuit is less likely. Even though online merchants often desire to collect more information from consumers, they must ensure that the interaction procedure is professional and seemingly fair. Furthermore, characteristics of the media used in online social interactions are inclined to differ from those of online commercial transactions. For instance, online social interaction sites often focus on enriching information presentation via personalized communication and feedback immediacy, whereas online commercial transactions usually collect factual information through registration or payment forms.

Third, though self-disclosure is typical privacy-protective behavior in social interactions, it has been observed that individuals may occasionally demonstrate alternative behavior, i.e., they might opt to misrepresent information when interacting with others (Joinson et al. 2007). In our study, self-disclosure is defined as giving away *true* personal information whereas misrepresentation is about *falsifying* personal information. It is worth noting that self-disclosure and misrepresentation are independent behaviors. Individuals may disclose extensive information about themselves truthfully and, at the same time, adopt misrepresentation to protect themselves without disrupting the conversation flow.

Essentially, we hope to advance the discourse in this field with a more holistic and comprehensive understanding of privacy trade-off and behavior in synchronous online social interactions. Generally, the objectives of our paper are

(i) to extend the privacy calculus perspective to the context of synchronous online social interactions;

(ii) to discover and examine the antecedents of privacy concerns and social rewards in privacy calculus; and

(iii) to study the strategies that individuals adopt to protect their privacy.

2. Literature Review

2.1. Hyperpersonal Framework

The main thrust of considerable prior research has been on understanding online relationship development, which can be intimate and socially desirable. The hyperpersonal framework offers an approach to understanding the way in which users of mediated communications experience relational intimacy (Walther 1996). Specifically, this framework underscores four aspects of mediated communications, which depict how *senders* select, *receivers* magnify, *channels* promote, and *feedback* facilitates the development of social relationships in the mediated environment. First, as senders, users of mediated communications engage in selective self-presentation involving inspection, editing, and revision of information. Furthermore, because of the provision of limited physical cues, unintended nonverbal behavior and appearance information will not be accidentally transmitted to others. Therefore, users may reallocate their cognitive-behavioral resources to create a favorable impression on others. Second, as receivers, users of mediated communications typically receive reduced physical cues that are essential in constructing initial impressions about partners. Under these conditions, individuals tend to overestimate their similarities and shared norms with others when interacting through mediated channels. Third, the channel underscores issues with regards to how information is communicated between partners, e.g., richness or cue multiplicity of communication channels. Lastly, feedback considers how social relationships can be reinforced by the behavior of others in interactions. By interpreting others' behavior, users establish understanding of the interactions and form expectations of others.

Extant studies have drawn on the hyperpersonal framework in understanding relationship development in the mediated environment. For instance, the sender perspective helps explain the effects of self-awareness on individuals' social attractiveness in instant messaging (Yao and Flanagin 2006) whereas the receiver perspective sheds insights on impression management in teleconferencing (Walther 2007). Channel characteristics and feedback are important in shaping self-presentation behavior in online dating websites (Ellison et al. 2011).

Generally, the hyperpersonal framework identifies four essential aspects of mediated communications, namely, the sender, receiver, channel characteristics, and feedback, which are particularly useful in understanding relationship development.

2.2. Privacy Calculus

Whereas privacy is defined as the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others (Campell 1997), privacy concerns refer to individuals' subjective views of fairness within the context of privacy. Prior IS research has devoted substantial attention to privacy concerns in the contexts of direct marketing, electronic commerce, and online healthcare (Anderson and Agarwal 2011, Malhotra et al. 2004, Smith et al. 1996). Generally, these studies have suggested that privacy concerns lead to individuals being more cautious in handling their personal information. For instance, Son and Kim (2008) found that Internet users who were concerned about information misuse often withheld information about themselves in online transactions. Similarly, Stewart and Segars (2002) examined privacy concerns in the context of direct marketing and found that consumers refused to reveal their financial information to insurance companies when they were concerned about the way their information might be handled.

Researchers have also suggested that individuals are not totally dissuaded by privacy concerns but are willing to relinquish some privacy in return for benefits. In other words, they perform a calculus between the loss of privacy and the potential gain of surrendering their private information, and their final behavior is determined by the outcome of the privacy trade-off. For example, Xu et al. (2009) examined the usage of location-based services and found that privacy concerns deterred individuals from disclosing their locality to the service provider, but monetary incentives made them more willing to be located by the operator. Similarly, Milne and Gordon (1993) found that the provision of personal information for direct marketing services was influenced by the outcome of a cost-benefit analysis in which individuals evaluated the amount of compensation received against the potential risk associated with personal information exposure. Essentially, these studies suggest that individuals perform a privacy calculus in which privacy concerns are weighed against some tangible benefits.

Although tangible compensation (e.g., discounts and rebates) is generally recognized as the benefits of the calculus (Xu et al. 2009), some studies have indicated that certain intangible benefits might be equally relevant in affecting individuals' behavior. For example, Dinev and Hart (2006) found that individuals were more willing to provide personal information for Internet transactions when their interests in the content surpassed privacy concerns. Intangible benefits are particularly important in the context of synchronous online social interactions. This is because the exchange of monetary benefits in social interactions is atypical, if not unprecedented. Rather, individuals are more likely to be attracted by the companionship, approval, and respect that can be derived from participating in a social exchange

(Eisenberger et al. 1990). Indeed, past research suggests that individuals could possibly trade some social commodity (e.g., information privacy) for other benefits as part of a social exchange. This exchange for other benefits becomes part of what is known as a social contract, as individuals have something of value to others and both decide to engage in a mutually agreeable trade (Lawler and Thye 1999). For example, Hemetsberger (2002) found that individuals in virtual communities engaged in collaborative design of digital goods and services to fulfil their social needs such as gaining social approval, social reaffirmation, friendship, or moral support. Occasionally, people socialize in online chat rooms simply to mingle around, relax and enjoy. Chatting with others online in itself may elicit pleasure. Hence, we contend that *social rewards*, which refer to the pleasure, satisfaction, and gratification individuals derive from participating in interpersonal interactions (Eisenberger et al. 1990), are the alternative benefits in synchronous online social interactions. Essentially, these individuals conduct a privacy trade-off, in which privacy concerns are weighed against social rewards, to determine their privacy-protective behavior in online social interactions.

3. Research Model and Hypotheses

By integrating the hyperpersonal framework and privacy calculus perspective, we designed our proposed research model, which is presented in Figure 1. Specifically, we hypothesize the relationships between four distinct aspects of the hyperpersonal framework and the privacy trade-off. We also propose investigating the effects of privacy trade-off on privacy-protective behavior.

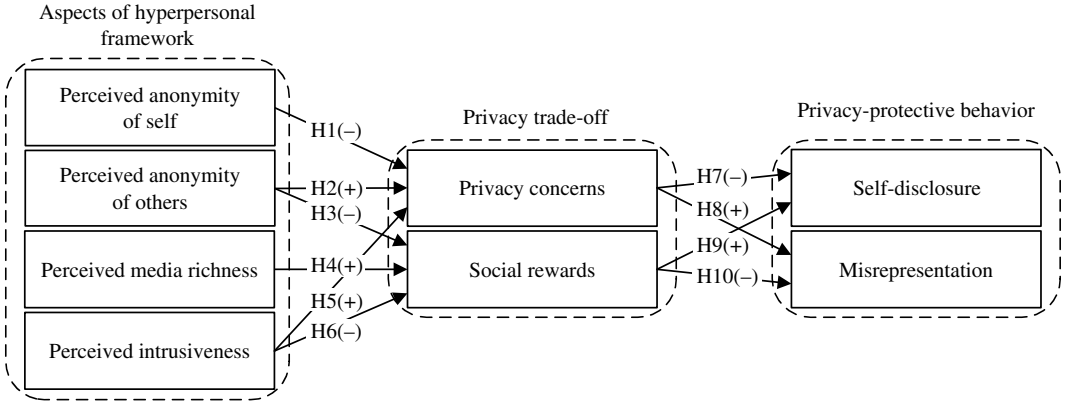
3.1. Hyperpersonal Framework and Privacy Trade-off

This study draws upon the hyperpersonal framework in proposing four antecedents of privacy trade-off, which balances the risks of privacy concerns with the benefits of social rewards. The four antecedents include perceived anonymity of self, perceived anonymity of others, perceived media richness, and perceived intrusiveness. First, according to the hyperpersonal framework, the sender perspective considers the effects of limited identity cues on individuals' impression management. From this perspective, individuals focus on the identity information they have selectively sent to others. In synchronous online social interactions, individuals can largely maintain their anonymity by completely or partially concealing their identity information. Therefore, to reflect the sender perspective, perceived anonymity of self is examined in this study.

