THREE ESSAYS ON INFORMATION PRIVACY IN ONLINE SOCIAL AND COMMERCIAL CONTEXTS

CHOI CHUN FUNG (BEN)

(B. Comp. (Hons.), National University of Singapore)

A THESIS SUBMITTED

FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF INFORMATION SYSTEMS

NATIONAL UNIVERSITY OF SINGAPORE

2013

DECLARATION

I hereby declare that this thesis is my original work and it has been written by me in its entirety. I have duly acknowledged all the sources of information which have been used in the thesis.

This thesis has also not been submitted for any degree in any university previously.

_____

Choi Chun Fung

12 November 2013

ACKNOWLEDGEMENTS

First and foremost I want to thank my advisor Dr. Jack Z. Jiang. It has been an honor to be his Ph.D. student. He has taught me, both consciously and unconsciously, how good research is done. I appreciate all his contributions of time, ideas, and guidance to make my Ph.D. experience productive and stimulating. The joy and enthusiasm he has for his research was contagious and motivational for me, even during tough times in the Ph.D. pursuit.

Faculty members at the National University of Singapore and at external universities have contributed to the success of this study. Dr. C.S. Heng, Dr. Sophia B. Xiao, and Dr. S.S. Kim gave interesting and useful suggestions for carrying out this piece of research work. This work has also benefited from the insightful comments by several anonymous editors and reviewers of journals and conferences. For the dissertation I would like to thank my committee members: Dr. Klarissa, T.T. Chang, Dr. Sharon S.L. Tan, and Dr. Chen Y.Y. for their time, interest, and helpful comments.

Lastly, I would like to thank my family for all their love and encouragement. For my parents who raised me with a love of curiosity and supported me in all my pursuits. For the presence of my sister Loky. And most of all for my loving, supportive, encouraging, and patient wife Cammy whose faithful support throughout the entire Ph.D. experience is so appreciated. Thank you.

TABLE OF CONTENTS

SUMMARY

Information privacy has been an increasingly important issue for both information systems (IS) researchers and practitioners. In this thesis, three studies are conducted to explore the prevalent issues associated with information privacy. Specifically, Study I (Chapter Two) draws on the hyperpersonal framework and the privacy calculus perspective to elucidate the interesting roles of privacy concerns and social rewards in synchronous online social interactions and examine the causes and the behavioral strategies that individuals utilize to protect their privacy. An empirical study involving 251 respondents was conducted in online chatrooms. Overall, this study contributes to the IS literature by integrating the hyperpersonal framework and the privacy calculus perspective to identify antecedents of privacy tradeoff and predict individuals' behavior in synchronous online social interactions.

Study II (Chapter Three) seeks to elucidate the consequences of an embarrassing exposure in online social networks. Drawing on the social exchange theory, this study examines the effects of information dissemination and network mutuality on individuals' exchange assessment as well as how this assessment shapes their behavioral responses. The results of a laboratory experiment involving 109 subjects provide strong evidence that information dissemination and network mutuality jointly influence individuals' perception of relationship bonding and privacy invasion. In addition, whereas perceived relationship bonding impedes both transactional avoidance and interpersonal avoidance, it leads to approach behavior. Further, while perceived privacy invasion increases transactional avoidance, it reduces approach behavior.

Overall, this study contributes to the IS literature by deepening the understanding of individuals' behavioral responses to embarrassing exposures in online social networks.

Study III (Chapter Four) develops and tests a model that explains online customer behavior after a privacy breach; more specifically, this study focuses on an online firm's postincident recovery endeavor in mitigating the impact of a privacy breach on customer relationships. Drawing on the service recovery literature, Study III integrates the notions of justice perceptions and psychological responses into a theoretical framework that describes how individuals react to an online firm's postincident recovery endeavor. The proposed model was tested against data collected from 1,007 actual users of online vendors. The results of the analysis using structural equation modeling generally supported our model. Specifically, the three types of justice perceptions, i.e., distributive, procedural, and interactional justice, were found to differently affect psychological responses, i.e., perceived breach and feelings of violation. Moreover, justice perceptions were found to interact to influence their psychological responses in a way highly consistent with the proposed model. In addition, psychological responses were shown to be important in shaping postincident outcomes such as post-word of mouth and post-likelihood of switching. Overall, this study gives researchers and practitioners a useful conceptual tool for analyzing the effectiveness of organizational practices in mitigating the damage a privacy breach poses for customer relationships.

Overall, Study I identifies antecedents of privacy concerns and social rewards in synchronous online social interactions. Study II enriches the information privacy literature by suggesting that embarrassing information is an important object of exposure in online social networking. Study III extends the boundary of knowledge in the field of information privacy by developing nuanced accounts specific to the online privacy breach recovery domain and basing them on a more generalized and integrative framework. This thesis concludes with Chapter Five, which includes a discussion on the contributions, implications, limitations, as well as future research direction.

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1 INTRODUCTION

1.1 BACKGROUND AND MOTIVATION

1.1.1 Information Privacy

Information privacy is an increasingly important issue to both individuals and business. Individuals could be the victims of various privacy problems, such as identity thefts, impersonations, as well as bodily harm, when information privacy is threatened in online social interactions. The popularity of online social networks has exacerbated the issue. Unlike other online social interaction environment, online social networks facilitate the dissemination of personal information to individuals' actual social circles. Furthermore, given the diversity in social circles, personal information could be concurrently exposed to both known friends as well as unacquainted strangers.

Whereas the disclosure of personal information is important in developing online relationships, information provision is typically compulsory in online commercial transactions. Often, to complete transactions, online businesses are entrusted with personal information, such as identity information, contact numbers, and most importantly, credit card information. Consequently, when an online firm fails to recover from a privacy breach, individuals are likely to think the firm has violated the psychological contact because it is not only incompetent in safeguarding customer information but also is unable to remedy the issue (Wang and Huff 2007).

Information systems (IS) research has progressed significantly in expanding our understanding of individuals' predispositions, beliefs, attitudes,

and behavior in relation to information privacy (Dinev and Hart 2006, Son and Kim 2008). Earlier studies on these topics focused on identifying the nature of concern for information privacy in the context of direct marketing (Smith et al. 1996, Stewart and Segars 2002). Subsequently, Malhotra et al. (2004) developed a scale of information privacy concerns specific to the Internet context. IS researchers also have tried to identify the impact of privacy concerns on privacy-protective behaviors, such as willingness to release personal information, identity misrepresentation, relationship termination, word of mouth, and complaints (Dinev and Hart 2006, Awad and Krishnan 2006, Son and Kim 2008, Culnan and Williams 2009). Furthermore, several IS studies have explored the strategies adopted by firms in reducing privacy breaches (Gal-Or and Ghose 2005, Yue and Cakanyildirim 2007). Although IS research deals with numerous aspects of information privacy, limited research has been done to understand how individuals' behavior can be shaped by privacy issues in online social interactions as well as organizational remedies after a privacy breach incident (Elson and LeClerc 2006, Son and Kim 2008, Culnan and Williams 2009). This thesis empirically investigates how individuals respond to privacy-related issues on synchronous online social interactions and online social network, as well as the recovery strategies undertaken by online firms after a privacy breach incident.

1.1.2 Privacy-protective behavior in Synchronous Online Social Interactions: Reviews and Problems

Synchronous online social interactions have revolutionized lives by enabling 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 chatroom 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, an individual's privacy is subject to public scrutiny in synchronous online social interactions. 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.

It has, however, been observed that despite privacy concerns, individuals are very willing towards the sharing of personal and intimate information with others, including complete strangers (Madden et al. 2007). Hence, it would be interesting to investigate why users' privacy behavior is at times inconsistent with their privacy concerns. Therefore, Study I investigates what drives individuals' privacy-protective behavior in the context of synchronous online social interactions and reveals that social rewards can be just as compelling as privacy concerns in affecting behavior. Furthermore, Study I identifies the antecedents of privacy concerns and social rewards as well as studies the strategies that individuals adopt to protect their privacy in developing online relationships.

1.1.3 Embarrassing Exposures in Online Social Networks: Reviews and Problems

Online social networking websites provide an environment where individuals can easily maintain and develop social relationships by creating profiles with information about themselves and connecting their profiles to those of others (Bumgarner 2007; Ellison et al. 2011). These connections facilitate the exchange of socially meaningful information (such as birthday wishes and jokes) and the sharing of common interests (such as arts and sports) (McLaughlin and Vitak 2011). At times, for amusement, individuals may playfully tease each other by revealing their friends' embarrassing information in online social networks (Wang et al. 2011). Indeed, the teasing literature suggests that embarrassing exposures could lead to relationship development (e.g., Lange 2007).

Yet it has been observed that the target of an embarrassing tease might not be amused but instead feel offended by the involuntary exposure resulting from friends' postings about the target (Kruger et al. 2006). Hence, it is interesting to investigate why targets interpret embarrassing exposure differently and how such interpretations influence their behavioral responses in online social networks. Study II of this thesis thus focuses on elucidating the role of an embarrassing exposure in online social networking. Specifically, this study considers the way embarrassing information is involuntarily exposed through the posting and tagging mechanisms. Posting involves the publication of information about a target on the disseminator's profile. Tagging, which is performed in addition to posting, identifies the

target in the information and associates the information to the target's profile. In addition, to represent the role that social relationship structure plays in individuals' assessment of social exchange, Study II examines the network mutuality between the disseminator and the target. Whereas high network mutuality underscores high degree of commonality among the disseminator's and the target's social networks, low network mutuality denotes two largely distinct networks.

Furthermore, Study II investigates a target's benefit and cost perceptions related to an embarrassing exposure in online social networks. In particular, in terms of benefits assessment, this study examines the impact of an embarrassing exposure on the social relationship between the disseminator and the target. In terms of cost assessment, this study examines the way an involuntary exposure intrudes the target's privacy. Study II also proposes and empirically tests a taxonomy of behavioral responses to embarrassing exposures in online social networks.

1.1.4 Customer Behavior after an Online Privacy Breach: Reviews and Problems

Online privacy breach has become an increasing alarming issue. According to the Identity Theft Resource Center (2009), approximately 600 breaches are publicly reported annually in the United States. Undoubtedly, this unfortunate trend endangers the information privacy of customers and, at the same time, threatens the profitability and reputations of businesses, which can be illustrated by several high-profile privacy breaches (e.g., Zetter 2009,

Jewell 2007, FTC 2006). On the whole, a privacy breach is highly likely to hurt the performance of a firm.

Although IS research deals with numerous aspects of information privacy, researchers (with the notable exception of Culnan and Williams 2009) have rarely focused specifically on customers' reaction to a privacy breach within the context of a specific business-to-customer relationship. Moreover, no research has been done to understand how remedial responses to a data breach can change online customer behavior such as word of mouth and likelihood of switching (Elson and LeClerc 2006, Son and Kim 2008, Culnan and Williams 2009). Therefore, Study III develops and tests a model that explains online customer behavior after a privacy breach.

1.2 RESEARCH FOCUS AND POTENTIAL CONTRIBUTIONS

This thesis explores individuals' privacy-related behavior in both online social interactions and commercial transactions. In particular, Study I focuses on identifying antecedents of individuals' privacy tradeoff, which drives their privacy-protective behavior in synchronous online social interactions. Meanwhile, Study II focuses on two key aspects of embarrassing exposures on online social networks, namely information dissemination and network mutuality, to elucidate the effects of involuntary exposure on usage behavior. Study III focuses on aspects of organizational remedies to investigate individuals' responses after an online privacy breach.

1.2.1 Study I: Privacy Tradeoff

Information systems (IS) research has made some progress in understanding the determinants of individuals' privacy-related behavior.

Overall, past 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, Study I proposes 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.

The second motivation of Study I 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), the theoretical framing of Study I 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 Study I, 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.

1.2.2 Study II: Information Dissemination and Network Mutuality

Study II elucidates the role of an embarrassing exposure in online social networking by integrating the Social Exchange Theory with the teasing literature and privacy research. This theory posits that an individual assesses a

social exchange with reference to two important features of the exchange, namely (1) exchange behavior (i.e., the way the social exchange is conducted) and (2) social relationship structure (i.e., the structure of relationships between individuals involved in the social exchange) (Emerson 1972a; Emerson 1972b; Homans 1961). Correspondingly, to explore the impact of an embarrassing exposure (i.e., the exchange behavior) in a social exchange, this study considers the way embarrassing information is involuntarily exposed through the posting and tagging mechanisms. In addition, to represent the role that social relationship structure plays in individuals' assessment of social exchange, Study II examines the network mutuality between the disseminator and the target.

Furthermore, according to the Social Exchange Theory, the assessment of a social exchange entails the evaluation of two important components, namely exchange benefit and exchange cost (Blau 1986; Cook and Rice 2006). Whereas exchange benefit represents the resources individuals obtain from a social exchange, such as relational associations and recognitions, exchange cost involves the resources they devote to completing a social exchange, such as time and information (Molm et al. 2000). Following past research on social exchange, this study investigates a target's benefit and cost perceptions related to an embarrassing exposure in online social networks. Specifically, in terms of benefit assessment, Study II relies on the teasing literature to understand the impact of an embarrassing exposure on the social relationship between the disseminator and the target. In terms of cost assessment, this study relies on extant privacy research to elucidate the way an involuntary exposure intrudes

the target's privacy. This study is among the first in the information systems (IS) literature to evaluate both the benefit and the cost of an embarrassing exposure in online social networks.

The other objective of this study is to investigate the target's behavioral responses to an embarrassing exposure. Previous IS research suggests that privacy invasion leads to protective behavior, such as denial of information requests, relationship terminations, and complaints (e.g., Culnan and Williams 2009; Dinev and Hart 2006; Son and Kim 2008). However, there has been a paucity of research that examines individuals' responses associated with involuntary exposures of embarrassing information. While the privacy invasion associated with an involuntary exposure may induce relationship termination as well as withdrawal behavior, the humor implied by the exposure is known to stimulate the target's active involvement in interactions (Lampert and Ervin-Tripp 2006; Petronio 2002). To address this gap in prior research, Study II proposes and empirically tests a taxonomy of behavioral responses to embarrassing exposures in online social networks.

1.2.3 Study III: Aspects of Organizational Remedies and Psychological Contract

The objective of Study III is to enrich the IS literature by developing and testing a model that explains online customer behavior after a privacy breach; more specifically, this study focuses on an online firm's postincident actions in mitigating the impact of a privacy breach. The overarching theory in this study is drawn from the service recovery literature, which posits that customers' specific beliefs with regard to organizational remedies determine

overall psychological evaluations, which in turn regulate behavior (Hoffman and Kelley 2000, Maxham and Netemeyer 2002, Smith and Bolton 2002). Specifically, the justice framework is used as a theoretical basis in identifying consumers' beliefs associated with key attributes of privacy breach remedies (Moorman 1991, Culnan 1995). This framework suggests that people evaluate privacy related issues in terms of three criteria, namely, distributive justice, procedural justice, and interactional justice (Culnan and Bies 2003, Malhotra et al. 2004). According to the literature, these justice factors have been constantly shown to be salient in the context of information privacy (Alge 2001, Zweig and Webster 2002, Ashworth and Free 2006, Son and Kim 2008, Poddar et al. 2009, Wirtz and Lwin 2009). Thus, this study argues that these three types of justice perceptions can reasonably indicate the specific criteria that online customers employ in assessing organizational actions undertaken to remedy a breach incident.

Meanwhile, Study III borrows the concept of psychological responses from prior literature to represent general thoughts and feelings relevant to the context of information privacy (Pavlou and Gefen 2005, Robinson and Morrison 2000). Specifically, the service recovery literature suggests that individuals' overall psychological evaluations are summarized into cognitive and emotional factors, which are represented by, respectively, perceived breach and feelings of violation (Morrison and Robinson 1997, Robinson and Morrison 2000). Furthermore, much research shows that these psychological responses can be shaped by various types of justice perceptions jointly, instead of independently (Folger 1986, Luo 2007, Tang et al. 2008). Thus, Study III

proposes not only main effects of justice perceptions but also their interaction effects on perceived breach and feelings of violation. The research model of this study posits that, consistent with the service recovery literature, online customers' psychological responses (i.e., general thoughts and feelings) regulate postincident outcomes that include post-word of mouth and post-likelihood of switching.

1.2.4 Potential Contributions

This thesis seeks to contribute to both the academic and practitioner arenas by investigating information privacy issues in both online social interactions and commercial transaction contexts. Specifically, by addressing the research gaps proposed in the previous sections, the three studies in this thesis are expected to make the following contributions.

Study I contributes 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 tradeoffs 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.

Furthermore, Study I also presents new insights to prior privacy-related studies by extending the privacy calculus lens to the context of synchronous online social interactions. This study argues that privacy concerns alone 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). Study I has advocated and attested the role of social rewards as the intangible benefits individuals derive from synchronous online social interactions.