Second, the hyperpersonal framework suggests that limited identity cues do not only establish the sender perspective but also play a key role in establishing the receiver perspective. When receiving information, individuals will evaluate the identity information of their communication partners. Because of the lack of physical presence in synchronous online social interactions, the identity information individuals receive from others can often be partial and fragmented. As a result, others can at times remain largely unidentifiable. Therefore, to reflect the receiver perspective, this study examines the impact of perceived anonymity of others.

Third, the hyperpersonal framework posits that characteristics of the communication channel affect information exchange in online social interactions (Walther 1996). Past studies have predominately focused on media richness, which circumscribes the richness of information delivered by the communication medium (e.g., Caplan and Turner 2007, Jiang et al. 2010, Ratan et al. 2010). Furthermore, extant research suggests that media richness facilitates the development of meaningful online relationships (e.g., Dennis et al. 1999, Sheer 2011). In view of the

Figure 1 Research Model



relevance of this channel characteristic, this study examines perceived media richness afforded by the communication channel.

Lastly, Walther (1996) states that individuals interpret others' feedback in social interactions to establish understanding of others, which is essential to developing relationships. In online synchronous social interactions, feedback is manifested in the way personal information is exchanged as others ask questions or provide answers in a to-and-fro manner. In such an exchange, individuals typically maintain a psychological boundary to control access to their private self (Petronio 2002). This psychological boundary is penetrated when individuals provide personal information in response to others' requests. Although allowing others to penetrate this psychological boundary is essential to the development of meaningful online relationships (Gibbs et al. 2006, Kim and Yun 2007), it might also evoke individuals' perception of intrusiveness (Vandebosch and Van Cleemput 2009, Wolak et al. 2007). Therefore, we examine individuals' perceptions of intrusiveness in this study.

3.1.1. Perceived Anonymity of Self. In synchronous online social interactions, individuals may manipulate their anonymity status by revealing or concealing their real names, or using partially or completely fake identities. When perceived anonymity of self is high, individuals may experience deindividuation, which is a state of diminished focus on self and reduced concern for social evaluation (Postmes and Spears 1998). In this case, they will perceive low accountability in their social interactions and possess a sense of immunity (Moral-Toranzo et al. 2007). Conversely, if individuals sense that others know their identity information, they will be held responsible for their online adventures (e.g., Ji and Lieber 2010, Xu et al. 2011).

Hence, if individuals perceive themselves to be unidentifiable in online social interactions, they feel protected against others' ridicules and scrutiny, and will become less concerned about their privacy. Thus we propose the following:

Hypothesis 1 (H1). *Higher perceived anonymity of self will reduce privacy concerns*.[1]

3.1.2. Perceived Anonymity of Others. When other parties are anonymous, it is impossible for individuals to know who they are or hold them accountable for their actions and opinions. Consequently, individuals face greater risks and uncertainty in their synchronous online social interactions. When others refuse means of identification, individuals find it difficult to assimilate enough factual information to better understand others' opinions (Hancock and Dunham 2001). In fact, evidence suggests that individuals who fail to know much about other parties in social interactions, are anxious and paranoid about losing their privacy (e.g., Schoenbachler and Gordon 2002, Viégas 2005). Essentially, past studies suggest that individuals' inability to construct meaningful others exacerbates privacy concerns in online social interactions.

In addition, the other party's identity often serves to justify the information that is requested. For example, if the other party reveals who he or she is (e.g., Mary, a mother of two kids), it does assist in enlightening individuals as to why that other party is always asking about their kids. Otherwise, individuals may erroneously misconstrue that person to be a pedophile with ill intents. When others provide adequate explanations, individuals will become more acceptable and tolerant toward privacy loss (Colquitt 2001). In summary, perceived anonymity of others constantly poses challenges to individuals' privacy concerns. Hence we posit the following:

Hypothesis 2 (H2). *Higher perceived anonymity of others will increase privacy concerns*.

Within the hyperpersonal framework, the identity of the other party provides an important basis for the commencement of online social interactions (Walther 1996). Past research suggests that the identity information of the other party is essential to impression formation in the online environment. Prior to embarking on online synchronous social interactions, individuals occasionally feel uncertain about others (Caplan and Turner 2007). In this case, individuals may find it difficult to develop meaningful relationships with unknown others. In contrast, with knowledge about others' identity, individuals can have better understanding of others, which is imperative to developing online relationships (Joinson 2001). Hence, when others are less anonymous, individuals will find the online synchronous social interaction more socially rewarding (Perreault and Bourhi 1999).

Furthermore, the identity information of others enhances formation of a shared "interlocutory space" (Riva and Galimberti 1998, p. 147). This mutually shared space is critical toward a better appreciation of others. As a result of meaningful communication and interaction, better relationships can be developed. Otherwise, individuals would fail to benefit from the social rewards available in online social interactions. Hence we hypothesize the following:

Hypothesis 3 (H3). *Higher perceived anonymity of others will reduce social rewards*.

[1] Because existing theories and empirical evidence do not hint at a clear causal relationship between perceived anonymity of self and social rewards, we do not hypothesize on them.

3.1.3. Perceived Media Richness. The media richness theory, developed by Daft and Lengel (1986) and Daft et al. (1987), is used to characterize a medium's ability to change understanding within a specific time interval. The theory suggests that the evaluation of the richness of media can be based on four criteria, namely, the multiplicity of information cues, the immediacy of feedback, language variety, and the degree of "personalness." Based on these criteria, various media can be ranked along a media richness continuum, ranging from very rich to very lean. The media richness theory also advocates a media-task fit, i.e., equivocal messages are better communicated using rich media than lean media (McGrath and Hollingshead 1993). Despite some conflicting findings that primarily challenge "the media-task fit," past empirical studies consistently demonstrate the positive effects of rich media on social perceptions. Indeed, the ranking of the richness of media was found to be very similar to the ranking of social presence afforded by media (Carlson and Davis 1998). Evidence also has suggested that increased multiplicity of cues is closely tied to individuals' social communication, interpretation of communication, and gain of consensus (Dennis and Kinney 1998). In summary, past research has suggested that the richness of the communication media would effectively contribute to creating the overall shared meaning and thus lead to a more socially fulfilling experience (Canessa and Riolo 2003). Hence, we posit the following:

Hypothesis 4 (H4). *Higher perceived media richness will increase social rewards*.[2]

3.1.4. Perceived Intrusiveness. In synchronous online social interactions, perceived intrusiveness is of particular importance to developing relationships. Perceived intrusiveness refers to the extent to which individuals perceive unsolicited invasion into their personal space (Burgoon et al. 1989). Past studies suggest that individuals generally erect psychological boundaries around their perception of private-self to ward off public visibility. These boundaries are often penetrated as individuals' personal space is invaded in developing relationships (Gibbs et al. 2006). Although invasion of these boundaries is inevitable in social interactions, others' intrusiveness, in the form of interruption, interference, and harassment, often annoys individuals. Consequently, individuals lose their rights to be left alone and feel susceptible to harm on their private self (Petronio 1991, Woo 2006). Hence, intrusiveness is undesirable and uncalled for. This encroachment on individuals' space and infringement on their personal rights trigger their concerns about privacy (Burgoon et al. 1989). Hence, we posit the following:

Hypothesis 5 (H5). *Higher perceived intrusiveness will increase privacy concerns*.

Relationships are usually developed over time as intimacy progresses with proper social exchange (Lawler and Thye 1999). However, intrusiveness critically upsets the pattern and pace of gradual information exchange with interruption and haste (Petronio 2002). Feeling pestered, pressured, or disrespected, individuals are denied the opportunity to pause, contemplate, and reply accordingly. This hurts online social interactions as conversations evolve into something more confrontational and abrasive. Sometimes, intimate questions are asked prematurely; sometimes, inappropriate questions are asked unwittingly. Whatever the case, intrusiveness is frowned upon, resulting in a less than rewarding social experience.

In addition, intrusiveness would disrupt the equity in synchronous online social interactions. Prior research suggests that imbalances in the exchange of personal information would have dire consequences (Burgoon et al. 1989). High intrusiveness indicates that others are attempting to get more information out of the social interactions, thereby upsetting the balance ensuring stability (Le Poire et al. 1992). When others increase their efforts to gain information over affected individuals, the latter would perceive such synchronous online interactions to be less socially fulfilling. Consequently, this leads to a reduction in social rewards. Hence, we posit the following:

Hypothesis 6 (H6). *Higher perceived intrusiveness will reduce social rewards*.