Study II contributes to IS literature by examining factors relevant to online social networks that influence individuals' bonding experience and privacy perception in an embarrassing exposure. This study investigates two antecedents of perceived relationship bonding and perceived privacy invasion, namely, information dissemination and network mutuality. Study II rationalizes that information dissemination (i.e., posting only vs. posting with tagging) exemplifies exchange behavior in initiating social exchange. Reflecting the way a bonding experience can be shaped by target participation, information dissemination illustrates how exclusion and inclusion of target notification determine perceived relationship bonding. Furthermore, this study contends that network mutuality depicts the social relationship structure in which the social exchange occurs. On one hand, network mutuality determines the audience type, which influences the impact of target notification on perceived relationship bonding. On the other hand, network mutuality determines the exposure size, which influences the effect of target individuation on perceived privacy invasion. Taken as a whole, the two antecedents of perceived relationship bonding and perceived privacy invasion (i.e., information dissemination and network mutuality) are particularly relevant to online social networks.

Second, Study II advances privacy-related research by examining perceived relationship bonding, in addition to perceived privacy invasion, as an important component in individuals' assessment of an embarrassing exposure in online social networks. This study reveals that, while the involuntary nature of the embarrassing exposure influences the perception of privacy invasion, the humor implied by the exposure may also induce relationship bonding. Given that the exposure of embarrassing information is typically considered negative in past research, the findings of this study shed light on a multi-faceted interpretation of the phenomenon.

Third, Study II enriches extant IS research on social interactions by providing a taxonomy of behavioral responses to embarrassing exposure in online social networks. Drawing on the dichotomy of passive and active behavior, this study classifies individuals' behavioral responses into four different types, namely inaction, transactional avoidance, interpersonal avoidance, and approach. The findings of this study indicate that the proposed taxonomy is helpful in analyzing a variety of behavior commonly performed in response to embarrassing exposures and thus serves as a useful tool for in-depth examination of individuals' response behavior in online social networks.

Study III contributes significantly to IS literature by showing how justice perceptions differ from each other in the context of an online firm's responses to a data breach. Specifically, this study demonstrates that distributive justice has positive effects on both cognitive and emotional evaluations. However, we found that procedural justice affects cognitive evaluations (i.e., perceived breach), whereas interactional justice determines

emotional evaluations (i.e., feelings of violation). Our findings bolster a common notion that compensation exerts profound effects on individuals' overall evaluations of a situation in question. More interesting, this study reveals a relatively unknown fact of justice perceptions that once compensation is taken into account, fair procedures control only the cognitive side but not the emotional side, whereas respectful treatments control the emotional side but not the cognitive side. We suspect that the emergence of this discernible pattern from this particular study results, at least partly, from its lean online context in which individuals' judgments about fairness are rarely intermixed with rich human relationships. In any case, more research is needed to explore the distinct nature of justice perceptions that may vary with respect to various privacy contexts. Overall, this study adds to the justice literature by showing theoretically as well as empirically the clearly discernible patterns behind justice perceptions, especially when these patterns are examined within the context of an online privacy breach

Furthermore, Study III formally examines psychological contract violation in an online privacy breach. The lack of attention to the psychological contract perspective is surprising when one considers that a privacy breach constitutes a severe breach of a psychological contract in online commercial transactions. Drawing on the taxonomy proposed by Morrison and Robinson (1997), Study III explicitly differentiates between perceived breach, which represents a cognitive response, and feelings of violation, which indicate an emotional response. Overall, this dual approach to

psychological responses is effective not only in examining privacy problems but also in understanding other social exchange relationships.

This thesis provides practitioners with valuable insights. Given the influence of network mutuality on target's interpretation of an embarrassing exposure, application designers may contemplate how they can use information on network mutuality to their advantage. For example, in cases where embarrassing content is disseminated, a target's perception of privacy invasion can be mitigated if posting with tagging is discouraged for a disseminator who has low network mutuality with the target. On the other hand, if the disseminator has high network mutuality with the target, the disseminator should be promptly notified regarding the option of tagging the target to induce the perception of relationship bonding.

The three types of active behavioral responses identified in Study II alerts service providers to various user actions that go beyond inaction. Study II reveals that users may file reports to the service provider to seek transactional avoidance. This finding can steer online service providers toward designing effective mechanisms to facilitate transactional avoidance. For example, when users complain against a piece of content, the online social network provider should consider suspending the content from dissemination. Furthermore, Study II shows that users, despite their strong perception of privacy invasion, may refrain from interpersonal avoidance to avoid abrupt relationship termination. To this end, this thesis advocates that service providers should allow individuals to gradually de-escalate their relationships. For example, to distance oneself from the disseminator, users should be

permitted to engage in gradual relationship dissolution by progressively excluding the disseminator from his or her online social networking activities. Study II also shows that users may engage in active exchange with the disseminator through approach behavior. Therefore, it is important that service providers provide participatory features, such as threaded commenting and content rating, to stimulate rich interactions.

Study III reveals important insights into how to salvage customer relationships damaged by privacy-related incidents. First, Study III advocates that privacy breach recovery should be carefully reengineered. Specifically, managers could consider creating privacy breach remedies that allow for recovery efforts directed at improving the psychological responses experienced by customers. They should have an array of tools and resources available to address the specific needs of customers. Study III shows that perceived breach and feelings of violation are greatly affected by compensation. However, perceived breach becomes less sensitive to compensation when a fair procedure was in place, and feelings of violation are less affected by compensation when respectful interpersonal treatment was experienced. This result is an important reminder that redressing privacy breaches means more than enacting all three aspects of privacy recovery. Thus, online firms must carefully consider the specific psychological responses to improve customers' privacy situations.

Study III also notes that interactional justice amplifies the effect of procedural justice on perceived breach. This finding implies that when interactional justice is low, organizational efforts to boost procedural justice

are likely to be wasted and have little impact on perceived breach. Procedural justice and interactional justice are similar in that both are concerned with "means" to ends. Because of this resemblance, interpersonal treatment might be considered as a testimonial for the firm's practices. Although conventional wisdom suggests the significance of procedural justice and interactional justice, their synergistic power is not yet widely known. Study III clearly shows that interactional justice is a necessary condition to maximize the return from a firm's adherence to fair procedures. The online environment facilitates information dissemination, which is vital for notifying customers about the process of remedying a privacy breach. However, the lack of physical contacts could hinder customers' understanding of the complex recovery process. In light of this understanding, to maximize the return from adherence to fair procedures, online firms should consider enhancing interpersonal interactions in developing their privacy breach recovery capabilities.

1.3 THESIS ORGANIZATION

This opening chapter provides an overview of the entire study context and the general motivations based on the current research gaps. It highlights the importance of the information privacy for both online social interactions and electronic commerce, and raises the research questions that will be addressed in the studies as well as the potential contributions. The following paragraphs discuss the organization of the remaining chapters in this thesis.

Chapter 2 describes Study I in detail. It first reviews the literature on the hyperpersonal framework, which is drawn upon as the theoretical basis in identifying antecedent pertinent in the context of synchronous online social

interactions. It then discusses the privacy calculus perspective, which underscores the role of psychological tradeoff in driving individuals' privacy-protective behaviors. A survey is conducted to test the proposed hypotheses. Theoretical and practical implications are discussed.

Chapter 3 reports the detail of Study II, which investigates individuals' responses to involuntary embarrassing exposures on online social networks. This study integrates the social exchange theory with the teasing literature and privacy research to elucidate the impact of embarrassing exposures on perceived privacy invasions and perceived relationship bonding. Furthermore, using the Kuhl's (1981) classification of response behavior, this study proposes four types of behavioral responses to embarrassing exposures, namely inaction, transactional avoidance, interpersonal avoidance, and approach. A laboratory experiment is conducted to test the research model. This chapter concludes with a discussion on its theoretical and practical implications, limitations, as well as future research directions.

Chapter 4 elaborates the detail of Study III. This chapter first reviews on online privacy breach and the typical organizational remedies undertaken by online firms. To investigate the impact of organizational remedies on consumer postincident behaviors, this study employs the service recovery literature as the overarching framework. Furthermore, following the service recovery literature, we draw upon the justice framework to identify the key aspects of organizational remedies after an online privacy breach and the psychological contract theory to understanding customers' overall psychological evaluation of the recovery efforts undertaken by an online firm.

A scenario-based survey is conducted to test the proposed research framework. Discussions and implications are then reported.

Chapter 5 concludes this thesis by summarizing the findings and implications of the three studies, followed by discussion on the limitations and a projection of possible future research directions.

CHAPTER 2 STUDY I: PRIVACY CONCERNS AND PRIVACY-PROTECTIVE BEHAVIOR IN SYNCHRONOUS ONLINE SOCIAL INTERACTIONS

2.1 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 chatroom 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 U.S. 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 towards the sharing of personal and intimate information with others, including complete strangers. For example, in another survey of 1,623 Internet users in the U.S., 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 while 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 tradeoff 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 behavioral responses that individuals adopt to protect their privacy.

2.2 LITERATURE REVIEW

2.2.1 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, due to 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 over-estimate 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.

2.2.2 Privacy Calculus – Privacy Concerns

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; Westin 1967), privacy concerns refers to individuals' subjective views of fairness within the context of privacy (Malhotra et al. 2004). Smith et al. (1996) developed the Concern for Information Privacy (CFIP) scale which regards privacy concerns as "individuals' concerns about organizational information privacy practices" (p.169), such as information collection, confidentiality, errors and secondary usage.

Reflecting on the origin of privacy concerns, collection refers to the extensiveness of personal information collected by organizations (Smith et al. 1996; Stewart and Segars 2002). Increasingly, it induces the perception of intensive data logging, as well as the impression that organizations are getting more intrusive (Sheehan and Hoy 2000). The second factor, confidentiality, deliberates on the challenges posed by unauthorized accesses to personal information (Smith et al. 1996; Stewart and Segars 2002). Personal information is especially vulnerable to illegitimate explorations when technological protections are amiss or data policies are flimsy (Miyazaki and Fernandez 2001). Noting the consequences of errors, CFIP also emphasizes

the importance of information accuracy (Smith et al. 1996; Stewart and Segars 2002). If it is unintentional, erroneous information could portray individuals in a false light, such as wrongfully diminishing their financial creditability and hence impairing their borrowing opportunities (Metzger 2004). The final factor, secondary usage, reflects on the impact of using information beyond individuals' acknowledged purposes (Smith et al. 1996; Stewart and Segars 2002; Xu et al. 2008). For instance, some banks are known to use financial data collected on loan applications for subsequent sales offerings, an act which applicants would never anticipate (Sheehan and Hoy 2000).

Even though privacy concerns exist in both online and offline environments, CFIP primarily focuses on individuals' concerns in the latter. Hence, Stewart and Segars (2002) acknowledge that "CFIP needs to be reinvestigated in light of emerging technology, practice and research" (p.37). In particular, Sheehan and Hoy (2000) note that the study of online privacy concerns should identify "underlying influences on privacy concern in the online environment" (p.63). Indeed, privacy concerns would not be properly measured when factors pertinent to the online context are left disregarded. For instance, the extents of personal information collection and subsequent usages have been fundamentally broadened with the growth in Internet usage. Conventionally, information about consumers was mostly collected anonymously, via unidentified surveys and public polls. In contrast, collection can be individualized using online technologies, such as website visitor monitoring, whereby consumers are traced in online commercial websites.

To address privacy issues in the online environment, Malhotra et al. (2004) built upon CFIP and proposed Internet Users Information Privacy Concerns (IUIPC) which encompasses collection, control and awareness as the essential factors of privacy concerns. Similar to CFIP, collection refers to individuals' concerns about the approach and the amount of individual-specific data demanded by others (Malhotra et al. 2004). The act of data collection forms the "foundation" of privacy concerns and is predicated on the principle of equity which relates to one's gains from information exchange (Culnan and Bies 2003).

Constituting the "active" component of privacy concerns, control refers to the degree to which individuals perceive themselves to be vested with control of the procedures (Malhotra et al. 2004). While CFIP hints at the importance of control through their emphasis on "confidentiality" and "secondary usage", IUIPC singles "control" out as one of its three essential factors. Evidence suggests that issues with access and usage are more appropriately managed through "control over who has access to personal data, how personal data are used" (Phelps et al. 2000, p.29). In the online environment, individuals could be bestowed with information control functionally and environmentally. Functional control is related to the enforcement of integrity for personal information (Pavlou et al. 2007). With accurate information, individuals can ensure that proper impression is formed about them. Environmental control cogitates the ability to regulate unintentional self exposure (Olivero and Lunt 2004). The loss of

environmental control causes individuals to feel vulnerable and become uncomfortable (Goffman 1959).

Constituting the "passive" component of privacy concerns, awareness is related to individuals' knowledge of their privacy context such as organizational privacy practices for online commercial transactions (Culnan and Bies 2003). Evidence shows that despite the existence of security measures, these mechanisms might remain inconspicuous and hence individuals could still have privacy concerns (e.g., Hui et al. 2007; Milne et al. 2005). Adequate contextual awareness provides individuals with justifications for how information is exchanged and explanations for why certain information is requested (Colquitt 2001). If individuals are deprived of these contextual information, privacy concerns would prevail (Hoffman et al. 1999). Malhotra et al. (2004) thus suggest that awareness can be manifested as informational justices which relate to the articulation of information, such as the availability of privacy assurances in online commercial transactions or identity information in online social interactions (Pavlou et al. 2007).

2.2.3 Privacy Calculus – Social Rewards

As Homans (1958: p.606) correctly pointed out in his Social Exchange Theory, "social behavior is an exchange of goods, material goods but also non-material ones, such as the symbols of approval or prestige. … For a person in an exchange, what he gives may be a cost to him, just as what he gets may be a reward, and his behavior changes less as the difference of the two, profit, tends to a maximum." This concurs with researchers who argue that individuals could possibly trade some commodity (e.g., information

privacy) for other benefits as part of a social exchange (Acquisti 2008). This exchange for other benefits becomes part of what is known as a "social contract" (Dunfee et al. 1999), as individuals have something of value to others and both decide to engage in a mutually agreeable trade, abiding by the norm of reciprocity (Lawler and Thye 1999).

In Social Exchange Theory, individuals are often motivated by self-interest to transact with others to accomplish individual goals (Lawler and Thye 1999). These interactions are usually seen as interdependent and contingent on the actions of others (Blau 1964). For instance, when something is being offered, the receiving parties would respond in kind. Furthermore, individuals are assumed to always act in ways to ensure that their benefits commensurate, if not outweigh, their costs. Social Exchange Theory has been tested in various settings. For example, in a study on system implementations, Ridings et al. (2002) investigated the effect of responsiveness of technical implementation teams on the users' adoption of new systems. Results from a quasi-experiment showed that the degree of responsiveness, as an indicator of social exchange, resulted in significant differences in the users' assessment of the correctness and eventual approval of the system.

In the context of online social interactions, individuals may engage in social exchanges to gain social rewards, which refer to the pleasures, satisfactions, and gratifications they derive from participating in a relationship or interpersonal interactions (Eisenberger et al. 1990; Gilbert and Horenstein 1975). For example, Hemetsberger (2002) found that individuals in virtual communities engage in collaborative production of digital goods and services

to fulfill their social needs such as gaining social approval, social reaffirmation, friendship, or moral support. At times, individuals socialize in online chat rooms simply to mingle around, relax and enjoy. Chatting with others online in itself may elicit pleasure and psychological reward.

Besides maximizing benefits, individuals are also known to minimize costs incurred when fulfilling personal objectives (Blau 1964). For instance, prior studies have often considered time and effort as part of the costs in developing social relationships (e.g., Altman et al. 1981; Walther 1996). By devoting time into social exchanges, individuals accumulate knowledge for reducing uncertainty about others (Afifi and Guerrero 2000). Through exerting effort to understand others' expectations, individuals prudently avoid interactions which could be seen as inappropriate and detrimental to developing relationships (Parks and Floyd 1996).

In the synchronous online environment, social exchange is substantially expedited and hence the costs in time and effort have been much discounted (Ellison et al. 2006). However, this improvement in efficiency and convenience might come at the expense of privacy when developing online social relationships. Individuals may become overly indulged in synchronous online social interactions and divulge too much personal and sensitive information (Tidwell and Walther 2002). Subjecting their private thoughts and feelings to others' scrutiny, individuals could jeopardize their own beliefs and deflate their self esteem, especially when their revelation is subsequently misused, criticized or rejected (Guerrero and Afifi 1995). Wary about these

costly repercussions, individuals would become particularly concerned about their self disclosure (Dainton and Stafford 1993).