3.2. Privacy Trade-off and Privacy-Protective Behavior

Extant privacy studies have shed some light on the outcomes of privacy trade-off. For instance, privacy concerns are known to exacerbate cynical perceptions and induce worries about others' opportunism (Milne and Gordon 1993). Consequently, a relationship could be jeopardized (Dinev and Hart 2006). Furthermore, individuals would feel betrayed, thereby inducing a sense of unfairness, inequality, and emotional distress (Culnan and Bies 2003). They would then adopt various behavioral strategies to protect their privacy (Zwick and Dholakia 2004). Although several types of privacy-protective behaviors have been identified in online commercial transactions (e.g., complaints, negative word of mouth, and information removal) (Son and Kim 2008), interpersonal communication studies exemplify the provision of personal information to be the most relevant behavior in synchronous

[2] Because there are no theories or empirical evidence that indicate any possible relationship between perceived media richness and privacy concerns, we do not hypothesize on them.

online social interactions (e.g., Toma and Hancock 2010, Walther 2007). Generally, individuals regulate social interactions by resorting to reducing revelation or opting for deception. Deceptive behavior could help maintain the continuous flow of information in synchronous online social interactions, thereby reducing the chances of irritating others. In summary, the pressure for continuous and rapid information flow in synchronous online social interactions necessitates more immediate responses. Accordingly, this study focuses on two types of individuals' immediate privacy protective-behavior, namely, self-disclosure and misrepresentation.

3.2.1. Privacy Concerns and Self-Disclosure. In this study, self-disclosure refers to the act of revealing *truthful* personal information to others (Wheeless and Grotz 1976). The information can be descriptive and public-self oriented (e.g., name, affiliation, address, etc.) or evaluative and private-self oriented (e.g., religious beliefs, political opinions, etc.). Self-disclosure plays a pivotal role in creating social relationships (Petronio 1991). It is by the gradual disclosure of personal information and the revelation of views and opinions that ambiguities are resolved and understanding is established.

Despite the pertinence of self-disclosure and its accrual benefits, potential risks exist. As self-disclosure often involves highly personal or intimate information, and at times even innermost emotions, attitudes, or feelings, individuals can become vulnerable. Others may misjudge them or react adversely to the information. Furthermore, instead of being the sole owner in absolute possession of the information, others are in possession of it too. Hence they can further disseminate the information and exploit it for marketing solicitations or other misuses (Debatin et al. 2009). Consequently, victims may suffer psychologically, physically, or materially.

Avoiding self-disclosure becomes one of the most common strategies adopted by individuals to protect their privacy (Zwick and Dholakia 2004). In a social interaction, when individuals face privacy threats, such as the unauthorized use, modification or dissemination of their private information, they can lessen their exposure to others simply by deciding not to disclose personal information. This is especially so in the case of synchronous online social interactions, where the communication is electronic and easily terminated or avoided. Generally, great privacy concerns indicate a lack of confidence in the reliability and integrity of others, and this inevitably leads to a corresponding reduction in self-disclosure, because the potential risks to individuals are substantial. Hence we posit the following:

Hypothesis 7 (H7). *Greater privacy concerns will lead to less self-disclosure*.

3.2.2. Privacy Concerns and Misrepresentation. Even though potential risks may diminish any desire for self-disclosure, individuals are occasionally denied the opportunity to withhold information in order to proceed with an interaction. For example, in online commercial transactions, it is mandatory for them to supply information that is designated as a compulsory field to complete membership registration. In synchronous online social interactions, the continuous flow of conversations may induce in individuals, faced with a lack of choice, the need to provide some falsified information.

Misrepresentation of information refers to the act of creating and conveying false information to others (Argo et al. 2006), regardless of its intent, be it to mislead, to deceive, or simply for fun. Consequently, misrepresentation can facilitate self-protection and self-presentation (Joinson et al. 2007). For example, in response to others' requests for contact information, individuals might fabricate such information to reduce their vulnerability to others' opportunistic behavior. Individuals might also lie about their appearance and ability so as to make a positive impression on others if they have no wish to reveal their actual physical appearance and competency. In addition, misrepresentation enables individuals who are concerned about their privacy to temporarily placate or satisfy others, thereby maintaining the flow of interactions. Based on these arguments, misrepresentation is used in synchronous interactions when individuals have to sustain a conversation but do not desire to disclose much private information. Thus, we posit the following:

Hypothesis 8 (H8). *Greater privacy concerns will lead to greater misrepresentation*.

3.2.3. Social Rewards and Self-Disclosure. In social interactions, individuals are bound by the norms of reciprocity to engage in a fair exchange of information (Lawler and Thye 1999). In particular, open and sincere self-disclosure forms the basic tenet of maintaining an intimate and rewarding relationship (Ben-Ze'ev 2003). When individuals perceive a relationship to be rewarding, they will make greater efforts to maintain or further develop the relationship. In particular, it is found that the more individuals consider others' responses to be understanding (i.e., understanding the speaker's needs, feelings, and situations), validating (i.e., confirming that the speaker is accepted and valued), and caring (i.e., showing affection and concern for the speaker), the more the individuals would be inclined to indicate that they value the social bond (Schimel et al. 2001). Other empirical findings also support this proposition. Tidwell and Walther (2002), for example, examined the exchange of personal information in computer-mediated communication and found

that individuals revealed their personal beliefs, needs, and values to others with whom they have socially rewarding relationships. Indeed, in a social exchange, self-disclosure is expected when individuals return favors received from others (Lawler and Thye 1999). Consequently, individuals are more likely to increase their self-disclosure toward the source of the rewarding relationship because they benefit from doing so. Hence we posit the following:

Hypothesis 9 (H9). *Greater social rewards will lead to greater self-disclosure.*

3.2.4. Social Rewards and Misrepresentation. Social rewards and misrepresentation are negatively related. Individuals who perceive greater social rewards will refrain from misrepresentation because of potential repercussions and costs (Burgoon et al. 1989). Specifically, as misrepresentation is perceived to violate the mutual agreement of openness and authenticity with others (Argo et al. 2006), its discovery may bring about undesired or even disastrous consequences. Because social rewards in the form of a long-term relationship necessitate truthfulness, individuals cannot afford to misrepresent and mislead. Apart from these deterrents, individuals are also prone to refraining from misrepresentation because of their inclination to uphold interpersonal fairness and equal contributions (Colquitt 2001). By ensuring propriety in interactions, individuals demonstrate their respect for one another. In summary, individuals are less willing to risk violating the exchange norms and interaction protocols when they are in a more rewarding relationship. Hence, they are less likely to misrepresent. Thus we posit the following:

Hypothesis 10 (H10). *Greater social rewards will lead to less misrepresentation.*

4. Research Methodology

Online chat rooms were selected to test our research model inasmuch as chat rooms are reported to be one of the main socialization channels for individuals (Peris et al. 2002) as well as a cyberspace where users are often plagued by privacy issues (e.g., Finn 2004). Prior to the main study, we conducted three rounds of preliminary tests to compare and evaluate different methods of data collection (see Appendix A).

Addressing all the issues revealed in the preliminary tests, we conducted our main survey. Respondents were students from a public university in Singapore. The rationale for using student samples was to exemplify those who often use online chat rooms (IDA 2007).[3]

[3] In a study on Internet users, IDA (2007) found that "14% of 15-year-old to 24-year-old users said they communicated via online chat rooms, but less than half as many, only 5% of the next age bracket (25- to 34-year-old) said they had done this" (p. 37).

An email invitation was sent to 768 students who had been randomly selected from the email directory of the university. They were notified that participation was voluntary and they would be rewarded with 25 Singapore dollars each. The registration system captured their demographic information, Internet experience, and general chat room experience. A total of 251 students volunteered to participate. The average age of the subjects was 22.5 and 51% were female.

The study was completed in three weeks, comprising three chat sessions, with each lasting an hour. In the period between these sessions, participants were also encouraged to use the chat room for further social interactions. Thus, they were allowed sufficient time to become familiarized with the allocated chat room and to develop social relationships.[4] At the end of the third chat session, a survey was conducted to measure all research variables. All survey items were measured on a 7-point Likert scale (see Appendix B). We were concerned that the results of the survey could be confounded by multiple interaction episodes. For example, a respondent might be answering questions on perceived anonymity of self based on a particular experience whilst answering questions on perceived anonymity of others based on an entirely unrelated experience. Hence, it was decided that respondents would be first instructed to recall a specific experienced incident and that all their responses to the research variables should be based on that particular experience.

5. Data Analyses and Results

5.1. The Measurement Model

The partial least squares (PLS) regression was used to test the research model. The measurement model was assessed by examining (1) individual item reliability, (2) internal consistency, and (3) discriminant validity (Barclay et al. 1995).