Likewise, this cost-benefit tradeoff is also evident in online commercial transactions (e.g., Culnan and Bies 2003). Individuals are known to perform a "privacy calculus" to assess the outcomes they could receive as a result of mutual exchanges (cf. Laufer and Wolfe 1977). The financial compensations (e.g., discounts and rebates) as part of the calculus, however tempting, might be non-applicable beyond the commercial contexts. The exchange of monetary benefits in synchronous online social interactions is atypical, if not unprecedented. Rather, individuals are more likely to be seduced by the prospect of social benefits whereby personal information is revealed for relationship development. Hence, to extend privacy calculus beyond commercial transactions, we contend social rewards as the alternative benefit for individuals plagued with privacy concerns in synchronous online social interactions.

2.3 RESEARCH MODEL AND HYPOTHESES

By integrating the hyperpersonal framework and privacy calculus perspective, we designed our proposed research model, which is presented in Figure 2.1. Specifically, we hypothesize the relationships between four distinct aspects of the hyperpersonal framework and the privacy tradeoff. We also propose investigating the effects of privacy tradeoff on privacy-protective behavior.

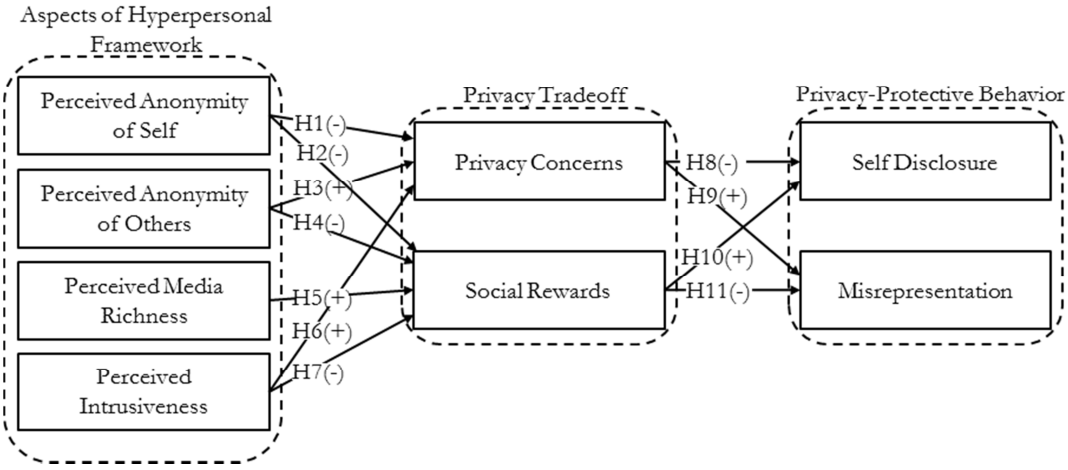


Figure 2.1: Study I Research Model

2.3.1 Hyperpersonal Framework and Privacy Tradeoff

This study draws upon the hyperpersonal framework in proposing four antecedents of privacy tradeoff, 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. Due to

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 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. While 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.

2.3.1.1 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:

H1: Higher perceived anonymity of self will reduce privacy concerns.

High perceived anonymity of self entails deindividuation, which detaches individuals from their own identities and cause them to be more apathetic toward the relationship being developed (Schimel et al. 2001). In other words, their perceived anonymity of self causes them to distance

themselves, lower their social connectedness and reduce their interpersonal dependence with communication partners (McLeod 2011). Resultantly, individuals will perceive less social rewards from the exchange relationship. Furthermore, prior research suggests that being responsive to social validation and gaining effective social affirmation are essential toward boosting individuals' socially rewarding experience (Leary and Kowalski 1990). However, perceived anonymity of self makes social validation and affirmation very difficult, if not impossible. When individuals cannot understand how they are valued as relational partners by others (Leary and Kowalski 1990), they are hindered from fostering mutual acceptance and eventually cultivating a socially rewarding experience. Thus, we hypothesize:

H2: Higher perceived anonymity of self leads to a decrease in social rewards.

2.3.1.2 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 towards privacy loss (Colquitt 2001). In summary, perceived anonymity of others constantly poses challenges to individuals' privacy concerns. Hence we posit:

H3: 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:

H4: Higher perceived anonymity of others will reduce social rewards.

2.3.1.3 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:

H5: Higher perceived media richness will increase social rewards.[1]

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). While 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). 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:

[1] Since 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.

H6: 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:

H7: Higher perceived intrusiveness will reduce social rewards.

2.3.2 Privacy Tradeoff and Privacy-Protective Behavior

Extant privacy studies have shed some light on the outcomes of privacy tradeoff. 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 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.

2.3.2.1 Privacy Concerns and Self Disclosure

In this study, we use self disclosure to refer 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) (Petronio 1991). Self disclosure plays a pivotal role in founding social relationships (Altman et al. 1981). By gradually disclosing their personal information and revealing their views and opinions, ambiguities are resolved and expectations are aligned (Dolen et al. 2004).

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 (Altman et al. 1981), individuals can become vulnerable. Others may wrongly judge them or react adversely to the information (Petronio 1991). Also, instead of being the sole owner in absolute possession of the information, others possess it too (Joinson et al. 2007). They can disseminate the information to others, use it for marketing solicitations, or even misuse the information (Phelps et al. 2000). Consequently, victims may suffer psychologically, physically or materially (Tavani and Moor 2001).

Hence, avoiding self disclosure becomes one of the most common strategies adopted by individuals to protect their privacy (Joinson et al. 2007). In a social interaction, when individuals face privacy threats, such as the unauthorized use, modification or dissemination of their private information, they can lower 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 easy to terminate or avoid. Generally, high privacy concerns indicate a lack of confidence in the reliability and integrity of others, and this should rationally lead to a corresponding reduction in self disclosure since the potential risks to individuals are significant (Olivero and Lunt 2004). Hence we posit:

H8: Greater privacy concerns will lead to less self disclosure.

2.3.2.2 Privacy Concerns and Misrepresentation

Even though potential risks may diminish any desire for self disclosure, individuals are occasionally repudiated the opportunity to withhold information (Miyazaki and Fernandez 2001) in order to proceed with an interaction. For example, in online commercial transactions, they must fill in some information designated as compulsory fields to complete membership registration. In synchronous online social interactions, the persistence of others may also make individuals feel devoid of choice, and a need to provide some falsified information.

Thus, 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 out of fun (Walther 2007). As a result, misrepresentation can serve to self protect, self explore or impress upon others (Joinson et al. 2007). To illustrate, misrepresentation enables impression management by allowing individuals to manipulate others' perception through shielding psychological information and camouflaging physical information about oneself (Leary and Kowalski 1990; Walther 2007).

Likewise, misrepresentation can also allow individuals to temporarily placate or satisfy others, thereby maintaining the flow of interactions. Based on these arguments, misrepresentation is used in synchronous interaction when individuals have to follow up on a conversation, but do not want to disclose their true private information.

Furthermore, according to Social Exchange Theory, interactions are bound by the norm of reciprocity to engage in a fair exchange of information under normal social circumstances (Lawler and Thye 1999). When their privacy is threatened, individuals might perceive a violation of this norm and take necessary steps to protect themselves. In the context of synchronous online social interactions, when individuals experience greater privacy concerns, they may resort to misrepresentation to minimize the level of threat (Milne et al. 2005). Thus, we posit:

H9: Greater privacy concerns will lead to greater misrepresentation.

2.3.2.3 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 would the individuals 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 towards the source of the rewarding relationship because they benefit from doing so. Hence we posit:

H10: Greater social rewards will lead to greater self disclosure.

2.3.2.4 Social Rewards and Misrepresentation

Social rewards and misrepresentation are negatively related. Individuals who perceive greater social rewards will refrain from misrepresentation due to 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. Since 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 due to 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:

H11: Greater social rewards will lead to less misrepresentation.

2.4 RESEARCH METHODOLOGY

Online chatrooms were selected to test our research model inasmuch as chatrooms 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 employed an online survey questionnaire to test the effects of the independent variables on privacy tradeoff, which in turn, drives individuals' privacy-protective behavior. In privacy research, a realistic setting is crucial to data collection because one's privacy-related perceptions are largely shaped by his or her actual experience. Thus, in order for our subjects to respond meaningfully to our survey questionnaire, they were asked to interact on actual online social interaction platforms. Following past privacy research (e.g., Malhotra et al. 2004, Nowak and Phelps 1992, Sheehan and Hoy 2000, Son and Kim 2008), we used a survey questionnaire to measure the research variables in Figure 2.1.

Respondents were students from a public university in Singapore. 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 chatrooms, but less than half as many, only 5% of the next age bracket (25-year-old to 34-year-old) said they had done this" (p.37). Compared to other age groups, the age group of the university student had the highest percentage of Internet usage (i.e., 99%) IDA2012. Moreover, the extent of Singapore students who had used the Internet was highly comparable to that of students in the U.S. (i.e., 98%) (PEW 2013). Therefore, the student samples exemplified those who often participate in synchronous online social interactions.

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 S$25 each. The registration system captured their demographic information, Internet experience, and general chatroom 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 chatroom for further social interactions. Thus, they were allowed sufficient time to become familiarized with the allocated chatroom and to develop social relationships.[2] At the end of

[2] In order 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 chatroom over total

the third chat session, a survey was conducted to measure all research variables. The survey also captured demographic characteristics and other general items that might confound our finding. 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.

2.5 DATA ANALYSIS AND RESULTS

2.5.1 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 2.1. 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

concurrent chatroom users): (i) SpinChat [9.4%], (ii) ICQ [9.2%], (iii) JustaChat [6.0%], (iv) TalkCity [6.8%], (v) Yahoo!Chat [10.2%].

factor scores were then considered as indicator variables for privacy concerns. As one of the items measuring perceived anonymity of self (i.e., PAS2) had a low loading of 0.46, it was omitted. Since 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 .87 to .98 (see Table 2.2), thus indicating high internal consistency.

Table 2.1: 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.

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. 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 2.2 represent correlations of all latent variables, while the diagonal elements are the square roots of the Average Variances Extracted (AVE) of the latent variables. Data shown in Table 2.2 therefore satisfy this requirement.

Table 2.2: 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.

2.5.2 The Structural Model

The results of the structural model are presented in Figure 2.2. Out of 11 hypotheses, ten are supported. Perceived anonymity of self is found to be negatively related to privacy concerns (β=-0.20, $p<0.01$), but not social rewards, therefore H1 is supported and H2 is rejected. Consistent with our prediction, perceived anonymity of others is positively related to privacy concerns (β=0.20, $p<0.01$) but negatively related to social rewards (β=-0.24, $p<0.01$), thus supporting H3 and H4. As anticipated, perceived media richness

exhibits a positive influence on social rewards (β=0.28, $p<0.01$), hence supporting H5. Both H6 and H7 are also supported as perceived intrusiveness exhibits a positive relationship with privacy concerns (β=0.31, $p<0.01$), but a negative relationship with social rewards (β=-0.40, $p<0.01$). The results of the structural model indicated that the amount of variance explained by privacy concerns and social rewards were 20% and 35% respectively.

In addition, privacy concerns are found to have a negative impact on self disclosure (β=-0.16, $p<0.01$) but a positive impact on misrepresentation (β=0.14, $p<0.05$), and hence both H8 and H9 are supported. Conversely, social rewards have a positive impact on self disclosure (β=0.50, $p<0.01$) but a negative impact on misrepresentation (β=-0.22, $p<0.01$), thus supporting both H10 and H11. The variance explained by self disclosure and misrepresentation were 31% and 13% respectively.

In order to ensure that our findings are not confounded by other variables, we controlled for the possible effects of gender, age, Internet experience, general chatroom experience, chatroom 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 (β=-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.

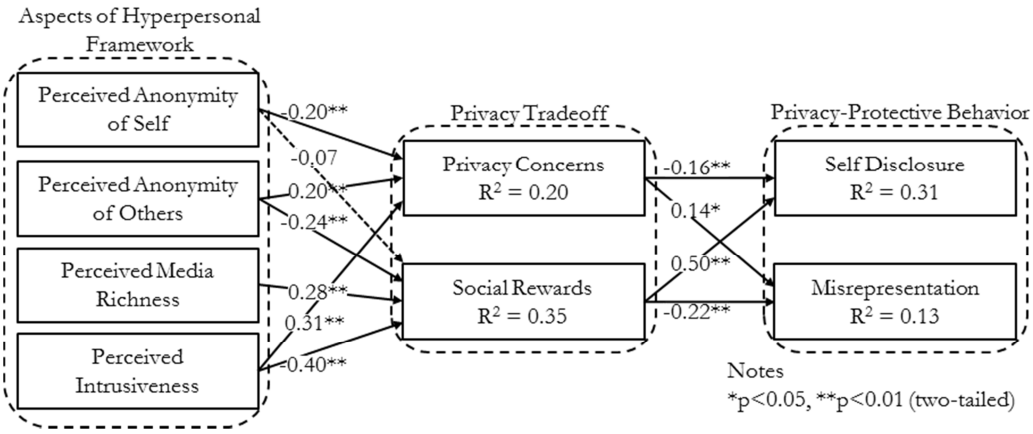


Figure 2.2. Study I Research Model Results (Completely Standardized Solutions)

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).[3] The results indeed confirm such mediation effects, with one exception. Although the effect of perceived intrusiveness on misrepresentation is mediated by privacy tradeoff 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 tradeoff 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

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

social rewards, as a whole, mediate the effects of the four antecedents on self disclosure and misrepresentation.

2.5.3 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 ten-factor model was estimated, which included eight constructs in the research model with privacy concerns consisting of three first-order factors.[4] Each of the 35 measurement items was restricted to being an indicator for the respective latent factor. Fit indices of the first model (α^2 (515) = 505.94) were as follows: α^2/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[5] and hence indicate a good fit of the model to the data.

In the second model, in addition to the ten 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 ten factors. The fit indices for the second model (α^2 (513) = 505.90) were largely identical to those of the first model (α^2/df = 1.01, SRMR = 0.463,

[4] The ten 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.

[5] 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] (Genfen et al. 2000; Hu and Bentler 1999; Tucker and Lewis 1973).

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 (α^2 (2) = 0.04, p = n.s.), suggesting that the common method bias was not a serious concern.

2.6 DISCUSSION AND CONCLUSION

2.6.1 Discussion of Results

The results are in support of our hypotheses, with one exception. 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. Overall, our findings suggest that the four aspects of the hyperpersonal framework and privacy tradeoff are the keys to a better understanding of individuals' privacy-protective behavior in synchronous online social interactions. This study provides researchers and practitioners with a theoretical framework for understanding the impact of

synchronous online social interactions on self disclosure and misrepresentation behavior.

Although perceived anonymity of self is expected to induce psychological detachment, thereby hindering the development of a socially rewarding experience, our results exhibit no significant relationship. A plausible explanation is that the negative effect of psychological detachment on social rewards may have been counteracted by the positive effect of self exploration and impression management on social rewards (Walther 2007). Specifically, as individuals are usually bound by social expectations, any deviance and nonconformity could generate social disapproval (Elster 1989). Staying unidentified, they could be true to their innate selves without experiencing social sanctions, especially when their views and beliefs dramatically differ from others. Hence, they may feel socially relieved and satisfied instead. In addition, perceived anonymity of self allows individuals to selectively present themselves (Leary and Kowalski 1990) to impose impression management. When others react positively to it, individuals would feel better off in comparison to others. Gaining higher self esteem, they find it socially rewarding. In sum, self exploration and impression management may counteract the effects of psychological detachment and hence, perceived anonymity of self as a whole is not significantly related to social rewards.

2.6.2 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 tradeoffs 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 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 non-optional 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.

2.6.3 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 due to 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 (β=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 due to 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.

Finally, this study considers privacy issues in synchronous online social interactions. It is worth noting that individuals might share vastly different types of information in developing online relationships. Consequently, individuals' privacy concerns could be affected by the information exchanged in synchronous online social interactions. Therefore, future research could explore the potential impact of information sensitivity on individuals' privacy concerns. Furthermore, the extent of information security and privacy protection mechanisms might vary in different online social interaction platforms. We believe that the theoretical framework presented in this study will provide a solid basis for examining additional antecedents of privacy concerns in online social interactions.

CHAPTER 3 STUDY II: EMBARRASSING EXPOSURES IN ONLINE SOCIAL NETWORKS: AN INTEGRATED PERSPECTIVE OF RELATIONSHIP BONDING AND PRIVACY INVASION

3.1 INTRODUCTION

Online social networking websites, such as Facebook and Twitter, provide an environment where individuals can easily maintain and develop social relationships by creating profiles with information about themselves and connecting their profiles to those of others (Bumgarner 2007; Ellison et al. 2011). These connections facilitate the exchange of socially meaningful information (such as birthday wishes and jokes) and the sharing of common interests (such as arts and sports) (McLaughlin and Vitak 2011). At times, for amusement, individuals may playfully tease each other by revealing their friends' embarrassing information. For instance, Wang et al. (2011) found that online social network users made a laugh at friends by revealing their indecent pictures and making playful comments about them. Indeed, the teasing literature suggests that embarrassing exposures could lead to relationship development. For example, Lange (2007) found that individuals enhanced interpersonal affinity by publicizing friends' mischiefs on online social networks and expressing mock disappointment at their embarrassing behavior. The author further noted that friends, who had become the target in the embarrassing exposure, sometimes did enjoy the humor and feel a strong sense of attachment with the individuals.

It has, however, been observed that the target of an embarrassing tease might not be amused but instead feel offended by the involuntary exposure

resulting from friends' postings about the target. For example, Kruger et al. (2006) found that a majority of the targets reported that they felt insulted as well as humiliated by the embarrassing exposure. Likewise, in a survey of 2,253 online social network users in the United States, one in five users aged 18 to 29 expressed displeasure towards involuntary exposure and requested their embarrassing information to be removed (Madden and Smith 2010), despite the benign nature of their friends' postings. Hence, it is interesting to investigate why targets interpret embarrassing exposure differently and how such interpretations influence their behavioral responses in online social networks.

This paper draws on the Social Exchange Theory as the overarching framework to elucidate the role of an embarrassing exposure in online social networking. This theory posits that an individual assesses a social exchange with reference to two important features of the exchange, namely (1) *exchange behavior* (i.e., the way the social exchange is conducted) and (2) *social relationship structure* (i.e., the structure of relationships between individuals involved in the social exchange) (Emerson 1972a; Emerson 1972b; Homans 1961). Correspondingly, to explore the impact of an embarrassing exposure (i.e., the exchange behavior) in a social exchange, this paper considers the way embarrassing information is involuntarily exposed through the posting and tagging mechanisms. Posting involves the publication of information about a target on the disseminator's profile. Tagging, which is performed in addition to posting, identifies the target in the information and associates the information to the target's profile. In addition, to represent the role that social

relationship structure plays in individuals' assessment of social exchange, we examine the *network mutuality* between the disseminator and the target. Whereas high network mutuality underscores high degree of commonality among the disseminator's and the target's social networks, low network mutuality denotes two largely distinct networks.

Furthermore, according to the Social Exchange Theory, the assessment of a social exchange entails the evaluation of two important components, namely exchange benefit and exchange cost (Blau 1986; Cook and Rice 2006). Whereas exchange benefit represents the resources individuals obtain from a social exchange, such as relational associations and recognitions, exchange cost involves the resources they devote to completing a social exchange, such as time and information (Molm et al. 2000). Following past research on social exchange, the first objective of this study is to investigate a target's benefit and cost perceptions related to an embarrassing exposure in online social networks. Specifically, in terms of benefit assessment, we rely on the teasing literature to understand the impact of an embarrassing exposure on the social relationship between the disseminator and the target. In terms of cost assessment, we rely on extant privacy research to elucidate the way an involuntary exposure intrudes the target's privacy. To the best of our knowledge, this study is among the first in the information systems (IS) literature to evaluate both the benefit and the cost of an embarrassing exposure in online social networks.

The second objective of this study is to investigate the target's behavioral responses to an embarrassing exposure. Previous IS research

suggests that privacy invasion leads to protective behavior, such as denial of information requests, relationship terminations, and complaints (e.g., Culnan and Williams 2009; Dinev and Hart 2006; Son and Kim 2008). However, there has been a paucity of research that examines individuals' responses associated with involuntary exposures of embarrassing information. While the privacy invasion associated with an involuntary exposure may induce relationship termination as well as withdrawal behavior, the humor implied by the exposure is known to stimulate the target's active involvement in interactions (Lampert and Ervin-Tripp 2006; Petronio 2002). To address this gap in prior research, we propose and empirically test a taxonomy of behavioral responses to embarrassing exposures in online social networks.

The remainder of the paper is organized as follows. The next section reviews previous literature and discusses the theoretical foundation for this study. The research model and hypotheses are then proposed, followed by the introduction of research methodology and the report of the data analysis results. This paper concludes with the discussion of theoretical and practical contributions, limitations, and avenues for future research.

3.2 LITERATURE REVIEW

In this section, we develop our theoretical perspective on embarrassing exposures in online social networks. We begin by reviewing the Social Exchange Theory, which serves as the overarching framework in integrating the teasing literature and privacy research. We then turn to the literature in teasing and extant research in privacy to understand individuals' exchange benefit perception and exchange cost perception associated with embarrassing

exposures. Finally, we review extant research in exchange response behavior to explore how individuals respond to embarrassing exposures.

3.2.1 Social Exchange Theory

A social exchange is a social interaction (or joint activity) in which two or more individuals are engaged in activities directed towards one another to exchange valuable resources, such as emotional support, time, and information (Homans 1958). The basic assumption of the Social Exchange Theory is that individuals engage in social interactions on the basis of their perceptions that such interactions are mutually advantageous (Blau 1964; Cook and Rice 2003).

While different views of social exchange have emerged, theorists agree that an individual's behavior in a social exchange is contingent on the behavior of others and the relationship structure in which the social exchange occurs. One example is the theoretical framework proposed by Homans (1961), which theorizes that an individual's response behavior in social exchange is shaped by the social behavior of others. Although the focus of this theoretical framework is on others' behavior in social exchange, it also emphasizes on the importance of exchange relationships in influencing an individual's responses (see Cook and Whitmeyer 1992). Emerson (1972a; 1972b), in his seminal works on the Social Exchange Theory, considers social behavior (similar to those proposed by Homans) and social structures as the central subject matters in shaping social interactions. Specifically, Emerson posits that the value of a social exchange is jointly determined by the behavioral attribute of an exchange and the structural attribute of exchange

networks. The seminal works by Emerson have been widely drawn upon as the theoretical basis in investigating social exchange (e.g., Brass and Burkhardt 1993; Molm 1990).

Following Homans (1961) and Emerson (1972a; 1972b), this study focuses on two important features of a social exchange, namely *exchange behavior* and *social relationship structure*. *Exchange behavior* describes communication actions performed by individuals in a social exchange process (Blau 1986; Cook and Whitmeyer 1992). While an embarrassing exposure can be voluntarily initiated through exchange behavior performed by individuals themselves (Collins and Miller 1994), their embarrassing information may also be involuntarily exposed through exchange behavior performed by others (Ellison et al. 2011; Lenhart and Madden 2007). In this study, we focus on the latter and examine two types of exchange behavior that can be performed by the information disseminator: Posting only and posting with tagging. *Posting only* is an information dissemination mechanism that publishes content on the disseminator's profile. When posting only is performed, the content has no explicit association with the target and is exposed to an audience within the disseminator's social network. *Posting with tagging* is a dissemination mechanism that not only publishes information in the disseminator's profile but also establishes an explicit association between the content and the target by creating a link in the content that directs the audience to the target's profile. Further, posting with tagging inserts the content into the target's profile and hence exposing the content to the social networks of both the disseminator and the target. When tagging is performed,

the disseminator also triggers a notification that alerts the target about the tagging.

Social relationship structure represents the social interconnectivity in networks of exchange relations (Cook and Rice 2006). In our study, the social relationship structure through which the disseminator is connected with the target is characterized by *network mutuality*, defined as the number of social connections the target has in common with the disseminator in online social networks. On one hand, high network mutuality typifies tightly-bounded relationships between two individuals who share largely common social circles. This commonality provides social assurance for benevolent interactions (Rempel et al. 1985), and hence individuals are particularly entrusting toward the social exchange (Molm et al. 2000; Wellman and Wortley 1990). On the other hand, low network mutuality characterizes sparsely-knit relationship structures, in which individuals have largely independent social circles. Such independence underscores the scarcity of social assurance, and hence individuals are especially prudent toward the social exchange (Granovetter 1973).

3.2.2 Social Exchange and Teasing

Teasing is a form of social exchange in which individuals are targeted in playful provocations, such as humorous remarks and sarcasms, which may involve the exposure of their embarrassing information (Keltner et al. 2001). Researchers suggest that teasing is typically evaluated in terms of the relationship bonding perceived by the target. Accordingly, we examine perceived relationship bonding, which refers the extent to which an individual

believes that an interaction leads to improved social relationship (Beatty and Lee 1996; Wilson 1995), as a major benefit the target derives from an involuntary exposure of embarrassing information.

Research on teasing theorizes that individuals' perception of relationship bonding is highly dependent on target participation, which allows the target to take part in a teasing interaction (Keltner et al. 1998). Teasing between friends is commonly considered a positive bonding experience when the tease is made with the participation of the target (Campos et al. 2007). In a study examining conversational humor, Lampert and Ervin-Tripp (2006) examined personal humorous remarks in conversions and revealed that the target considered embarrassing comments among friends as bonding jokes when he or she was present as part of the conversation group. Nevertheless, teasing is at times concluded as a negative bonding experience when embarrassing information is exposed with the exclusion of target participation. In fact, the target might see such communications as rumors spread to damage his or her reputation (Terrion and Ashforth 2002). For instance, Foster (2004) noted that individuals considered communications inappropriate when their private matters were being talked about behind their backs.

The teasing literature also suggests that the effect of target participation on relationship bonding can be influenced by the type of audience of the involuntary dissemination of embarrassing information (Jones et al. 2005). In online social networks, the type of audience can be determined by the extent of network interconnectivity between the target and the disseminator. High interconnectivity typifies an audience type that consists

largely of the target's social networks. The acquainted nature of this audience type encourages individuals to attend to the humorous nature of the teasing communication (Keltner et al. 1998). On the contrary, low interconnectivity depicts an audience type that consists largely of social networks unknown to the target. The unknown nature of such audience type alerts individuals about the humiliating nature of a targeted tease. For instance, Alberts et al. (1996) asserted that audience type influenced individuals' perceptions of embarrassing conversations they had, such as the discussion about sex life, physical shortcomings, or inabilities. Specifically, when the audience was made up of closely related others, individuals perceived the embarrassing interaction as a manifestation of affiliations. However, when the embarrassing information was exposed mainly to distantly affiliated others, individuals considered the exposure as direct humiliation.

In essence, the teasing literature suggests that relationship bonding is an important benefit individuals could experience in an involuntary exposure of embarrassing information; and that experience of relationship bonding could be influenced by both target participation and audience type.

3.2.3 Social Exchange and Privacy

Researchers suggest that individuals do not only consider the benefit of a social exchange in terms of relationship bonding but are also concerned about the cost in terms of privacy associated with the involuntary exposure of embarrassing information (Petronio et al. 1989; Solove 2006). IS research has progressed significantly in enriching our understanding of privacy. Extant research has focused predominantly on examining privacy issues in online

commercial transactions (e.g., Awad and Krishnan 2006; Bélanger and Crossler 2011; Dinev and Hart 2006; Pavlou 2011; Smith et al. 2011). Some studies have investigated privacy problems (such as identity theft and stalking) in online social networks (e.g., Hoadley et al. 2010; Lewis et al. 2008). Evidence suggests that when individuals' embarrassing information is exposed involuntarily, individuals' perception of invasion of privacy becomes particularly aggravated (e.g., Debatin et al. 2009). In this study, we examine perceived privacy invasion, which refers to the extent to which an individual believes that his or her personal information space is intruded by others (Tolchinsky et al. 1981), as the major cost individuals experience in an involuntary embarrassing exposure.

The extent of privacy invasion individuals experience can be explained and predicted by two important mechanisms, namely target individuation and exposure size (e.g., Altman and Taylor 1973). Target individuation is a state in which individuals are being made explicitly identifiable through distinct identity reference (Maslach et al. 1985). Whereas a high level of target individuation connotes explicit identification of individuals and hence elevating individuals' perception of privacy invasion, a low level of target individuation represents submergence of identity information within an exposure and is known to limit individuals' perception of privacy invasion (Postmes and Spears 1998). In the online environment, high target individuation can be imposed by making individuals' personal profiles (in which identity information resides) traceable from the exposure. For instance, in a study on online social networks, Raynes-Goldie (2010) found that when

individuals' profiles were not traceable from embarrassing content posted by others, they were less concerned about privacy because readers of the embarrassing content might not know their identity. On the contrary, when their profiles were traceable in the embarrassing information, they became more apprehensive of privacy invasion.

Exposure size depicts the number of recipients in audience to the involuntary dissemination of embarrassing information (Acquisti and Gross 2006). In online social networks, the size of an embarrassing exposure is contingent on the extent of network interconnectivity between the target and the disseminator. High interconnectivity implies that the size of the exposure largely consists of a social network shared by the disseminator and the target. To illustrate, when all of the target's social network friends are also friends of the disseminator, the exposure size is entirely determined by the social networks of the disseminator, which encapsulates those of the target. This implies that the size of the embarrassing exposure can be limited by high interconnectivity. In contrast, low interconnectivity hints at an exposure size potentially consisting of two largely distinct social networks. This suggests that the size of the embarrassing exposure can be escalated by low interconnectivity. Empirical evidence has substantiated the role of exposure size in moderating the effect of target individuation on perceived privacy invasion. For example, Petronio (2002) examined the way in which exposure size shaped the effect of individuation on individuals' privacy perception in embarrassing social interactions. When their embarrassing information was discussed among a limited number of interactants, such discussions were

typically seen as a small-size exposure in which the embarrassing conversation was contained within the few interactants. The author noted that such small-size exposure diminished the effect of individuation on privacy invasion. However, when the exposure escalated beyond a limited number of interactants, the discussions were seen as a large-size exposure. As a result, the role of individuation in elevating individuals' perception of privacy invasion was amplified.

In summary, based on past privacy research, target individuation and exposure size are two key influences on individuals' perception of privacy invasion, which is regarded as the main cost in an involuntary exposure of embarrassing information.

3.2.4 Social Exchange and Response Behavior

The Social Exchange Theory contends that individuals' assessment of benefit and cost determines their behavioral responses (Blau 1986; Cook and Rice 2006). Past studies examining exchange responses suggest that individuals may engage in a myriad of behavior, such as expression of affiliation, acknowledgement, and mutual disclosure (Archer and Berg 1978; Collins and Miller 1994). Kuhl (1981) classified response behavior into a dichotomy of *passive* and *active* behavior. Passive behavior reflects inertia to act in response to social exchange. It is essentially an inaction strategy, which maintains a static orientation in social exchange through ignorance, negligence, or procrastination (Harris and Sutton 1983; Rusbult et al. 1988).

On the contrary, active behavior encompasses *avoidance* and *approach* strategies in response to social exchange (Higgins 1998). Whereas the

avoidance strategy is about shunning away from interactions and keeping a distance from others, the approach strategy is about "going to, heading for, or striving after" others in social exchange (Marsh et al. 2005). The *avoidance* strategy can be exercised at the transactional level and the interpersonal level (e.g., Burgoon et al. 1989; Ting-Toomey and Oetzel 2001). At the transactional level, individuals engage in avoidance by excusing themselves from an interaction. At the interpersonal level, avoidance strategy is performed in terms of relationship severance. For example, Sias and Perry (2004) examined communication behavior at workplace and found that others' adverse interactions induced two levels of avoidance behavior. In particular, they revealed that individuals took on transactional avoidance by staying away from others' phone calls and performed interpersonal avoidance through cutting off relational ties. The *approach* strategy, in contrast, is typically performed through individuals' pursuit of further interaction. For example, Drew (1987) found that individuals actively approached others' teases by supplying a related comment in return. Likewise, Alberts (1992) noted that tease targets responded to teasing interactions by actively participating in the subsequent conversations.

3.3 RESEARCH MODEL AND HYPOTHESIS DEVELOPMENT

The research model integrates the Social Exchange Theory with the teasing research and the privacy literature to explain the consequences of an embarrassing exposure in online social networks (see Figure 3.1).

Within the social exchange framework, the basic theoretical unit is the exchange of resources between two actors. In particular, an actor initiates the

social exchange by offering resources to an exchange partner through exchange behavior. More important, according to the social exchange theory, this exchange behavior is a choice behavior that the actor must choose among alternative behaviors that produce specific value for the partner. Indeed, scholars have categorically pointed out the importance of this behavioral basis of the social exchange theory. For example, Molm (1990) examined the dynamics of power in social exchange and found that individuals exercised their power by strategically taking on exchange behavior that produced monetary rewards or punishment to exchange partners. Likewise, Molm et al. (2003) found that given constant exchange value, individuals' perception of exchange outcome was determined by how the outcome was obtained through the fairness of others' exchange behavior. In the context of embarrassing exposures, scholars have paid special attention on the way embarrassing information is involuntarily disseminated. Consistent with the social exchange theory, embarrassing exposures occur when embarrassing information is involuntarily publicized through others' communication behavior. For instance, Boxer and Cortes-Conde (1997) found that the way embarrassing information was communicated to others helped define the nature of the communications. While embarrassing information communicated with the presence of the target was considered humorous and enhanced bonding, communications made in the absence of the target were deemed humiliating and relationship threatening. Likewise, Alberts (1992) noted that playful exposures were directed at the target with an invitation to join the interactions, whereas cruel exposures were often presented with an absent victim.