Measurement item factor loadings are presented in Table 1. To measure privacy concerns, we used the Internet Users' Information Privacy Concerns (IUIPC) scale, which captures privacy concerns as a second-order variable with three first-order factors, namely, awareness, collection, and control (Malhotra et al. 2004). Following Chin (1998), we computed three sets of factor scores based on the three first-order constructs. These three factor scores were then considered as indicator variables for privacy concerns. Because

[4] To enhance the generalizability of our results, respondents were randomly assigned to one out of five popular online chatrooms. The chatrooms were selected randomly from the Yahoo! Directory (figures in square brackets refer to the ratio of the number of survey participants in a chat room over total concurrent chat room users): (i) SpinChat [9.4%], (ii) ICQ [9.2%], (iii) JustaChat [6.0%], (iv) TalkCity [6.8%], (v) Yahoo!Chat [10.2%].

Table 1 Item Loadings and Cross-Loadings

	PAS	PAO	PMR	PI	PC	SR	SD	MIS
PAS1(*r*)	**0.88**	0.34	0.04	−0.09	0.23	0.00	0.04	0.00
PAS2(*r*)	*0.46*(*)	0.51	0.06	−0.14	0.03	−0.01	−0.05	−0.07
PAS3	**0.90**	0.49	0.14	−0.08	0.23	0.04	0.03	−0.01
PAO1(*r*)	0.41	**0.88**	−0.07	−0.06	0.18	−0.14	−0.11	−0.07
PAO2(*r*)	0.33	**0.81**	−0.05	−0.07	0.21	−0.23	−0.26	−0.11
PAO3	0.51	**0.81**	0.03	−0.12	0.27	−0.04	−0.05	−0.10
PMR1	0.12	−0.04	**0.84**	−0.28	−0.02	0.39	0.18	−0.12
PMR2	0.14	−0.04	**0.91**	−0.29	−0.09	0.38	0.20	−0.10
PMR3	0.01	0.02	**0.74**	−0.17	−0.03	0.23	0.14	−0.07
PMR4	0.00	−0.02	**0.76**	−0.20	−0.06	0.27	0.13	−0.12
PI1	−0.09	−0.07	−0.28	**0.93**	0.25	−0.45	−0.32	0.48
PI2	−0.10	−0.07	−0.29	**0.94**	0.25	−0.46	−0.28	0.48
PI3	−0.11	−0.13	−0.25	**0.92**	0.25	−0.40	−0.29	0.47
PI4	−0.08	−0.05	−0.31	**0.93**	0.29	−0.46	−0.31	0.49
PI5	−0.10	−0.10	−0.28	**0.92**	0.24	−0.42	−0.29	0.47
PC-AWA	0.21	0.20	−0.09	0.32	**0.96**	−0.13	−0.23	0.17
PC-COL	0.27	0.26	−0.05	0.24	**0.97**	−0.06	−0.17	0.08
PC-CON	0.26	0.30	−0.04	0.23	**0.96**	−0.09	−0.19	0.10
SR1	−0.05	−0.18	0.38	−0.40	−0.08	**0.92**	0.49	−0.19
SR2	0.04	−0.19	0.42	−0.47	−0.12	**0.96**	0.48	−0.26
SR3	0.07	−0.13	0.34	−0.44	−0.08	**0.92**	0.52	−0.22
SD1	0.05	−0.09	0.18	−0.26	−0.18	0.48	**0.77**	−0.17
SD2	0.01	−0.19	0.13	−0.15	−0.16	0.42	**0.83**	−0.03
SD3	0.08	−0.07	0.16	−0.33	−0.14	0.45	**0.83**	−0.21
SD4	0.07	−0.09	0.19	−0.32	−0.20	0.46	**0.88**	−0.23
SD5	−0.05	−0.25	0.20	−0.26	−0.21	0.46	**0.86**	−0.09
MIS1	0.00	−0.09	−0.18	0.52	0.11	−0.26	−0.18	**0.94**
MIS2	−0.03	−0.13	−0.08	0.46	0.13	−0.22	−0.17	**0.95**
MIS3	0.00	−0.11	−0.11	0.46	0.11	−0.20	−0.13	**0.92**

Notes. 1. PAS = perceived anonymity of self; PAO = perceived anonymity of others; PMR = perceived media richness; PI = perceived intrusiveness; PC = privacy concerns; SR = social rewards; SD = self-disclosure; MIS = misrepresentation.
2. (*) Item deleted.
3. (*r*) Reverse item.
4. Items under awareness (PC-AWA), collection (PC-COL), and control (PC-CON) constitute the 10-item second-order IUIPC scale.

one of the items measuring perceived anonymity of self (i.e., PAS2) had a low loading of 0.46, it was omitted. Because all remaining item loadings were above 0.7, the requirement for individual item reliability was met (Barclay et al. 1995, Chin 1998). In addition, the composite reliabilities of the different measures ranged from 0.87 to 0.98 (see Table 2), thus indicating high internal consistency.

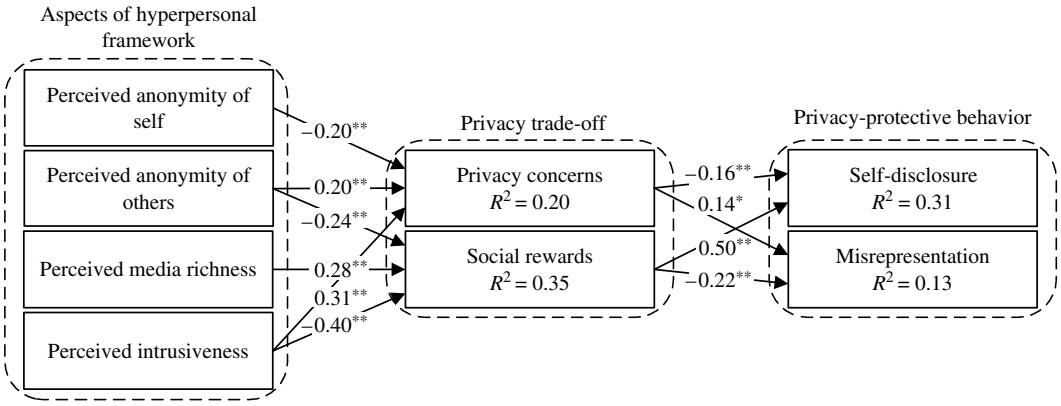
The next step in assessing the measurement model involved examining its discriminant validity. For adequate discriminant validity, loadings of indicators on their respective latent variables should be higher than loadings of other indicators on these latent variables and the loadings of these indicators on other latent variables. The loadings and cross-loadings presented in Table 1 demonstrate adequate discriminant validity.

Table 2 Reliabilities, Correlation Matrix, and Square Roots of Average Variance Extracted

	Mean	Standard deviation	Composite reliability	PAS	PAO	PMR	PI	PC	SR	SD	MIS
PAS	4.64	0.93	0.88	**0.89**							
PAO	4.93	1.05	0.87	−0.47	**0.84**						
PMR	4.53	1.26	0.89	−0.10	−0.03	**0.81**					
PI	4.10	1.75	0.96	0.10	−0.10	−0.30	**0.93**				
PC	5.31	0.95	0.98	−0.26	0.26	−0.06	0.27	**0.96**			
SR	4.11	1.50	0.96	−0.02	−0.18	0.40	−0.47	−0.10	**0.94**		
SD	3.39	1.28	0.91	−0.04	−0.18	0.20	−0.32	−0.21	0.53	**0.85**	
MIS	3.26	1.64	0.96	0.01	−0.12	−0.13	0.51	0.12	−0.24	−0.17	**0.94**

Notes. PAS = perceived anonymity of self; PAO = perceived anonymity of others; PMR = perceived media richness; PI = perceived intrusiveness; PC = privacy concerns; SR = social rewards; SD = self-disclosure; MIS = misrepresentation.

Figure 2 Research Model Results (Completely Standardized Solutions)



Note. All paths are significant.
$^{*}p < 0.05$, $^{**}p < 0.01$ (two-tailed).

Another criterion for adequate discriminant validity requires that the square roots of average variances extracted (AVE) of any latent variable be greater than the correlations shared between the latent variable and other latent variables (Barclay et al. 1995). Off-diagonal elements in Table 2 represent correlations of all latent variables, and the diagonal elements are the square roots of the AVE of the latent variables. Data shown in Table 2 therefore satisfy this requirement.