Research examining online social networking has identified information dissemination to be a key technical feature that facilitates social interactions. For example, Greenhow and Robelia (2009) noted that posting and tagging enabled sustainable social interactions through information sharing in online social networks. Unlike information sharing in offline social interactions, posting and tagging disseminate information which is duplicable and intransient. In a study on social popularity, Zywica and Danowski (2008) reported that posting and tagging did not only promote self-presentation but also formed an important indication of social popularity on Facebook. Specifically, when Facebook users had more posting on their walls and content tagged by friends, they perceived higher popularity. Similarly, Carpenter and Spottswood (2013) examined online social networking behavior of couples and found that tagging was frequently used to convey intimacy. Therefore, to reflect the importance of others' exchange behavior in an online embarrassing exposure, this study examines the disseminator's behavior in exposing the embarrassing information. Specifically, the exchange behavior of the disseminator is studied in two modes of information dissemination, i.e., posting only vs. posting with tagging.

Social exchange theorists have unambiguously conceptualized network structure as a configuration of social relations (i.e., as a set of actors diversely linked in a social network), where valued items, such as symbolic, material, and information, are exchanged among actors. For example, according to Homans' (1961, 1964) theorization of social exchange structure, whereas the relations between actors in direct contact with one another play an important

role in shaping social exchange, the indirect relationships between the two actors underpins the overall social exchange structure. Likewise, Emerson (1972ab) emphasizes on the macro orientation of social structure. In his view, individuals understand dyadic social exchange based on common values, which are implied by the patterns of connections among exchange actors. Extending Emerson's emphasis of network structure in shaping social exchange, Cook and Whitmeyer (1992) posit that network structure might manifest in several key properties, such as network density (i.e., the amount of secondary connections between actors), structural equivalence (i.e., having equivalent ties to the same other actors), and structural cohesion (i.e., being closely tied to each other). Indeed, ample empirical studies have demonstrated the importance of network structure in social exchange. For example, Grosser et al. (2010) drew on social exchange theory to examine the effects of network structures on gossiping behavior. In particular, the authors focused on the impact of structural embeddedness, which refers to the extent that friends have mutual friends in common, on gossiping behavior in social networks. Likewise, Fox et al. (forthcoming) found that the amount of common friends provided Facebook users the social context in which they developed perceptions of romantic relationships.

More importantly, social network research has established that network commonality is a key network structure attribute in understanding social exchange. For instance, in a study examining the exchange of product information on social media, Soh (2014) found that network commonality was the primary indicator of how the network environment was structured and

individuals paid special attention to network commonality in evaluating the value of the product information they contributed to their peers. Likewise, Zohar and Tenne-Gazit (2008) found that the number of paths connecting actors in a social network helped promote social exchange and enhanced the formation of organizational climate. Hence, to elucidate the role of social relationship structure in an online embarrassing exposure, this study examines the network mutuality between the disseminator and target. In particular, we study two types of network mutuality, i.e., low network mutuality vs. high network mutuality.

The effects of these two independent variables on individuals' assessment of social exchange are investigated in terms of *perceived relationship bonding* and *perceived privacy invasion.* In addition, we assess the effects of these two perceptions on individuals' behavioral responses to the embarrassing exposure.

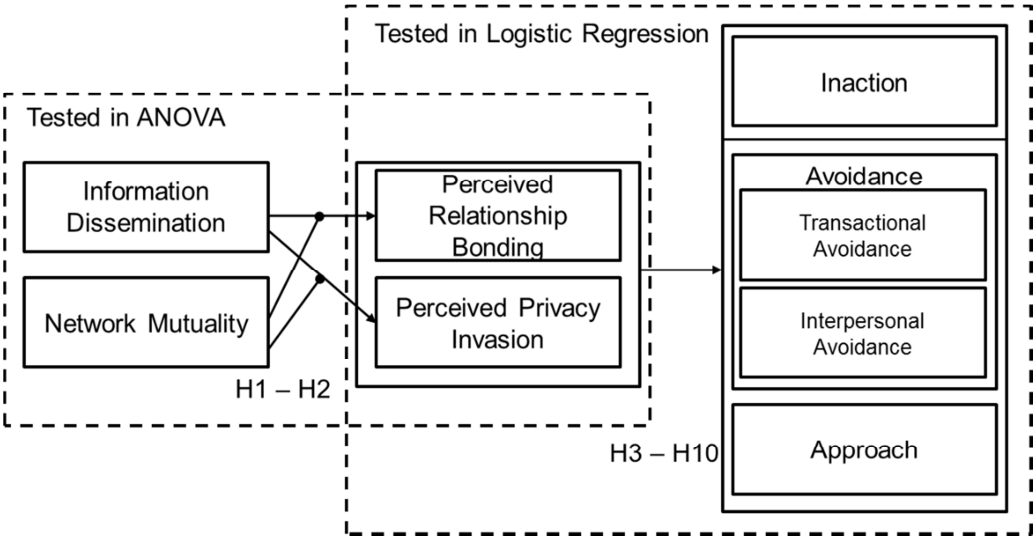


Figure 3.1. Study II Research Model

3.3.1 Determinants of Perceived Relationship Bonding

The teasing literature suggests that audience type influences the impact of target participation on individuals' perception of relationship bonding (e.g., Alberts et al. 1996). In online social networks, as mentioned earlier, network mutuality succinctly determines the types of audience in an involuntary exposure of embarrassing information. In cases of low network mutuality, the target's social network and the disseminator's social network are largely distinct. Therefore, friends of the disseminator, who are likely unknown to the target, form a substantial part of the audience regardless of the presence or absence of tags. This unacquainted audience type induces prudence in the target's interpretation of the way in which the embarrassing information is disseminated (Tedeschi 2001). In particular, when the embarrassing information is posted with tagging, the target is made the subject of a mockery in front of an unacquainted audience and hence might interpret the embarrassing exposure as a direct humiliation (Kotthoff 2003). Moreover, posting with tagging explicitly associates the embarrassing information with the target. This association deprives the target from remaining anonymous in the exposure and hence he or she is likely to be affronted by the dissemination. Posting only, however, does not explicitly turn the target into the subject of a humiliating communication about him or her. Furthermore, posting only allows the target to remain anonymous in the dissemination and hence he or she might not be seriously offended by the embarrassing exposure to an unacquainted audience. As such, when the embarrassing information is posted only, the target will feel less offended than when the information is posted with tagging (Turner et al. 2003). In essence, when network mutuality is low,

posting with tagging constitutes a direct humiliation and hence will lead to lower perception of relationship bonding when compared to posting only.

On the contrary, when network mutuality is high, the social network of the target is highly similar to that of the disseminator. As a result, the audience of the embarrassing exposure consists mainly of the target's and disseminator's mutual friends. This acquainted audience provides the social assurance that the embarrassing exposure is benign and helps emphasize the positive impact of target notification on the target's perception of the humorous interaction (Boxer and Cortés-Conde 1997). In particular, in the absence of target notification, as in the case of posting only, the target will be excluded from participating in the teasing interactions with friends. In contrast, posting with tagging explicitly notifies the target about the embarrassing exposure, an act that ensures target participation in the teasing interactions among friends. Given the acquainted audience type, the target is likely to consider the embarrassing exposure an unequivocal humor (Keltner et al. 2001). Therefore, in high network mutuality condition, posting with tagging connotes stronger interpersonal affiliation and hence reinforces the perception of relationship bonding between the disseminator and the target when compared to posting only. Thus, we predict the following effects:

H1a: In the low network mutuality condition, compared to posting only, posting with tagging will lead to lower level of perceived relationship bonding when embarrassing information is disseminated.

H1b: In the high network mutuality condition, compared to posting only, posting with tagging will lead to higher level of perceived relationship bonding when embarrassing information is disseminated.

3.3.2 Determinants of Perceived Privacy Invasion

Past privacy research suggests that the effect of target individuation on perceived privacy invasion is moderated by the size of an exposure (e.g., Petronio 2002). In cases of low network mutuality, the target's social network is mostly distinct from that of the disseminator. As such, when the embarrassing information is posted only, the target is likely to conclude that the exposure size is limited to the disseminator's social network (Postmes and Spears 1998). Posting with tagging, however, leads to an enlarged overall size of exposure when compared to posting only, as the embarrassing information is also exposed to the social network of the target. Furthermore, posting with tagging associates the target's profile to the embarrassing information. Through this association, the target's identity in the information becomes explicitly traceable by the audience. This explicit traceability helps accentuate target individuation, which draws the audience's attention to the target. Therefore, when network mutuality is low, the enlargement of exposure size and the individuation of the target enabled by posting with tagging will enhance the target's perception of privacy invasion.

In contrast, when network mutuality is high, the target's social network is highly convergent with that of the disseminator. Therefore, posting with tagging is not likely to contribute to a significant gain in overall exposure size when compared to posting only. High network mutuality also implies that the

social networks of the target constitute most of the audience. Being the target's social network friends, this audience is likely to individuate the target in the exposure regardless of the presence or absence of profile association enabled by tagging. Therefore, when network mutuality is high, the increase in the target's perception of privacy invasion associated with posting with tagging will not be as marked as when network mutuality is low. We thus predict the following hypothesis:

H2: Compared to posting only, posting with tagging will lead to an increase in perceived privacy invasion and this increase is more pronounced in the low network mutuality condition than in the high network mutuality condition.

3.3.3 Behavioral Responses

Drawing on the Social Exchange Theory and Kuhl's (1981) classification of response behavior, this study proposes four types of behavioral responses to an embarrassing exposure, namely *inaction*, *transactional avoidance*, *interpersonal avoidance,* and *approach*. First, *inaction* refers to the target's assumption of indolence in an embarrassing exposure. By taking no action, individuals demonstrate their apathy and disinterests regarding the exposure. Second, *transactional avoidance*, refers to the extent to which the target actively dissociates himself or herself from the embarrassing information. In online social networks, through transactional avoidance, individuals aim to stop the embarrassing information from being further disseminated. Third, *interpersonal avoidance* is defined as the extent to which the target actively terminates his or her relationship with the

disseminator. Individuals typically dissociate themselves from unsatisfactory relationships but enhance their relational associations with decent others. Lastly, *approach* refers to the extent to which the target actively engages in the social interactions associated with the embarrassing exposure. Whereas *transactional avoidance* and *interpersonal avoidance* focus on detachment and dissociation that hinder further social exchange, *approach* considers the target's involvement behavior that completes a social exchange.

3.3.3.1 Perceived Relationship Bonding and Inaction

Perceived relationship bonding is expected to reduce inaction. According to the social exchange framework, individuals' emotional attachment to others induces obligation to offer others socio-emotional resources, such as approval, respect, and support (Eisenberger et al. 2001). Hence, when a target perceives strong relationship bonding with the disseminator, the target is likely to feel obligated to act up to his or her relational role by devoting increased socio-emotional resources to the disseminator. Accordingly, the target who perceives relationship bonding will be less likely to assume inaction.

Additionally, the target who perceives relationship bonding may refrain from not responding because inaction may wrongly hint at the target's impassivity toward the disseminator. When the target responds through inaction, the disseminator is essentially given a "cold shoulder", suggesting that the target neglects or ignores the affiliating behavior. As a result, the disseminator may feel dejected and unappreciated by the target. Moreover, inaction may be perceived as an indication of relationship de-escalation in

which the target drives the social relationship towards deterioration (Lipkus and Bissonnette 1996). Therefore, when the target perceives higher relationship bonding, he or she will be less willing to assume inaction.

H3: Perceived relationship bonding will reduce the likelihood of inaction.

3.3.3.2 Perceived Relationship Bonding and Avoidance

Past research suggests that perception of relationship bonding impedes avoidance behavior (Campos et al. 2007; Rusbult and Buunk 1993). Specifically, as transactional avoidance interrupts social communications, its enactment may bring an abrupt end to an affiliating interaction. Hence, the target who perceives relationship bonding is likely to continue his or her association with the dissemination and/or be reluctant to dispute the embarrassing exposure.

Furthermore, perceived relationship bonding represents increased emotional and cognitive attachment between the target and the disseminator (Aron et al. 1992). The elevated level of emotional and cognitive attachment induces additional motivations for the target to assume a long-term orientation in the relationship (Agnew et al. 1998). Therefore, when the target perceives higher relationship bonding, he or she will be more eager to remain in the relationship and less willing to engage in interpersonal avoidance.

H4: Perceived relationship bonding will reduce the likelihood of transactional avoidance.

H5: Perceived relationship bonding will reduce the likelihood of interpersonal avoidance.

3.3.3.3 Perceived Relationship Bonding and Approach

Approach behavior is essential in maintaining the relationship bonding derived from a social exchange (Firestone 1977). For example, Tidwell and Walther (2002) examined social exchange in computer-mediated communication and found that individuals maintained socially meaningful interactions by increasing interaction involvement, such as providing prompt responses, engaging in deep self-discloses, and asking personal questions. In a study examining interpersonal teasing, Boxer and Cortés-Conde (1997) revealed that relationship bonding derived from teasing prompted interlocutors to maintain the interaction by teasing back at each other. Approach behavior can also be understood as feedback in social exchange, in that the target acknowledges the social exchange initiated by the disseminator (Lawler and Thye 1999). Consequently, a target with strong perception of relationship bonding will engage in approach behavior in response to an embarrassing exposure.

H6: Perceived relationship bonding will increase the likelihood of approach behavior.

3.3.3.4 Perceived Privacy Invasion and Inaction

Perception of privacy invasion provides strong reasons for the target to resign from inaction. Specifically, invasion of privacy exposes the target to ridicules and defamation in a social exchange (Abril 2007). Taking no action against the involuntary exposure of his or her embarrassing information (by

keeping silent or ignoring the exposure) will not only sustain the privacy invasion but also express the target's apathy towards privacy invasion and tolerance of the exploitation. Past studies suggest that privacy invasion discourages the target from assuming inaction. For example, Debatin et al. (2009) examined self-disclosure in online social networks and found that individuals who experienced limited privacy invasion generally ignored taking active actions to protect their privacy. However, those who had personally experienced severe privacy invasion departed from inaction and engaged in active responses. Therefore, perceived privacy invasion is expected to dissuade the target from assuming inaction.

H7: Perceived privacy invasion will reduce the likelihood of inaction.

3.3.3.5 Perceived Privacy Invasion and Avoidance

Perceive privacy invasion is expected to induce avoidance at both the transactional level and the interpersonal level. At the transaction level, the target's perception of privacy invasion accentuates concerns about his or her association with the embarrassing information. In particular, a target who perceives high privacy invasion is likely to believe that the embarrassing exposure has fundamentally intruded his or her private space in online social networks. To re-establish the privacy space, the target may actively distance himself or herself from the embarrassing exposure (Greenberg and Firestone 1977). For instance, the target may mark the dissemination as spam to notify the service provider about the abuse. The target may also protest against the dissemination by reporting it to the online social network operator. By marking the dissemination as spam and/or protesting to the operator, the target

aims to prevent such embarrassing information from staying visible in online social networks.

In addition to performing avoidance at the transactional level, a target who perceives high privacy invasion may actively engage in interpersonal avoidance through relationship dissolution (Petronio 1991). By withdrawing affiliation with the disseminator, the target avoids subjecting himself or herself to further privacy invasion. Son and Kim (2008) offered empirical evidence to support such an assertion. They found that individuals who were concerned about privacy withdrew their relationship with the online vendor and filed complaints against the vendor. In online social networks, the target may simply terminate his or her social connection with the disseminator. Additionally, the target may lodge a report to the online social network operator to complain against the disseminator. Such behavior may be motivated by the target's desire to terminate the relationship with the disseminator. We therefore hypothesize perceived privacy invasion as an important determinant of both transactional avoidance and interpersonal avoidance.

H8: Perceived privacy invasion will increase the likelihood of transactional avoidance.

H9: Perceived privacy invasion will increase the likelihood of interpersonal avoidance.

3.3.3.6 Perceived Privacy Invasion and Approach

Approach behavior not only draws the target towards the embarrassing exposure but also makes him or her vulnerable to further privacy invasion (Drew 1987). When the target engages in approach behavior, the disseminator can be instigated by the target's active involvement and hence engage in further embarrassing exposures. Past research suggests that individuals' perception of privacy invasion reduces approach behavior in online exchange. For instance, Youn (2005) examined online privacy protective behavior and revealed that Internet users coped with privacy invasions by reducing information provision to online firms and limiting participation in online transactions. Thus, we hypothesize:

H10: Perceived privacy invasion will reduce the likelihood of approach behavior.

3.4 RESEARCH METHOD

Facebook is chosen as the online social network platform for the present study for two reasons: (1) It provides functionalities such as information posting as well as content tagging, and thus is a suitable platform for information dissemination; (2) it is widely used and thus findings from the present study may have greater generalizability to the general online social network user population.

3.4.1 Experimental Design

A laboratory experiment with 2 (*Information Dissemination*: Posting only vs. Posting with Tagging) x 2 (*Network Mutuality*: Low vs. High) factorial design was conducted to test the proposed hypotheses. Information

dissemination was manipulated by the exclusion and inclusion of tagging on a note published on the disseminator's profile. Network mutuality was facilitated by manipulating the number of shared friends the target has in common with the disseminator. Evidence suggests that an average Facebook user has 130 friends in his or her friend list and the average number of mutual friends shared by two Facebook friends is 35 (Eldon 2010; Mavridis et al. 2010). Accordingly, low network mutuality was represented by 7 shared friends, which is about 5% of the average number of friends a user has, whereas high network mutuality was represented by 65 shared friends, which is about 50% of the average number of friends per user.

Our experiment involved a stimulation of an online embarrassing exposure using a hypothetical scenario. (Brass and Burkhardt 1993; Greenberg and Eskew 1993). Hypothetical scenarios have been used in previous IS and privacy research (e.g., Anderson and Agarwal 2011; Grace 2009; Sheehan and Hoy 2000; Tragesser and Lippman 2005) and this method is particularly valid for this study due to three important reasons. First, social networks are highly personal, so it is difficult to create such an artificial environment in a lab that resembles users' actual social networks experience. Second, although a field experiment might better mimic an actual situation, it is not possible to administrate the experimental conditions that involve credible embarrassing treatments without impairing the realism of the treatments. As a result, subjects' true perceptions and responses might be undermined. Lastly, if a survey was used, it would not be practical for subjects to report their responses toward an embarrassing exposure. This is because some of them might not

have experienced such embarrassment in online social networks and even if some had, it would be extremely challenging, if not impossible, for them to vividly recall the entire incident in order to respond to survey questions.

A pilot test with 20 subjects was conducted prior to the main experiment to assess the appropriateness of the experimental stimulus (i.e., the note publication scenario that exposes an embarrassing incident). Subjects were instructed to go through five incidents (i.e., shopping for condoms, purchasing disposal underwear, kissing on the subway, reading adult magazine, and sleeping in lecture), which were typical embarrassing situations occurring at public settings and observable by others (Dahl et al. 2001; Sabini et al. 2001). They were asked to imagine that each of the incidents was published in a Facebook note and then rated on the perceived *embarrassment*[6] caused by the note and judge the extent to which each incident was *relevant*[7] to people like themselves (Table 3.1).

Results showed that all five scenarios were embarrassing (mean = 6.08). No significant differences were found among the scenarios with respect to perceived embarrassment ($F(4, 95) = 1.45$, $p = 0.22$).

[6] Perceived embarrassment represents the extent to which a person is uncomfortable about the note publication. It was measured by three 7-point Likert scale items based on Sabini et al. (2000): "The note publication makes me embarrassed," "The note publication makes me feel awkward," and "The note publication makes me feel uncomfortable."

[7] Perceived relevance represents the extent to which a person believes that the embarrassing incident is meaningful to him or her. It was measured by three 7-point Likert scale items based on Zaichkowsky (1985): "The incident discussed in the note is important to people like myself," "The incident discussed in the note matters to people like myself," and "The incident discussed in the note is significant to people like myself".

Table 3.1: Means of the Five Scenarios

Incident	Perceived Embarrassment		Perceived Relevance	
	M	SD	M	SD
A	6.23	0.68	3.54	0.73
B	5.80	0.96	4.29	0.77
C	5.95	0.71	4.35	0.49
D	6.15	0.69	2.13	0.75
E	6.28	0.69	6.03	0.73

Notes:
A = Shopping for Condoms
B = Purchasing Disposal Underwear
C = Kissing on the Subway
D = Reading Adult Magazine
E = Sleeping in Lecture

In addition, the exposure scenario depicting the subjects sleeping in a lecture theatre (i.e., the note, see Table 3.2) was rated by the subjects as the most relevant (mean = 6.03), hence it was selected as the stimulus for this study.

Table 3.2: Embarrassing Scenario[8]

Note Title: Caught Sleeping in Lecture
Note Content: I was sitting somewhere in the middle of the lecture theatre just now. After about 30 minutes of lecture, I started to feel really tired and begun stretching my neck. While turning my head around for the stretch, I somehow realized [subject's nickname] was also in the LT![9] I was thinking that he/she was also doing some neck stretches, but I was wrong! I realized he/she was actually falling asleep and jerking his/her head left and right. Besides jerking his/her head around, he/she was dripping saliva from his/her mouth! Then out of a sudden, he/she banged his/her head onto the desk! It was a really hard hit and the whole LT was shocked by the BANG sound! I am sure it wakes you up for the rest of the lecture yeah? Lolx :p

3.4.2 Sample and Experimental Procedures

Subjects in this experiment were students at a large public university in South-East Asia. Prior to the experiment, subjects were asked to provide information about demographics, Internet experience, Facebook experience, and their names commonly known by their friends. They were also assessed

[8] The embarrassing scenario was customized for each subject by reflecting his or her nickname (or the name typically known by his or her friends) and gender, which were obtained prior to the experiment.
[9] LT is the abbreviation of lecture theatre.

in terms of perceived network closeness, shyness, and sociability. One week before the experiment, subjects attended an online Facebook training on several key technical features, such as posting, tagging, and social browsing. Upon completing the training, subjects were given an online quiz of 20 multiple choice questions to assess their understanding of the technology features. On average, subjects provided 18 correct answers. These results show that subjects had concrete understanding of the key technical features (i.e., posting and tagging).

Subjects were also instructed to send friend requests to a research Facebook account. Subjects were informed that their profile information would be collected for the purpose of this study. One day before the experiment, the research account was used to capture the profile information of each subject. The captured information included the subject's profile page, wall postings for the past three months, photo albums, and the note section. All subjects were shown to have experience in being tagged in contents posted by others. Furthermore, they were found to have used Facebook actively for the past three months.

In order to ensure sufficient power (0.8) with a medium effect size for a 2 x 2 between-subjects factorial design, 109 subjects, who did not take part in the pilot study, were recruited to participate in the experiment.

Table 3.3: Experimental Conditions

	Low Network Mutuality	High Network Mutuality
Posting Only	N = 27	N = 28
Posting with Tagging	N = 28	N = 26

Subjects were randomly assigned to one of the four experimental conditions (Table 3.3) in a mock-up Facebook environment that mimicked actual Facebook layout and technology features (e.g., sponsored advertisements and comment) as well as customized with the subjects' actual Facebook profile information (i.e., profile names and profile pictures). They were presented with a hypothetical scenario in which an imaginary friend (i.e., denoted by the name "X" and a unisex avatar), who shared 7 mutual Facebook friends (or 65 mutual Facebook friends, see P.20 for the choice of 7 vs. 65) with the subjects, had posted (and tagged them to) a note in the mock-up environment. To ensure realism, the note was personalized with subjects' genders and names commonly known by others. Subjects were told to imagine that the scenario was real and read through it carefully. Afterwards, subjects were instructed to complete a questionnaire that contained manipulation checks and measurement items of the research variables. Subsequently, they were given the option to respond (or not to respond) to the note published in the mock-up environment (see Figure 3.2). Upon completing their responses in the mock-up environment, subjects were debriefed and thanked.

Notes:

1 = No response
2 = Mark the note as spam
3 = Report the note to Facebook
4 = Remove the disseminator as a Facebook friend
5 = Report the disseminator to Facebook
6 = Write a public comment
7 = Send a private message
A = Note content

Figure 3.2. Study II Mock-Up Facebook Environment

3.5 DATA ANALYSIS

3.5.1 Subject Demographics and Background Analysis

Among the 109 subjects participating in the study, 52 were females. The age of the subjects ranged from 18 to 25, with average Internet experience and average Facebook experience being 7.3 years and 3.7 years, respectively. The average time a subject spent to complete the entire experiment was 30.4 minutes.

No significant differences were found among subjects randomly assigned to each of the four experimental conditions with respect to age,

gender, Internet experience, and Facebook experience, indicating that subjects' demographics were quite homogeneous across different conditions.

3.5.2 Measurement

The manipulation check for *information dissemination* was performed by asking subjects three true/false questions on whether the information was disseminated with tagging (see Appendix E for manipulation check items). All subjects in the posting only condition answered "false" to the three questions and all those in the posting with tagging condition answered "true", hence suggesting that the manipulation for information dissemination was successful. Manipulation check for *network mutuality* was conducted by asking subjects to rate on four items, measuring the extent to which their social networks overlapped with those of the disseminator. On a seven-point Likert scale, subjects in the low network mutuality condition reported a mean value of 2.57 for the extent of network overlap (standard deviation = 0.52) and subjects in the high network mutuality condition reported a mean value of 5.58 for the extent of network overlap (standard deviation = 0.57). The difference was significant (t = -28.89, p <0.01), and hence the manipulation for network mutuality worked as anticipated.

Five items measuring *perceived relationship bonding* were adapted from Wheeless and Grotz (1976) and Murray et al. (1996) (Cronbach's alpha = 0.90) (see Appendix E). Four items measuring *perceived privacy invasion* were adapted from Fusilier and Hoyer (1980) and Alge (2001) (Cronbach's alpha = 0.82). Three items measuring *perceived network closeness* were adapted from Floyd and Parks (1995) (Cronbach's alpha = 0.81). Three items

measuring sociability (Cronbach's alpha = 0.87) and three items measuring shyness (Cronbach's alpha = 0.83) were adapted from Cheek and Buss (1981). Exploratory factor analysis shows that, in general, items load well on their intended factors and lightly on the other factor, thus indicating adequate construct validity (see Table 3.4). The correlation between perceived relationship bonding and perceived privacy invasion was -0.18 (p =0.06).

Table 3.4: Rotated Factor Loadings

	PRB	PPI	PNC	SHY	SOC
PRB1	.011	**.870**	.023	.029	-.003
PRB2	-.013	**.853**	.032	.054	-.019
PRB3	-.071	**.870**	.002	.043	-.020
PRB4	-.026	**.804**	.017	.023	-.024
PRB5	-.001	**.843**	.021	.035	-.027
PPI1	**.779**	.119	.011	-.008	.027
PPI2	**.815**	.052	.017	-.045	.043
PPI3	**.830**	-.170	.025	-.051	.055
PPI4	**.787**	-.093	.027	-.034	.052
PNC1	.028	.002	**.823**	.017	.005
PNC2	.018	.011	**.865**	.013	.009
PNC3	.002	.021	**.888**	.021	.012
SHY1	.030	-.003	.013	**.768**	-.310
SHY2	.066	-.054	.018	**.840**	-.238
SHY3	.045	-.045	.026	**.832**	-.349
SOC1	-.012	.026	.002	-.388	**.882**
SOC2	-.023	.043	.010	-.320	**.850**
SOC3	-.009	.065	.013	-.318	**.849**

Notes:
PRB = Perceived Relationship Bonding; PPI = Perceived Privacy Invasion; PNC = Perceived Network Closeness; SHY = Shyness; SOC = Sociability. Given that network mutuality was only used for manipulation checks, its measurement items were excluded.

Table 3.5 Descriptive Statistics

	Min	Max	Mean	S.D.
PRB	1.40	7.00	4.27	1.32
PPI	2.50	6.75	5.18	1.01
NM	1.50	6.50	4.06	1.61
AGE	18	25	21.35	0.68
IN-EXP	6.00	8.5	7.30	0.52
FB-EXP	1.5	6.0	3.7	1.04
PNC	4.00	7.00	5.35	0.72
SHY	1.67	5.00	3.23	1.57
SOC	4.33	7.00	4.87	1.38

Notes:
NM = Network Mutuality (manipulation check)
IN-EXP = Internet Experience
FB-EXP = Facebook Experience

Table 3.6: Categorization of Subjects' Behavioral Responses

Passive Response	Active Response		
Inaction	Transactional Avoidance	Interpersonal Avoidance	Approach
(1) No response	(2) Mark the note as spam (3) Report the note to Facebook	(4) Remove the disseminator as a Facebook friend (5) Report the disseminator to Facebook	(6) Write a public comment (7) Send a private message

Notes:
(1) to (7) are coded in binary scores (0 or 1)
Transactional Avoidance = (2) + (3)
Interpersonal Avoidance = (4) + (5)
Approach = (6) + (7)

Whereas subjects' passive response (i.e., inaction) was manifested by their choice not to respond to the note publication, their active responses were classified into three behavior types (i.e., transactional avoidance, interpersonal avoidance, and approach). Transactional avoidance consists of two communication cessation functions, namely marking the note as spam and reporting the note to Facebook. Removing the disseminator as a Facebook friend and reporting the disseminator to Facebook are captured to reflect the behavior type interpersonal avoidance. Approach comprises two participatory functions, namely writing a public comment and sending a private message

(Table 3.5). For each response performed, subjects received a score of 1. Overall, a subject could receive a score of 0 and 1 for passive response, a score of 0, 1, or 2 for each of the three active responses.

3.5.3 Results on Perceived Relationship Bonding

MANOVA was conducted with perceived relationship bonding and perceived privacy invasion being dependent variables.[10] Results show an overall significant difference between the four experimental groups ($F(2, 104) = 64.44$, $p < 0.01$).[11] Given the significance of the overall test, ANOVAs were conducted on the two dependent variables separately.

ANOVA with perceived relationship bonding as dependent variable yields the significant effects of information dissemination ($F(1, 105) = 8.69$, $p < 0.01$) and network mutuality ($F(1, 105) = 153.43$, $p < 0.01$) (see Table 3.6). The significant interaction effect ($F(1, 105) = 68.99$, $p < 0.01$) suggests that the effect of information dissemination on perceived relationship bonding is moderated by network mutuality. Simple main effect analysis reveals that (1) posting with tagging is associated with significantly lower perceived relationship bonding than posting only under the low network mutuality condition ($F(1, 53) = 52.52$, $p < 0.01$), and (2) posting with tagging is associated with significantly higher perceived relationship bonding than posting only under the high network mutuality condition ($F(1, 52) = 18.26$, $p < 0.01$) (see Table 3.6 and 3.7; Figure 3.3). Therefore, H1a and H1b are supported.

[10] The significant Box's test suggests that the equality of variance-covariance matrices assumption is satisfied.

[11] Perceived network closeness, shyness, and sociability were found to have insignificant effects on the two dependent variables and hence were excluded from further analysis.

Table 3.7: ANOVA and Analysis of Simple Mean Effects

Source	Type III Sum of Squares	Df	Mean Square	F	Sig.
Overall Sample					
ID	4.87	1	4.87	8.69	.004
MN	85.98	1	85.97	153.43	.000
ID * NM	38.66	1	38.66	68.99	.000
Error	58.84	105	.56		
Total	2172.44	109			
NM = Low					
ID	35.83	1	35.83	52.52	.000
Error	36.16	53	.68		
Total	71.99	54			
NM = High					
ID	7.97	1	7.97	18.26	.000
Error	22.68	52	.44		
Total	30.65	53			

Notes:
Dependent Variable: Perceived Relationship Bonding
ID = Information Dissemination; NM = Network Mutuality.
a. R Squared = .69 (Adjusted R Squared = .68)

Table 3.8: Mean Values of Perceived Relationship Bonding

	Low Network Mutuality	High Network Mutuality	Mean
Posting Only	4.21	4.79	4.51
Posting with Tagging	2.59	5.56	4.02
Mean	3.39	5.16	

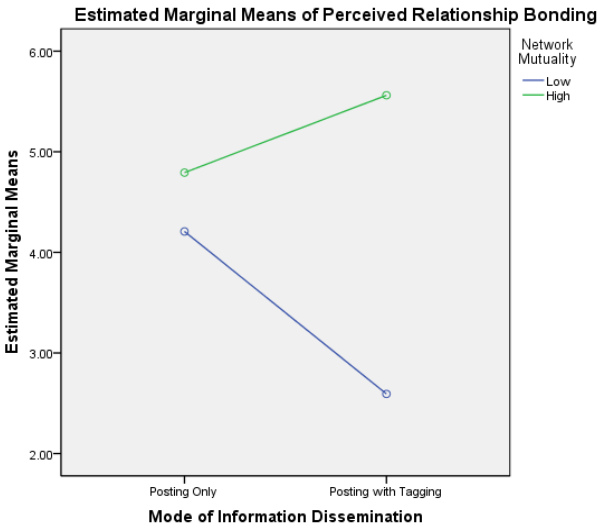


Figure 3.3. Study II Mean Plot of Perceived Relationship Bonding

3.5.4 Results on Perceived Privacy Invasion

ANOVA with perceived privacy invasion as dependent variable reveals the significant effects of information dissemination (F (1, 105) = 100.61, p <0.01) and network mutuality (F (1, 105) = 22.24, p <0.01) (see Table 3.8). The significant interaction effect (F (1, 105) = 75.47, p <0.01) suggests that the effect of information dissemination on perceived privacy invasion is moderated by network mutuality. Simple main effect analysis reveals that (1) posting with tagging is associated with significantly higher perceived privacy invasion than posting only under the low network mutuality condition (F (1, 53) = 151.69, p <0.01), and (2) posting only and posting with tagging are not different from each other in affecting perceived privacy invasion under the high network mutuality condition (F (1, 52) = 1.08, p =0.31) (see Table 3.8 and 3.9; Figure 3.4). Therefore, H2 is supported.