5.2. The Structural Model

The results of the structural model are presented in Figure 2. All 10 hypotheses are supported. Perceived anonymity of self is found to be negatively related to privacy concerns ($\beta = -0.20$, $p < 0.01$), therefore H1 is supported. Consistent with our prediction, perceived anonymity of others is positively related to privacy concerns ($\beta = 0.20$, $p < 0.01$) but negatively related to social rewards ($\beta = -0.24$, $p < 0.01$), thus supporting H2 and H3. As anticipated, perceived media richness exhibits a positive influence on social rewards ($\beta = 0.28$, $p < 0.01$), hence supporting H4. Both H5 and H6 are also supported as perceived intrusiveness exhibits a positive relationship with privacy concerns ($\beta = 0.31$, $p < 0.01$), but a negative relationship with social rewards ($\beta = -0.40$, $p < 0.01$).

In addition, privacy concerns are found to have a negative impact on self-disclosure ($\beta = -0.16$, $p < 0.01$) but a positive impact on misrepresentation ($\beta = 0.14$, $p < 0.05$), and hence both H7 and H8 are supported. Conversely, social rewards have a positive impact on self-disclosure ($\beta = 0.50$, $p < 0.01$) but a negative impact on misrepresentation ($\beta = -0.22$, $p < 0.01$), thus supporting both H9 and H10.[5]

Sobel tests (Sobel 1982) were next conducted to examine whether privacy concerns and social rewards fully mediate the effects of the four independent variables (i.e., perceived anonymity of self, perceived anonymity of others, perceived media richness, and perceived intrusiveness) on the two dependent variables (i.e., self-disclosure and misrepresentation).[6] The results indeed confirm such mediation effects, with one exception. Although the effect of perceived intrusiveness on misrepresentation is mediated by privacy trade-off in general, this mediation is realized mainly through privacy concerns (Sobel $Z = 2.78$, $p < 0.05$) rather than social rewards (Sobel $Z = 0.20$, $p =$ n.s.). A plausible explanation is that when individuals consider misrepresentation, perceived intrusiveness alerts them about others' unsolicited invasions, which prime the costs in privacy trade-off and hardly emphasize the benefits individuals derive from the interaction. As such, social rewards do not come into play in mediating the impact of perceived intrusiveness on misrepresentation. Nonetheless, our results indicate that privacy concerns and social rewards, as a whole, mediate the effects of the four antecedents on self-disclosure and misrepresentation.

5.3. Common Method Bias

Following the recommendation of Podsakoff et al. (2003), we tested for possible common method bias by conducting confirmatory factor analysis (CFA) for two models. First, a 10 factor model was estimated, which

[5] To ensure that our findings are not confounded by other variables, we controlled for the possible effects of gender, age, Internet experience, general chat room experience, chat room allocation, usage frequency, and moral beliefs toward misrepresentation (Beck and Ajzen 1991). All control variables, except moral beliefs toward misrepresentation, have an insignificant impact on the endogenous variables (see Appendix C). Moral beliefs are found to have a significant negative effect on misrepresentation ($\beta = -0.20$, $p < 0.01$). This could be likely because individuals who consider misrepresentation as a moral violation are likely to refrain from misrepresenting themselves in synchronous online social interactions.

[6] Appendix D shows detailed results of the Sobel tests.

included eight constructs in the research model with privacy concerns consisting of three first-order factors.[7] Each of the 35 measurement items was restricted to being an indicator for the respective latent factor. Fit indices of the first model ($\alpha^2(515) = 505.94$) were as follows: $\alpha^2/\text{df} = 1.02$, SRMR = 0.463, RMSEA = 0.019, NFI = 0.952, CFI = 0.996, GFI = 0.905, AGFI = 0.864, TLI = 0.994. Generally, these indices satisfied the recommended thresholds[8] and hence indicate a good fit of the model to the data.

In the second model, in addition to the 10 factors examined in the first model, we conducted a CFA with one additional factor to represent the unmeasured common method. Each of the 35 items was allowed to load on its respective theoretical factor construct, and all were allowed to load on the additional methods factor, which was constrained to be uncorrelated with the other 10 factors. The fit indices for the second model ($\alpha^2(513) = 505.90$) were largely identical to those of the first model ($\alpha^2/\text{df} = 1.01$, SRMR = 0.463, RMSEA = 0.020, NFI = 0.952, CFI = 0.996, GFI = 0.905, AGFI = 0.864, TLI = 0.994). Furthermore, a chi-square test comparing the first model with the second model indicated that the difference between the two models was not significant ($\alpha^2(2) = 0.04$, $p =$ n.s.), suggesting that the common method bias was not a serious concern.

6. Discussion and Conclusion

6.1. Discussion of Results

The results supported all our hypotheses. Our research objective was to provide a more holistic understanding of privacy-related behavior by extending the privacy calculus perspective (Dinev and Hart 2006) to the context of synchronous online social interactions. We established that as a result of the contention between privacy concerns and social rewards, individuals do engage in both self-disclosure and misrepresentation. We also attempted to achieve a more comprehensive understanding of online synchronous social interaction by examining constructs that are derived from the four aspects of the hyperpersonal framework, namely, sender's perspective, receiver's perspective, channel characteristics, and feedback (Walther 1996). Our findings confirm that constructs derived from these four aspects are important antecedents of privacy concerns and social rewards.

6.2. Theoretical and Practical Contributions

We enrich privacy-related studies with several fresh insights. First, we contribute to the IS literature by identifying antecedents of privacy concerns and social rewards in synchronous online social interactions. Despite the prevalence of privacy research, extant studies have yielded scanty evidence on the causes of these trade-offs beyond commercial contexts. Based on the hyperpersonal framework (Walther 1996), this study investigates four antecedents of privacy concerns and social rewards, namely, perceived anonymity of self, perceived anonymity of others, perceived media richness, and perceived intrusiveness. On the one hand, these antecedents represent typical causes of privacy concerns in online synchronous social interactions. Specifically, perceived anonymity of self depicts the sender perspective, highlighting how individuals' limited identity cues induce a sense of immunity in the online environment (Postmes and Spears 1998). Perceived anonymity of others accounts for the receiver perspective, explaining how others' fragmented identity information renders them unaccountable in online synchronous social interactions (Viégas 2005). Perceived intrusiveness describes how feedback penetrates individuals' psychological boundary, which makes them feel susceptible to harm on their private selves (Kim and Yun 2007). On the other hand, the antecedents also represent important determinants of social rewards in online synchronous social interactions. In particular, perceived anonymity of others explicates the receiver perspective, demonstrating that individuals' perception of others is typically limited by fragmented identity cues (Caplan and Turner 2007). Perceived media richness depicts how the channel affects information exchange in online synchronous social interactions (Canessa and Riolo 2003). Perceived intrusiveness focuses on the way feedback upsets the pattern and pace of online social interactions (Petronio 2002). Holistically, our four antecedents of privacy concerns and social rewards, which are based on the hyperpersonal framework and literature on privacy and online social interactions, are particularly important and relevant to online synchronous social interactions.

Second, we also present new insights to prior privacy-related studies by extending the privacy calculus lens to the context of synchronous online social interactions. We argue that privacy concerns alone

[7] The 10 factors are perceived anonymity of self, perceived anonymity of others, perceived media richness, perceived intrusiveness, social rewards, self-disclosure, misrepresentation; as well as the three first-order IUIPC factors, namely, collection, control, and awareness.

[8] The fit indices criteria for an acceptable model are as follows: below 3 for α^2/df, below 0.05 for standardized root mean square residual [SRMR], below 0.06 for root mean square error of approximation [RMSEA], above 0.90 for normed fit index [NFI], above 0.95 for comparative fit index [CFI], above 0.90 for goodness-of-fit index [GFI], above 0.80 for adjusted goodness-of-fit index [AGFI], and above 0.90 for Tucker-Lewis Index [TLI] (Gefen et al. 2000, Hu and Bentler 1999, Tucker and Lewis 1973).

lack sufficient power to fully explain self disclosure behavior in online social interactions, as in the case of individuals who express privacy concerns, yet reveal private information to strangers (Ben-Ze'ev 2003). We have advocated and attested the role of social rewards as the intangible benefits individuals derive from synchronous online social interactions. This finding is vital because past research has predominantly applied the privacy calculus to commercial contexts. Given that synchronous online social interaction sites (or similar sites) do not promise any pecuniary or fiscal rewards, some researchers may question the applicability of the theory. As a consequence of our analyses, the effects of contextual differences on individuals' privacy-related behavior (see Smith et al. 1996, Stewart and Segars 2002) can now be better comprehended. Essentially, in the absence of monetary or tangible rewards, social rewards are just as attractive in balancing privacy concerns and governing individuals' behavior.

Third, we argue against the propositions of some extant studies that view disclosure and nondisclosure as the only two possible actions stemming from privacy protection in the context of synchronous online social interactions (Petronio 1991). Instead, we establish the presence of misrepresentation as well as its prevalence. The correlation ($r = -0.17$) between self-disclosure and misrepresentation was considered small (Cohen 1992). This suggests that the two types of behavior do not essentially contradict each other as one might presume. Adding to our findings on misrepresentation, we also dispel two misconceptions on misrepresentation. Often, individuals tend to misconstrue misrepresentation as being very negative and anti-normative, relating it to certain undesirable behavior with malicious intent (Argo et al. 2006). Instead, we argue that individuals do engage in misrepresentation as a protective measure, and not necessarily with the intention to harm or hurt. Furthermore, individuals often do not consider misrepresentation as a nonoptional protective measure, but rather as a strategy deployed to provide some data despite privacy concerns (e.g., in registration on websites). Our study suggests that individuals do misrepresent themselves even in the face of an option, such as the option of non self-disclosure (e.g., in online chatrooms). Despite this availability of choice, individuals prefer to provide falsified information. In summary, our study has provided more understanding on these two privacy-related behaviors, i.e., self-disclosure and misrepresentation.

Fourth, prior studies have failed to recognize that "anonymity of self" and "anonymity of others" may exert different influences. By subsuming these two constructs into one construct (i.e., "anonymity") (e.g., Lea et al. 2001), many researchers have failed to acknowledge the possible asymmetry of information. Individuals could choose to remain anonymous whilst others are identifiable, and vice versa. Based on our study, perceived anonymity of self is important to only privacy concerns whereas perceived anonymity of others is crucial to both privacy concerns and social rewards. Hence, the "self" and "others" perspectives of anonymity have fundamentally different roles in online social interactions.

6.3. Limitations and Future Research Directions

We acknowledge some limitations in this study. First, we did not monitor the actual conversation content that transpired between the respondents and those in actual online chatrooms. Neither could we dictate how much the respondents had actually communicated during their synchronous online social interactions. Although respondents' actual involvement in social interactions may vary, we attempted to mimic real-life interactions, by including any possible kind of conversations and interacting patterns. Second, our findings are best generalized to average users in synchronous online social interactions. Indeed, our model assumes that deceptive behavior is not essentially driven by malicious motivations, such as cyberbullying and Internet predation. Malevolent individuals could exhibit vastly different behavior because of their insidious motives. Despite this inadequacy, our model strives to be applicable to the general population, explaining what drives their self-disclosure and misrepresentation.

Third, although one of the path coefficients affecting misrepresentation ($\beta = 0.14, p < 0.05$) and the explained variance of misrepresentation ($R^2 = 0.13$) may not be very large, our results are valid. Indeed, past research involving actual behavior has reported similar path coefficients and explained variances. For example, Pavlou and Gefen (2004) examined self-reported transaction behavior in online marketplaces and reported a path coefficient of 0.10 and an explained variance of 10%. Likewise, in a study of actual purchase behavior, Verhoef (2003) reported a path coefficient of 0.14 and an explained variance of 12%. Hence, our results are comparable to prior studies and are thus valid.

As an extension of our study, we propose several future directions worthy of pursuit. First, there is value in investigating "objective" measures of self-disclosure and misrepresentation, as opposed to our current reflective self-reported measurements. It is possible that individuals' recall may not completely

reflect their actual behavior because of the social desirability bias, which is the tendency for individuals to portray themselves in a generally favorable light (Holden 1994). In view of this potential bias, a further investigation of actual self-disclosure and misrepresentation by analyzing communication protocols could be a future research avenue.

Furthermore, this study examines the causes of and reactions to privacy concerns and social rewards in a synchronous online social interaction context. It is likely that individuals may behave differently if asynchronous communication is used (e.g., Facebook). For example, individuals typically interact with others who are already known in asynchronous social interactions but interact with both known and unknown others in synchronous interactions. In addition, considering that individuals are not pressured into upholding a communication flow in an asynchronous environment, they may react differently to intrusive communication. Moreover, there are also some social interaction features (e.g., tagging) that are available on asynchronous platforms but not on synchronous sites. Generally, we believe all these issues deserve special attention in future research and our theoretical perspective of integrating the hyperpersonal framework and privacy calculus can be instrumental to these potential studies.

Acknowledgments
The authors thank the Senior Editor Prof. Elena Karahanna, the Associate Editor, and the three reviewers for their very constructive comments on this paper. Ben C. F. Choi serves as the corresponding author of the paper. The authors also thank the Ministry of Education (MOE) of Singapore [Grant: MOE2009-T2-1-062] for its financial support.

Appendix A. Preliminary Tests of Different Survey Methods

Three rounds of preliminary tests were conducted to compare and evaluate data collection methods. Several issues were revealed. In the first round, we sought realism by soliciting participation from existing online chatrooms. Recruitment messages were broadcast in selected public chatrooms that directed interested users to a questionnaire hosted on a well-known online survey website.[9] Although such a sampling method could utilize chat room users' actual experiences, it was challenging to recruit participants. This was because many users treated such recruitment messages as a "nuisance" or "spam" and some were even concerned that the posted URL link might direct them to malicious sites. Consequently, this method suffered from poor participation. Furthermore, a scan of the questionnaire responses showed that a considerable proportion of respondents did not devote sufficient thought and care to their answers. For example, many of them provided the same answers (e.g., an indication of "4" for all questions on a 7-point Likert scale). Hence, this first attempt was considered unsuccessful.

To encourage participation and improve the quality of data collected, we conducted a second round of testing. This time, we recruited participants from a public university. Thirty-two participants were invited to a computer laboratory. Instead of partaking in online chat sessions, they were asked to recall and describe any privacy-related experience that they had online. Based on the incident, they filled up a questionnaire. This method suffered from another problem, i.e., our post-survey interviews revealed that most participants were unable to recall a particular online chat experience because of the lack of recency. Hence, the responses gathered did not accurately reflect their perceptions over a particular interaction, but several possibly unrelated privacy episodes that they could recall.

To resolve this issue on recall, we conducted a third round of testing. Participants were asked to perform an online chat in an assigned public chat room prior to answering the online questionnaire. Although this method resolved issues identified in the previous tests, two additional issues surfaced. First, some participants expressed a lack of familiarity with the allocated chat rooms, resulting in much time and effort spent on familiarizing themselves rather than engaging in social interactions. Second, most participants reported that a single session was inadequate for the development of meaningful social relationships or to encounter any privacy concerns. Bearing in mind all the lessons learned from the three preliminary tests, we embarked on our main study.

Appendix B. Measurement Items

All items are based on a 7-point Likert scale (1 = strongly disagree to 7= strongly agree).

Perceived anonymity of self (PAS): adapted from Pinsonneault and Heppel (1997)

(1) Prior to this particular experience, I believe the other party knew about me. (*r*)

(2) Prior to this particular experience, I believe that it was possible for the other party to trace my true identity through my IP address or my chat history. (*r*)*

(3) Prior to this particular experience, I believe I was anonymous to the other party.

Perceived anonymity of others (PAO): adapted from Pinsonneault and Heppel (1997)

(1) Prior to this particular experience, I knew about the other party. (*r*)

(2) Prior to this particular experience, it was possible for me to trace the identity of the other party through the IP address or chat history. (*r*)

(3) Prior to this particular experience, the other party was anonymous to me.

Perceived media richness (PMR): **adapted from Carlson and Zmud (1999)**

(1) I believe that the online chat room I was using allowed me and the other party to communicate through a

[9] http://www.surveyconsole.com

variety of different cues (such as emotional tone, attitude, or formality) in our messages.

(2) I believe that the online chat room I was using allowed me and the other party to use rich and varied language (such as numeric data, pictures, or nonword expressions that have meanings) in our interaction.

(3) I believe that the online chat room I was using allowed me and the other party to tailor (customize) our messages to our own personal requirements.

(4) I believe that the online chat room I was using allowed me and the other party to give and receive timely feedback.

Perceived intrusiveness (PI): adapted from Burgoon et al. (1989)

(1) I felt that the other party was intrusive.

(2) The other party asked me questions that I felt intruded on my privacy.

(3) The other party was overly persistent in getting me to respond.

(4) The other party did not respect my need for personal space.

(5) I felt that the other party was harassing me during the interaction.

Privacy concerns: adapted from Malhotra et al. (2004)

Awareness (*PC-AWA*)

(1) In the particular experience, I believed the other party should disclose reasons for wanting my personal information.

(2) In the particular experience, I believed it was important that I was aware of and had knowledgeable about how the other party would use personal information that I had disclosed to him or her.

(3) In the particular experience, I believed that the privacy policy of the online chat room I was using should be clear and conspicuous.