Table 3.9: ANOVA Results

Source	Type III Sum of Squares	Df	Mean Square	F	Sig.
Overall Sample					
ID	36.60	1	36.60	100.61	.000
NM	8.09	1	8.09	22.24	.000
ID * NM	27.45	1	27.45	75.47	.000
Error	38.19	105	.36		
Total	2866.90	109			
NM = Low					
ID	64.35	1	64.35	151.69	.000
Error	22.48	53	.42		
Total	86.83	54			
NM = High					
ID	.33	1	.33	1.08	.305
Error	15.71	52	.30		
Total	16.04	53			

Notes:
Dependent Variable: Perceived Privacy Invasion
ID = Information Dissemination; NM = Network Mutuality.
a. R Squared = .65 (Adjusted R Squared = .64)

Table 3.10: Mean Values of Perceived Privacy Invasion

	Low Network Mutuality	High Network Mutuality	Mean
Posting Only	3.66	5.23	4.45
Posting with Tagging	5.81	5.39	5.61
Mean	4.74	5.31	

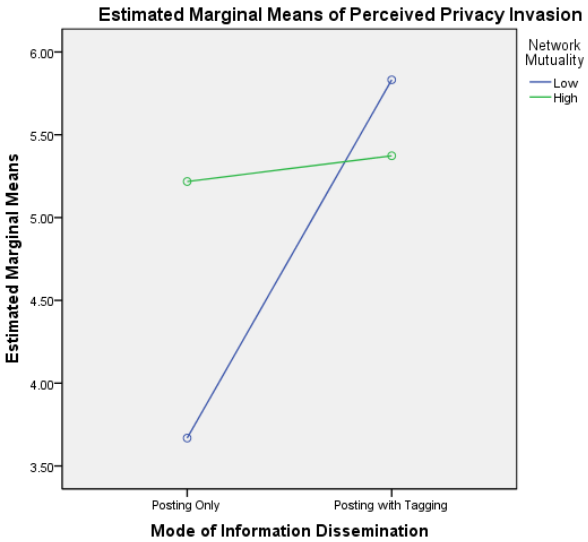


Figure 3.4. Study II Mean Plot of Perceived Privacy Invasion

3.5.5 Results on Behavioral Responses

Overall, 43 subjects assumed the passive behavioral response (with 66 subjects performing at least one active response). As the passive response variable (i.e., inaction) was binary (with subjects' score being 0 or 1), we conducted binary logistic regression to test the effects of perceived relationship bonding and perceived privacy invasion on inaction. To facilitate interpretation of the results, we standardized perceived relationship bonding and perceived privacy invasion scores before fitting the logistic regression models with *inaction* as outcome in model A (Table 3.10). As shown in Table 3.10, the results of the model fit test show satisfactory fit for the data (χ^2 (2) = 34.38, p <0.01, Cox & Snell's R^2 = 0.29). Perceived relationship bonding is found to have a significant negative effect on inaction (β = -0.80, p <0.01).

The odds-ratio is 0.45, with a 95% confidence interval of 1.26 to 3.79. This suggests that a one standard deviation increase in perceived relationship bonding decreases the likelihood of assuming inaction by 55%.[12] Perceived privacy invasion has a significant negative effect on inaction (β = -1.42, p <0.01). The odds-ratio is 0.24, with a 95% confidence interval of 1.13 to 2.43. This suggests that a one standard deviation increase in perceived privacy invasion decreases the likelihood of assuming inaction by 76%. Therefore, H3 and H7 are supported.

Further analyses were conducted to examine the active responses performed by the 66 subjects. As the three active response variables (i.e., transactional avoidance, interpersonal avoidance, and approach) coded from the subjects' behavioral responses were ordinal, we conducted ordinal regression regressions, in accordance with the guidelines set out by Peng et al. (2002), to test the remaining hypotheses. To facilitate the interpretation of the results, we standardized perceived relationship bonding and perceived privacy invasion scores before fitting the ordinal regression models with each of the three behavior types as outcomes (Table 3.10). Following Long (2000), we conducted parallel lines tests for each of the outcome variables and concluded that the proportional odds assumption was met[13].

[12] An odds ratio greater than 1 implies an increased likelihood; conversely, an odds ratio less than 1 implies a decreased likelihood. Following DeMaris (1991) and Duckworth et al. (2007), odds ratio less than 1 is reported in terms of likelihood percentage, which is computed based on (1 - odds ratio). Confidence intervals that do not contain 1 or -1 suggest that the relationship between the independent variable and the dependent variable is significant (Peng and So 2002).

[13] Ordinal logistic regression only applies to data that meet the parallel regression assumption, which requires equality of coefficient for all outcome categories of the dependent variable (McCullagh 1980). In other words, ordinal logistic regression assumes that the coefficients that describe the relationship between the lowest category of transactional avoidance (i.e., when transactional avoidance = 0) and all higher categories (i.e., when transactional avoidance

In model B, we conducted an ordinal logistic regression on *transactional avoidance*. The results of the model fit test shows satisfactory fit for the data (χ^2 (2) = 34.21, p <0.01, Cox & Snell's R^2 = 0.43). As shown in Table 3.10, perceived relationship bonding is found to have a significant and negative effect on transactional avoidance (β = -0.52, p <0.05). The odds-ratio is 0.59, with a 95% confidence interval of -2.00 to -1.43. This suggests that a one standard deviation increase in perceived relationship bonding reduces the likelihood of engaging in transactional avoidance by 41%. Perceived privacy invasion has a significant positive effect on transactional avoidance (β = 2.64, p <0.01). The odds-ratio is 14.01, with a 95% confidence interval of 1.35 to 3.93. This suggests that a one standard deviation increase in perceived privacy invasion increases the likelihood of engaging in transactional avoidance by 14.01 times. In essence, the results suggest that both perceived relationship bonding and perceived privacy invasion have significant influence on transactional avoidance, with the latter being a stronger predictor. Therefore, H4 and H8 are supported.

In model C, an ordinal logistic regression was conducted on *interpersonal avoidance*. The results of the model fit test show that the model fit the data well (χ^2 (2) = 30.24, p <0.01, Cox & Snell's R^2 = 0.51). Perceived relationship bonding is found to have a significant negative effect on interpersonal avoidance (β = -1.46, p <0.05). The odds-ratio is 0.23, with a 95% confidence interval of -4.53 to -1.18. This suggests that a one standard

---

= 1 or 2) are the same as those that describe the relationship between the middle category of transactional avoidance (i.e., when transactional avoidance = 1) and highest category (i.e., when transactional avoidance = 2). Our test revealed that the difference in the coefficients was not significant and thus the proportional odds assumption was met.

deviation increase in perceived relationship bonding reduces the likelihood of engaging in interpersonal avoidance by 77%. However, contrary to expectation, perceived privacy invasion is found to have no significant influence on interpersonal avoidance (β = -0.59, p = 0.55). Hence, H5 is supported but H9 is not.

In model D, an ordinal logistic regression was conducted on *approach*. The results of the model fit test show that the model fit the data well (χ^2 (2) = 58.65, p <0.01, Cox & Snell's R^2 = 0.62). Perceived relationship bonding is found to have a significant and positive effect on approach behavior (β = 4.15, p <0.01). The odds-ratio is 63.43, with a 95% confidence interval of 2.11 to 6.18. This suggests that a one standard deviation increase in perceived relationship bonding increases the likelihood of engaging in approach behavior by 63.43 times. Perceived privacy invasion has a significant and negative effect on approach (β = -1.76, p <0.05). The odds-ratio is 0.17, with a 95% confidence interval of -3.16 to -1.35. This suggests that a one standard deviation increase in perceived privacy invasion reduces the likelihood of engaging in approach behavior by 83%. In sum, the results suggest that both perceived relationship bonding and perceived privacy invasion have significant influence on approach behavior, with the former likely being a stronger predictor. Therefore, H6 and H10 are supported.

Table 3.11: Logistic Regression

	Dependent Variable					
	Model A	Model B		Model C		Model D
Parallel Lines Test						
Chi-Square		0.68		2.00		4.26
Degrees of Freedom		2		2		2
Significance		p =0.71 (N.S.)		p =0.37 (N.S.)		p =0.12 (N.S.)
Model Fit						
Likelihood Ratio Chi-Square	34.38	34.21		30.24		58.65
Degrees of Freedom	2	2		2		2
Significance	p <0.01	p <0.01		p <0.01		p <0.01
Cox & Snell	0.29	0.43		0.51		0.62
Threshold†		TA = 0	TA =1	IA = 0	IA = 1	AP = 0	AP = 1
Estimate		1.11	3.38	2.23	3.94	3.12	6.38
Standard Error		0.49	0.68	0.39	0.59	1.01	1.48
Wald Chi-Square		5.13	24.68	33.46	44.38	9.63	18.66
Significance		p <0.05	p <0.01	p <0.01	p <0.01	p <0.01	p <0.01
95% CI							
Lower Bound		1.49	2.05	1.47	2.78	1.15	3.48
Upper Bound		2.06	4.71	2.98	5.10	5.09	9.27
Predictors							
Perceived Relationship Bonding							
Estimate	-0.80	-0.52		-1.46		4.15	
Standard Error	0.29	0.24		0.63		1.04	
Wald Chi-Square	7.89	4.57		4.70		15.95	
Significance	p <0.01	p <0.05		p <0.05		p <0.01	
Odds-Ratio	0.45	0.59		0.23		63.43	
95% CI	(1.26, 3.79)	(-2.00, -1.43)		(-4.53, -1.18)		(2.11, 6.18)	
Perceived Privacy Invasion							
Estimate	-1.42	2.64		-0.59		-1.76	
Standard Error	0.30	0.66		0.67		0.72	
Wald Chi-Square	23.12	16.07		0.86		6.02	
Significance	p <0.01	p <0.01		p =0.38 (N.S.)		p <0.05	
Odds-Ratio	0.24	14.01		0.55		0.17	
95% CI	(1.13, 2.43)	(1.35, 3.93)		(-1.96, 0.98)		(-3.16, -1.35)	

Notes:
Model A: DV = Inaction
Model B: DV = Transactional Avoidance (TA)
Model C: DV = Interpersonal Avoidance (IA)
Model D: DV = Approach (AP)
† The threshold estimates indicate the cumulative logits when perceived privacy invasion and perceived relationship bonding equal zero (see Appendix F for discussion).

A mediation analysis was conducted following Baron and Kenny (1986)'s method. Results in Table 3.11 shown that the two mediating

variables, perceived relationship bonding and perceived privacy invasion, fully mediated the impact of information dissemination and network mutuality on inaction, transactional avoidance, interpersonal avoidance, and approach.

Table 3.12: Test for Mediating Effects

	Model 1				Model 2				Model 3			
	Inaction	TA	IA	AP	Inaction	TA	IA	AP	Inaction	TA	IA†	AP
ID	-1.22*	1.74**	2.59**	-2.01**	-0.18	0.34	0.38	-0.75	-0.29	0.03	-	-0.43
NM	-1.58*	3.08*	-3.05**	1.67*	-0.27	0.32	-0.21	0.65	-0.28	0.57	-	0.23

Notes:
Model 1: Unmediated model
Model 2: Model with perceived relationship bonding
Model 3: Model with perceived privacy invasion
† Since perceived privacy invasion has no significant influence on interpersonal avoidance, no mediation test was conducted.

3.6 DISCUSSION AND CONCLUDING REMARKS

3.6.1 Discussion of Results

The results supported all but one of our hypotheses. This study seeks to understand the consequences of an embarrassing exposure in online social networks. We postulate that network mutuality moderates the effect of information dissemination on perceived relationship bonding. As hypothesized, compared to posting only, posting with tagging leads to lower level of perceived relationship bonding when network mutuality is low. When network mutuality is high, posting with tagging results in higher level of perceived relationship bonding. Furthermore, we also predict that network mutuality moderates the effect of information dissemination on perceived privacy invasion. In line with our expectation, compared to posting only, posting with tagging leads to a significant increase in perceived privacy invasion when network mutuality is low. When network mutuality is high,

posting with tagging is not significantly different from posting only in terms of perceived privacy invasion.

We also establish that, in response to perceived relationship bonding and perceived privacy invasion, individuals either take on passive response such as inaction or engage in active responses in the form of transactional avoidance, interpersonal avoidance, and approach. Our results show that, as expected, perceived relationship bonding and perceived privacy invasion significantly reduce (increase) passive response (active response). Specifically, perceived relationship bonding has a significant negative influence on avoidance behavior (transactional and interpersonal) and a significant positive influence on approach behavior. Furthermore, our results show that perceived privacy invasion has a significant positive influence on transactional avoidance and a significant negative influence on approach behavior. However, contrary to our expectation, perceived privacy invasion has no significant influence on interpersonal avoidance. The results imply that although perception of privacy invasion is likely to induce withdrawal from an embarrassing exposure, it is not strong enough to elicit relationship dissolution. A plausible explanation is that the target's existing relationship with the disseminator dissuades him or her from engaging in relationship avoidance. As noted by Rusbult and Martz (1995), individuals' relational investment played an important role in their decision to maintain the relationship with abusive others. Likewise, in the context of online social networks, the target may be unwilling to terminate a relationship despite an elevated perception of privacy invasion following the embarrassing exposure.

3.6.2 Theoretical Contributions

Social networking is an important online activity and, at times, a major motive for individuals to come online (Madden and Zickuhr 2011). Past studies suggest that online social networks do not only facilitate the bonding and bridging of social relationships but also expose individuals to privacy abuses (Ellison et al. 2007). Although IS research has progressed significantly in understanding privacy in online social networks, its focus has been on privacy issues associated with exposures of identity information. We thus extend the privacy literature by suggesting that embarrassing information is an important object of exposure in online social networking.

This study makes several contributions to research. First, it contributes to IS literature by examining factors relevant to online social networks that influence individuals' bonding experience and privacy perception in an embarrassing exposure. Based on the Social Exchange Theory, this study investigates two antecedents of perceived relationship bonding and perceived privacy invasion, namely, information dissemination and network mutuality. We rationalize that *information dissemination* (i.e., posting only vs. posting with tagging) exemplifies *exchange behavior* in initiating social exchange. Reflecting the way a bonding experience can be shaped by target participation, information dissemination illustrates how exclusion and inclusion of target notification determine perceived relationship bonding. With respect to the role of individuation in privacy invasion, information dissemination illustrates how traceability of the target's profile in the embarrassing exposure determines perceived privacy invasion. Furthermore, we contend that *network*

mutuality depicts the *social relationship structure* in which the social exchange occurs. On one hand, network mutuality determines the audience type, which influences the impact of target notification on perceived relationship bonding. On the other hand, network mutuality determines the exposure size, which influences the effect of target individuation on perceived privacy invasion. Taken as a whole, the two antecedents of perceived relationship bonding and perceived privacy invasion (i.e., information dissemination and network mutuality) are particularly relevant to online social networks.

Second, this study advances privacy-related research by examining perceived relationship bonding, in addition to perceived privacy invasion, as an important component in individuals' assessment of an embarrassing exposure in online social networks. Our study reveals that, while the involuntary nature of the embarrassing exposure influences the perception of privacy invasion, the humor implied by the exposure may also induce relationship bonding. Given that the exposure of embarrassing information is typically considered negative in past research, the findings of this study shed light on a multi-faceted interpretation of the phenomenon.

Third, we enrich extant IS research on social interactions by providing a taxonomy of behavioral responses to embarrassing exposure in online social networks. Drawing on the dichotomy of passive and active behavior, we classify individuals' behavioral responses into four different types, namely inaction, transactional avoidance, interpersonal avoidance, and approach. Specifically, inaction represents the target's passive disregard of the

embarrassing exposure. Transactional avoidance exemplifies the target's active disengagement from the embarrassing information, which manifests avoidance strategy at the transactional level. Interpersonal avoidance colligates active relationship dissolution behavior, hence illustrating the avoidance strategy performed at the interpersonal level. Approach behavior subsumes the target's active involvement in social interactions, which characterizes typical behavior to complete a social exchange. The findings of this study indicate that the proposed taxonomy is helpful in analyzing a variety of behavior commonly performed in response to embarrassing exposures and thus serves as a useful tool for in-depth examination of individuals' response behavior in online social networks.