Collection (*PC-COL*)

(1) In the particular experience, I thought twice when the other party asked me for personal information.

(2) In the particular experience, it bothered me when my online chat partner asked me for personal information.

(3) In the particular experience, I was concerned that the other party was trying to collect too much information from me.

(4) In the particular experience, I believed that giving away personal information to my online chat partner could threaten my privacy.

Control (*PC-CON*)

(1) In the particular experience, my privacy was really a matter of my right to exercise control and autonomy over how my information was collected, used, and shared by the other party.

(2) In the particular experience, the control of my personal information lay at the heart of my privacy.

(3) In the particular experience, my privacy was invaded when control over my personal information was lost or unwillingly reduced.

Social rewards (SR): based on Eisenberger et al. (1990) and Gilbert and Horenstein (1975)

(1) In the particular experience, I believed that the interaction would fulfill my social needs (for example, companionship, approval, acceptance, respect, status) in some way.

(2) In the particular experience, I believed that the interaction would help me cultivate a good relationship with the other party.

(3) In the particular experience, I believed that I could derive satisfaction from interacting with the other party.

Self-disclosure (SD): adapted from Wheeless and Grotz (1976)

(1) In the particular experience, I revealed a great amount of information about myself to the other party.

(2) In the particular experience, I gave out intimate information to the other party.

(3) In the particular experience, I shared a variety of information about myself to the other party.

(4) In the particular experience, I disclosed information openly to the other party.

(5) In the particular experience, I revealed very personal thoughts, feelings and experiences to the other party.

Misrepresentation (MIS): developed from Nichols and Greene (1997)

(1) In the particular experience, I deliberately lied about myself to the other party.

(2) In the particular experience, I deliberately gave inaccurate information about myself to the other party.

(3) In the particular experience, I intentionally gave the other party a false impression about myself.

Notes

(1) *Item deleted.

(2) (*r*) reverse item.

(3) Privacy concerns are analyzed as a second-order latent variable. Factors scores are first computed by constructing first-order latent variables and related to their respective block of manifest variables (i.e., Awareness: PC-AWA1 to PC-AWA3, Collection: PC-COL1 to PC-COL4, and Control: PC-CON1 to PC-CON3). Subsequently, the second-order latent variable is constructed by relating them to the blocks of the underlying first-order latent variables (i.e., PC-AWA, PC-COL, and PC- CON).

Appendix C. Path Coefficients of Control Variables

	GEN	AGE	IE	GCE	CA	UF	MB
Privacy concerns	0.05	0.02	−0.02	0.03	0.02	0.07	0.11
Social rewards	0.01	−0.04	−0.04	−0.06	0.02	0.03	0.04
Self-disclosure	0.05	−0.03	−0.05	−0.01	0.04	−0.03	0.05
Misrepresentation	−0.10	−0.03	0.06	−0.08	0.03	−0.04	−0.20**

Notes. GEN = gender; AGE = age; IE = internet experience; GCE = general chat room experience; CA = chat room allocation; UF = usage frequency; MB = moral beliefs toward misrepresentation.

**$p < 0.01$ (two-tailed).

Appendix D. Sobel Test Results

	Self disclosure		Misrepresentation	
	Sobel Z	Mediation	Sobel Z	Mediation
PAS				
Privacy concerns	−2.32*	Yes	2.48*	Yes
Social rewards[a]	—	—	—	—
PAO				
Privacy concerns	−2.10*	Yes	2.41*	Yes
Social rewards	−2.53*	Yes	2.45*	Yes
PMR				
Privacy concerns[b]	—	—	—	—
Social rewards	4.37**	Yes	−2.20*	Yes
PI				
Privacy concerns	−2.99**	Yes	2.78*	Yes
Social rewards	−4.19**	Yes	0.20	No

Notes. PAS = perceived anonymity of self; PAO = perceived anonymity of others; PMR = perceived media richness; PI = perceived intrusiveness.
[a]No hypothesized relationship between perceived anonymity of self and social rewards.
[b]No hypothesized relationship between perceived media richness and privacy concerns.
*$p < 0.05$, **$p < 0.01$.

References

Anderson CL, Agarwal R (2011) The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Inform. Systems Res.* 22(3):469–490.

Argo JJ, White K, Dahl DW (2006) Social comparison theory and deception in the interpersonal exchange of consumption information. *J. Consumer Res.* 33(1):99–108.

Barclay D, Higgins C, Thompson R (1995) The partial least squares approach to causal modeling: Personal computer adoption and use as an illustration. *Tech. Stud.* 2(2):285–324.

Beck L, Ajzen I (1991) Predicting dishonest actions: Using the theory of planned behavior. *J. Res. Personality* 25(3):285–301.

Ben-Ze'ev A (2003) Privacy, emotional closeness, and openness in cyberspace. *Comput. Human Behav.* 19(4):451–467.

Burgoon JK, Parott R, Le Poire BA, Kelley DL, Walther JB, Perry D (1989) Maintaining and restoring privacy through communication in different types of relationships. *J. Soc. Personal Relationships* 6(2):131–158.

Campell AJ (1997) Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *J. Direct Marketing* 11(3):44–57.

Canessa E, Riolo RL (2003) The effect of organizational communication media on organizational culture and performance: An agent-based simulation model. *Computational Math. Organ. Theory* 9(2):147–176.

Caplan SE, Turner JS (2007) Bringing theory to research on computer-mediated comforting communication. *Computers in Human Behav.* 23(2):985–998.

Carlson JR, Zmud RW (1999) Channel expansion theory and the experiential nature of media richness perceptions. *Acad. Management J.* 42(2):153–170.

Carlson PJ, Davis GB (1998) An investigation of media selection among directors and managers: From "self" to "other" orientation. *Management Inform. Systems Quart.* 22(3):335–362.

Chin WW (1998) The partial least squares approach to structural equation modeling. Marcoulides GA, ed. *Modern Methods for Business Research* (Lawrence Erlbaum Associates Inc., Mahway, NJ), 295–336.

Cohen J (1992) A power primer. *Psych. Bull.* 112(1):155–159.

Colquitt JA (2001) On the dimensionality of organizational justice: A construct validation of a measure. *J. Appl. Psych.* 86(3):386–400.

Culnan MJ, Bies RJ (2003) Consumer privacy: Balancing economic and justice considerations. *J. Soc. Issues* 59(2):323–342.

Daft RL, Lengel RH (1986) Organizational information requirements, media richness and structural design. *Management Sci.* 32(5):554–571.

Daft RL, Lengel RH, Trevino LK (1987) Message equivocality, media selection, and manager performance: Implications for information systems. *MIS Quart.* 11(3):355–366.

Debatin B, Lovejoy JP, Horn A-K, Hughes BN (2009) Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *J. Comput.-Mediated Comm.* 15(1):83–108.

Dennis AR, Kinney ST (1998) Testing media richness theory in the new media: The effects of cues, feedback, and task equivocality. *Inform. Systems Res.* 9(3):256–274.

Dennis AR, Kinney ST, Hung Y-TC (1999) Gender differences in the effects of media richness. *Small Group Res.* 30(4):405–437.

Dinev T, Hart P (2006) An extended privacy calculus model for e-commerce transactions. *Inform. Systems Res.* 1(17):61–80.

Eisenberger R, Fasolo PM, Davis-LaMastro V (1990) Perceived organizational support and employee diligence, commitment, and innovation. *J. Appl. Psych.* 75(1):51–59.

Ellison NB, Hancock JT, Toma CL (2011) Profile as promise: A framework for conceptualizing veracity in online dating self-presentations. *New Media Soc.* 13(6):1–18.

Finn J (2004) A survey of online harassment of a university campus. *J. Interpersonal Violence* 19(4):468–483.

Gefen D, Straub D, Boudreau M (2000) Structural equation modeling and regression: Guidelines for research practice. *Comm. Assoc. Inform. Systems* 4(7):1–77.

Gibbs JL, Ellison NB, Heino RD (2006) Self-presentation in online personals. *Comm. Res.* 33(2):152–177.

Gilbert SJ, Horenstein D (1975) The communication of self-disclosure: Level versus valence. *Human Comm. Res.* 1(4): 316–322.

Hancock JT, Dunham PJ (2001) Impression formation in computer-mediated communication revisited: An analysis of the breadth and intensity of impressions. *Comm. Res.* 28(3):325–347.

Hann IR, Hui KL, Lee SY, Png PL (2007) Overcoming online information privacy concerns: An information-processing theory approach. *J. Management Inform. Systems* 24(2):13–42.

Hemetsberger A (2002) Fostering cooperation on the Internet: Social exchange processes in innovative virtual consumer communities. *Adv. Consumer Res.* 29(1):354–356.

Holden RR (1994) Social desirability. Corsini RJ, ed. *Encyclopedia of Psychology* (John Wiley, New York) 429–430.

Hu L-T, Bentler PM (1999) Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling* 6(1):1–55.

Hui KL, Teo HH, Lee SYT (2007) The value of privacy assurance: An exploratory field experiment. *MIS Quart.* 31(1):19–33.

IDA (Infocomm Development Authority of Singapore) (2007) Annual survey on infocomm usage in households and by individuals for 2007. Retrieved from http://www.ida.gov.sg/doc/Publications/Publications_Level2/20061205092557/ASInfocommUsageHseholds07.pdf.

Ji P, Lieber PS (2010) Am I safe? Exploring relationships between primary territories and online privacy. *J. Internet Commerce* 9(1):3–22.

Jiang LC, Bazarova NN, Hancock JT (2010) The disclosure-intimacy link in computer-mediated communication: An attributional extension of the hyperpersonal model. *Human Comm. Res.* 37(1): 58–77.

Joinson AN, Woodley A, Reips U-D (2007) Personalization, authentication and self-disclosure in self-administered Internet surveys. *Comput. Human Behav.* 23(1):275–285.

Joinson NA (2001) Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *Eur. J. Soc. Psych.* 31(2):177–192.

Kim K-H, Yun H (2007) Crying for me, crying for us: Relational dialectics in a Korean social network site. *J. Comput.-Mediated Comm.* 13(1):298–318.

Lawler EJ, Thye SR (1999) Bringing emotions into social exchange theory. *Annual Rev. Sociol.* 25:217–244.

Le Poire BA, Burgoon JK, Parrott R (1992) Status and privacy restoring communication in the workplace. *J. Appl. Comm. Res.* 20(4):419–436.

Lea M, Spears R, Groot D (2001) Knowing me, knowing you: Anonymity effects on social identity processes within groups. *Personality Soc. Psych. Bull.* 27(5):526–537.

Madden M, Smith A (2010) Reputation management and social media. Retrieved from http://pewinternet.org/~/media//Files/Reports/2010/PIP_Reputation_Management_with_topline.pdf

Madden M, Fox S, Smith A, Vitak J (2007) Digital footprint: Online identity management and search in the age of transparency. Retrieved from http://www.pewinternet.org/~/media//Files/Reports/2007/pip_digital_footprints.pdf.pdf

Malhotra NK, Kim SS, Agarwal J (2004) Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Inform. System Res.* 15(4):336–355.

McGrath JE, Hollingshead AB (1993) Putting the "group" back in group support systems: Some theoretical issues about dynamic processes in groups with technological enhancements. Jessup LM, Valacich JS, eds. *Group Support Systems: New Perspectives* (Macmillan, New York), 78–96.

Milne GR, Gordon ME (1993) Direct mail privacy-efficiency tradeoffs within an implied social contract framework. *J. Public Policy and Marketing* 12(2):206–215.

Moral-Toranzo F, Canto-Ortiz J, Gómez-Jacinto L (2007) Anonymity effects in computer-mediated communication in the case of minority influence. *Comput. Human Behav.* 23(3):1660–1674.

Nichols DS, Greene RL (1997) Dimensions of deception in personality assessment: The example of MMPI-2. *J. Personality Assessment* 68(2):251–266.

Ofcom (2011) Ofcom technology tracker. Retrieved from http://www.ofcom.org.uk/static/marketdataresearch/statistics/main_set.pdf

Pavlou PA, Gefen D (2004) Building effective online marketplaces with institution-based trust. *Inform. Systems Res.* 15(1):37–59.

Peris R, Gimeno MA, Pinazo D, Ortet G, Carrero V, Sanchiz M, Ibanez I (2002) Online chat rooms: Virtual spaces of interaction for socially oriented people. *CyberPsychology Behav.* 5(1):43–51.

Perreault S, Bourhi RY (1999) Ethnocentrism, social identification, and discrimination. *Personality Soc. Psych. Bull.* 25(1):92–103.

Petronio S (1991) Boundary management: A theoretical model of managing disclosure of private information between marital couples. *Comm. Theory* 1(4):311–335.

Petronio S (2002) *Boundaries of Privacy: Dialectics of Disclosure* (State University of New York Press, Albany, NY).

Pinsonneault A, Heppel N (1997) Anonymity in group support systems research: A new conceptualization, measure, and contingency framework. *J. Management Inform. Systems* 14(3):89–108.

Podsakoff P, MacKenzie S, Lee J, Podsakoff N (2003) Common method biases in behavioral research: A critical review of the literature and recommended remedies. *J. Appl. Psych.* 88(5):879–903.

Postmes T, Spears R (1998) Deindividuation and antinormative behavior: A meta-analysis. *Psych. Bull.* 123(3):238–259.

Ratan RA, Chung JE, Shen C, Williams D, Poole MS (2010) Schmoozing and smiting: Trust, social institutions, and communication patterns in an MMOG. *J. Comput.-Mediated Comm.* 16(1):93–114.

Riva G, Galimberti C (1998) The psychology of cyberspace: A sociocognitive framework to computer-mediated communication. *New Ideas in Psych.* 15(2):141–158.

Schimel J, Arndt J, Pyszczynski T, Greenberg J (2001) Being accepted for who we are: Evidence that social validation of the intrinsic self reduces general defensiveness. *J. Personality Soc. Psych.* 80(1):35–52.

Schoenbachler DD, Gordon GL (2002) Multi-channel shopping: Understanding what drives channel choice. *J. Consumer Marketing* 19(1):42–53.

Sheer VC (2011) Teenagers' use of MSN features, discussion topics, and online friendship development: The impact of media richness and communication control. *Comm. Quart.* 59(1):82–103.

Smith HJ, Milberg SJ, Burke SJ (1996) Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quart.* 20(2):167–196.

Sobel ME (1982) Asymptotic confidence intervals for indirect effects in structrual equations models. Leinhart S, ed. *Sociological Methodology* (Jossey-Bass, San Franciso), 290–312.

Son J-Y, Kim SS (2008) Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quart.* 32(3):503–529.

Stewart KA, Segars AH (2002) An empirical examination of the concern for information privacy instrument. *Inform. Systems Res.* 13(1):36–49.

Tidwell LC, Walther JB (2002) Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations: Getting to know one another a bit at a time. *Human Comm. Res.* 28(3):317–348.

Toma CL, Hancock JT (2010) Looks and lies: The role of physical attractiveness in online dating self-presentation and deception. *Comm. Res.* 37(3):335–351.

Tucker LR, Lewis C (1973) Reliability coefficient for maximum likelihood factor analysis. *Psychometrika* 38(1):1–10.

Vandebosch H, Van Cleemput K (2009) Cyberbullying among youngsters: Profiles of bullies and victims. *New Media Soc.* 11(8):1349–1371.

Verhoef PC (2003) Understanding the effect of customer relationship management efforts on customer retention and customer share development. *J. Marketing* 67(4):30–45.

Viégas FB (2005) Bloggers' expectations of privacy and accountability: An initial survey. *J. Comput.-Mediated Comm.* 10(3).

Walther JB (1996) Computer-mediated communication: Impersonal, interprsonal, and hyperpersonal interaction. *Comm. Res.* 23(1):3–43.

Walther JB (2007) Selective self-presentation in computer-mediated communication: Hyperpersonal dimensions of technology, language, and cognition. *Comput. Human Behav.* 23(5):2538–2557.

Wheeless LR, Grotz J (1976) Self-disclosure and interpersonal solidarity: Measurement, validation, and relationships. *Human Comm. Res.* 3(1):47–61.

Wolak JJD, Mitchell KJ, Finkelhor D (2007) Does online harassment constitute bullying? An exploration of online harassment by known peers and online-only contacts. *J. Adolescent Health* 41(6):51–58.

Woo J (2006) The right not to be identified: Privacy and anonymity in the interactive media environment. *New Media Soc.* 8(6): 949–968.

Xu H, Luo X, Carroll JM, Rosson MB (2011) The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems* 51(1):42–52.

Xu H, Teo HH, Tan BC-Y, Agarwal R (2009) The role of push-pull technology in privacy calculus: The case of location-based services. *J. Management Inform. Systems* 26(3):135–174.

Yao MZ, Flanagin AJ (2006) A self-awareness approach to computer-mediated communication. *Comput. Human Behav.* 22(3):518–544.

Zwick D, Dholakia N (2004) Whose identity is it anyway? Consumer representation in the age of database marketing. *J. Macromarketing* 24(1):31–43.