3.6.3 Practical Contributions

Our findings also have important implications for application designers and online service providers. By facilitating the traceability of the target's profile, posting with tagging has come under heavy criticism. Given the influence of network mutuality on target's interpretation of an embarrassing exposure, application designers may contemplate how they can use information on network mutuality to their advantage. For example, in cases where embarrassing content is disseminated, a target's perception of privacy invasion can be mitigated if posting with tagging is discouraged for a disseminator who has low network mutuality with the target. On the other hand, if the disseminator has high network mutuality with the target, the disseminator should be promptly notified regarding the option of tagging the target to induce the perception of relationship bonding.

Furthermore, this study has important implications for online service providers. The three types of active behavioral responses identified in this study alert service providers to various user actions that go beyond inaction. Our study reveals that users may file reports to the service provider to seek transactional avoidance. This finding can steer online service providers toward designing effective mechanisms to facilitate transactional avoidance. For example, when users complain against a piece of content, the online social network provider should consider suspending the content from dissemination. Furthermore, our study shows that users, despite their strong perception of privacy invasion, may refrain from interpersonal avoidance to avoid abrupt relationship termination. To this end, we advocate that service providers should allow individuals to gradually de-escalate their relationships. For example, to distance oneself from the disseminator, users should be permitted to engage in gradual relationship dissolution by progressively excluding the disseminator from his or her online social networking activities. Our study also shows that users may engage in active exchange with the disseminator through approach behavior. Therefore, it is important that service providers provide participatory features, such as threaded commenting and content rating, to stimulate rich interactions.

3.6.4 Limitations and Future Research

This study examines embarrassing exposures in a context where a note containing the target's embarrassing information is disseminated through posting only versus posting with tagging. We do not attempt to generalize the results to other forms of information dissemination in online social networks.

For example, the disseminator might expose the embarrassing information by writing it directly on the target's wall. In such a case, since the embarrassing information resides in the target's personal profile, the effects of posting with tagging (i.e., notification and profile traceability) on perceived relationship bonding and perceived privacy invasion may be different.

Our contributions may also be limited by using a mock-up online social networking website. While the general layout and technical features of the mock-up website resembled those of a real online social networking platform, the mock-up website may not reflect the actual online social networking environment entirely. However, in the actual environment, we could neither manipulate the experimental conditions (i.e., controlling the number of mutual friends the subjects and the friend share) nor capture subjects' actual behavioral responses (i.e., intercepting the private messages the subjects sent to his or her friends). Therefore, despite the limitation, the employment of this mock-up website is necessary. Future research will be necessary to verify the impact of embarrassing exposures on relationship bonding and privacy invasion in a more natural setting.

This study has examined the joint effects of information dissemination and network mutuality on the target's perceptions of relationship bonding and privacy invasion, but it is yet unknown whether these two factors influence an individual's intensity of online social networks usage. It is possible that a target who perceives high relationship bonding may be motivated to engage in extensive online social interactions, hence intensifying their participation in online social networking. Conversely, a target who experiences high privacy

invasion may resolve to general withdrawal from online social interactions, thus increasing his or her likelihood of resigning from online social networks. Therefore, it would be interesting for future research to examine individuals' social network usage behavior after an embarrassing exposure.

Furthermore, this study has focused on behavioral responses facilitated by online social networking websites. In a real setting, the target might engage in behavior beyond the online environment. For instance, in response to the embarrassing exposure, the target might actively avoid transaction by complaining to the disseminator in physical encounters. Likewise, interpersonal avoidance might not be limited to breaking up connectivity within online social networks but could also escalate to relationship termination in the offline environment. Approach behavior might manifest in the target's active involvement during face-to-face interactions. Hence, future research could investigate how an embarrassing exposure that occurs within online social networks influences individuals' behavior in the offline environment.

Finally, this study focuses on the effects of network mutuality on perceived relationship bonding and perceived privacy invasion. While network mutuality is a key aspect of social relationship structure on online social networks, other forms of social structure might play some roles in forming privacy-related perceptions in embarrassing online exposures. For instance, the size of the target's social network might elevate individuals' perception of privacy invasion in an involuntary exposure since a larger network size essentially implies that the embarrassing exposure has a larger group of

audience. Likewise, the extent of information dissemination could be further escalated through indirect connections in online social networks. In light of understanding the importance of social relationship structure in shaping privacy related perceptions, it might be worthwhile to examine how these alternative aspects of exchange structure would impact individuals' exchange evaluations and subsequent response behavior in involuntary embarrassing exposures.

CHAPTER 4 STUDY III: ONLINE CUSTOMER BEHAVIOR AFTER A PRIVACY BREACH: A THEORETICAL MODEL AND EMPIRICAL TEST

4.1 INTRODUCTION

In recent years, privacy breaches — the theft, loss, or other forms of compromise of personally identifiable information such as credit card and Social Security numbers — have soared in the United States. According to the Identity Theft Resource Center (2009), approximately 600 breaches are publicly reported annually in the United States. A more sobering piece of news is that the publicized breaches are thought to be less than 5% of the breaches that actually occur (Claburn 2008). Undoubtedly, this unfortunate trend endangers the information privacy of customers and, at the same time, threatens the profitability and reputations of businesses. Several high-profile privacy breaches clearly illustrate these threats to practitioners (e.g., Zetter 2009, Jewell 2007, FTC 2006). For example, the computer system at TJX, which includes retailers Marshalls and TJ Maxx, was hacked over a two-year period before the breach was detected in 2006 (Acohido and Swartz 2007). Nearly 100 million customer records (e.g., credit and debit card numbers) were compromised, and the stolen data were used for various fraudulent activities, including an $8 million gift card scheme (Hines 2007, Jewell 2007). Experts estimated that TJX's costs associated with legal settlements exceeded $200 million (Kerber 2007). Additionally, lost sales resulting from damages to the firm's reputation are believed to be about $200 per compromised record

(Ponemon 2009). On the whole, a privacy breach is highly likely to hurt the performance of a firm.

Privacy breaches are not just the outcome of carelessness. Although firms may implement various organizational and technical measures to prevent privacy breaches, customers' data may nevertheless leak through unforeseen holes (Culnan and Williams 2009). Thus, managers should be well prepared for such a disaster so that their business can return to normal as quickly as possible (Whitman and Mattord 2008). Identifying and addressing technical problems that may permit a privacy breach can be complex and may require a significant amount of time, money, and effort. Nevertheless, an equal challenge is to repair the damaged relationships with customers after a breach (Culnan and Williams 2009). Given that reputation is one of the most valuable assets in a networked economy, firms cannot afford to underestimate the potential magnitude of damage that a privacy breach poses to customer referrals in the form of word of mouth (Taylor et al. 2009). Moreover, firms should take appropriate steps to keep their customers from switching to competitors after a disaster, because in this digital economy, customer loyalty can be easily lost (Reichheld and Schefter 2000). To mitigate the potentially disastrous consequences of a data breach for customer relationships, firms have recourse to numerous recovery tactics. These include, but are not limited to, providing monetary compensation for the privacy damages, establishing channels of clarification to permit effective customer feedback, and apologizing for the service failure. Yet little is known about the effectiveness of these organizational measures in regulating word of mouth and likelihood

of switching, which are the metrics critical to gauging the quality of customer relationships.

Information systems (IS) research has progressed significantly in expanding our understanding of online customers' predispositions, beliefs, attitudes, and behavior in relation to information privacy (Dinev and Hart 2006, Son and Kim 2008). Earlier studies on these topics focused on identifying the nature of concern for information privacy in the context of direct marketing (Smith et al. 1996, Stewart and Segars 2002). Subsequently, Malhotra et al. (2004) developed a scale of information privacy concerns specific to the Internet context. IS researchers also have tried to identify the impact of privacy concerns on customer behaviors, such as willingness to release personal information, identity misrepresentation, relationship termination, word of mouth, and complaints (Dinev and Hart 2006, Awad and Krishnan 2006, Son and Kim 2008, Culnan and Williams 2009). Furthermore, several IS studies have explored the strategies adopted by firms in reducing privacy breaches (Gal-Or and Ghose 2005, Yue and Cakanyildirim 2007). Although IS research deals with numerous aspects of information privacy, to the best of our knowledge, no research has been done to understand how organizational remedies to a privacy breach can change online customer behavior such as word of mouth and likelihood of switching (Elson and LeClerc 2006, Son and Kim 2008, Culnan and Williams 2009).

The objective of this study is to enrich the IS literature by developing and testing a model that explains online customer behavior after a privacy breach; more specifically, our study focuses on an online firm's postincident

recovery endeavor in mitigating the impact of a privacy breach.[14] The overarching theory in this study is drawn from the service recovery literature, which posits that customers' specific beliefs with regard to organizational remedies determine overall psychological evaluations, which in turn regulate behavior (Hoffman and Kelley 2000, Maxham and Netemeyer 2002, Smith and Bolton 2002). Specifically, the justice framework is used as a theoretical basis in identifying consumers' beliefs associated with the key attributes of privacy breach remedies (Moorman 1991, Culnan 1995). This framework suggests that people evaluate privacy related issues in terms of three criteria, namely, distributive justice, procedural justice, and interactional justice (Culnan and Bies 2003, Malhotra et al. 2004). According to the literature, these justice factors have been constantly shown to be salient in the context of information privacy (Alge 2001, Zweig and Webster 2002, Ashworth and Free 2006, Son and Kim 2008, Poddar et al. 2009, Wirtz and Lwin 2009). Thus, we argue that these three types of justice perceptions can reasonably indicate the specific criteria that online customers employ in assessing organizational endeavor undertaken to remedy a breach incident.

Meanwhile, we borrowed the concept of psychological responses from prior literature to represent general thoughts and feelings relevant to the context of information privacy (Pavlou and Gefen 2005, Robinson and Morrison 2000). Specifically, the service recovery literature defines psychological responses as consumer's cognitive and emotional responses

[14] Please note that our model is specifically designed for a situation in which a customer has been notified of a privacy breach and is now reacting to an online firm's postincident actions in mitigating the impact of the breach on customer relationships. Thus, the term "online customer behavior after a privacy breach" in this study refers to customers' behavioral reactions to organizational remedies after an online privacy breach incident.

associated with a firm's service recovery endevaor, which are represented by, respectively, perceived breach and feelings of violation (Morrison and Robinson 1997, Robinson and Morrison 2000). Furthermore, much research shows that these psychological responses can be shaped by various types of justice perceptions jointly, instead of independently (Folger 1986, Luo 2007, Tang et al. 2008). Thus, we propose not only main effects of justice perceptions but also their interaction effects on perceived breach and feelings of violation. Our model posits that, consistent with the service recovery literature, online customers' psychological responses (i.e., general thoughts and feelings) regulate postincident outcomes that include word of mouth and likelihood of switching.

Our theoretical framework is intended to make several contributions to information privacy literature. First, we attempt to extend justice theories by including psychological responses as mediating variables between justice perceptions and postincident outcomes. Second, our conceptual model includes various interaction effects in addition to the simple linear relationships between justice perceptions and psychological responses. Third, we differentiate perceived breach, which represents a cognitive response, from feelings of violation, which indicate an emotional response. Finally, we are the first to offer a conceptual framework on the effectiveness of organizational responses to a privacy breach; in doing so, we carefully consider the specificity of the online privacy context under study (Cho et al. 2001, Zeithaml et al. 2002, Holloway and Beatty 2003, Forbes et al. 2005, Fan et al. 2010). Overall, our model is expected to contribute significantly to the body

of knowledge relating to online customer behavior after a privacy breach; moreover, the findings of this study will help managers develop effective organizational practices to retain desirable customer relationships after an incident.

4.2 LITERATURE REVIEW

4.2.1 Online Privacy Breach and Organizational Remedies

An online privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information (OPC 2008). Past studies have identified several common types of privacy breaches, including insider disclosure or theft (Rindfleisch 1997), selling personal data to third parties, or sharing information with third parties (Preston 2004). Given that a privacy breach endangers customers' privacy, online firms are typically expected to uphold their moral responsibilities in implementing sound technical, structural, and procedural improvements to minimize the possibility of privacy breaches (Culnan and Williams 2009). In order to reduce negative consequences, firms need to react proactively to a privacy breach so as to mitigate and recover from its consequences. As shown in Table 4.1, a number of organizational remedies can be considered, and such options should be carefully evaluated in terms of their effects on customer behavior.

Table 4.1: Key Prior Research on Service Recovery

Authors	Type of Service	Online or Offline	Organizational Remedies	Major Findings
Chuang and Cheng (2012)	Banking	Offline	Gift vouchers and apology	Both gift vouchers and apology enhanced customer satisfaction.
DeWitt et al. (2008)	Restaurants and hotels	Offline	Compensation adequacy, response time, and demonstration of concerns	The effects of organizational recovery on behavioral loyalty were mediated by cognitive trust and emotions.
Forbes et al. (2005)	Online retailing	Online	Discounts, refunds, and apology	Issues associated with website system were the most frequent type of online service failure. Tangible compensations (i.e., discounts and refunds) were most effective in enhancing customer satisfaction.
Goodwin and Ross (1992)	Various (i.e., auto repair, air travel, and restaurants)	Offline	Tangible compensation (i.e., refunds), voice (i.e., opportunity to express feelings), and apology	The effect of compensation on satisfaction was enhanced by voice and apology.
Grewal et al. (2008)	Air travel and restaurants	Offline	Monetary compensation (i.e., cash vouchers and discounts)	Compensation increased repurchase intentions.
Holloway and Beatty (2003)	Online retailing	Online	Service recovery efforts experienced (i.e., refund credits, recovery delays, and apology)	Most dissatisfied online customers indicated that they deserved more (i.e., refunds) for the problems. They were critical of the service recovery (i.e., delays and lack of an apology).
Liao (2007)	Various (i.e., online retailing, restaurants, and hotels)	Both online and offline	Service recovery performance (i.e., problem solving, prompt handling, providing an explanation, making an apology, and being courteous)	The impact of service recovery performance on repurchase intent was fully mediated by satisfaction.
Maxham (2001)	Hairdressing	Offline	Recovery strategies (i.e., refunds, future discounts, and apology)	Recovery strategies enhanced satisfaction, purchase intent, and word of mouth.
Parasuraman et al. (2005)	Online retailing	Online	E-recovery service quality (i.e., compensation, responsiveness, and contact)	E-recovery service quality had consistently strong and positive correlations with perceived overall value and loyalty intentions.
Smith and Bolton (2002)	Restaurants and hotels	Offline	Recovery efforts (i.e., compensation, speed, and apology)	The three types of recovery efforts significantly influenced customers' overall satisfaction after service recovery.
Smith et al. (1999)	Restaurants and hotels	Offline	Recovery attributes (i.e., discounts, response speed, and apology)	The three attributes of service recovery significantly enhanced overall satisfaction.
Wirtz and Mattila (2004)	Restaurants	Offline	Service recovery attributes (i.e., discounts, response immediacy, and apology)	Service recovery attributes enhanced customer satisfaction after a service failure.

Although online privacy breaches share some features with privacy breaches in traditional retailing, they also exhibit significant differences. For example, the ease of copying personal information implies that the damages of an online privacy breach may unfold over a long window because personal information can be easily reproduced, disseminated, and reused in the online environment (Zeithaml et al. 2002, Malhotra et al. 2004). Furthermore, online transactions are often completed through self-service mechanisms, which tend to eliminate human interaction and limit relationship development; thus, the interaction between an online firm and its customers is likely to be thin and superficial in the context of service recovery (Meuter et al. 2000). Overall, given the unique characteristics of an online privacy breach, it is necessary to consider the specificity of the online privacy context in examining the effectiveness of organizational remedies after a breach.

4.2.2 The Service Recovery Perspective

The service recovery literature offers a theoretical perspective for understanding customer behavior in response to organizational recovery efforts after an online privacy breach. Specifically, the literature posits that customers' specific beliefs with regard to organizational remedies determine their overall psychological evaluations of these measures (Hoffman and Kelley 2000, Maxham and Netemeyer 2002, Smith and Bolton 2002). Central to this argument is the idea that customers' judgment of a firm arises from their specific assessment of the key attributes of the firm's service recovery effort (Bitner et al. 1990, Tax et al. 1998). A growing volume of empirical evidence supports this perspective. For instance, in a study on service

recovery encounters, Schoefer and Ennew (2005) paid special attention to customers' beliefs associated with monetary compensation, waiting time, and service agent interactions. Their results suggested that customers' overall appraisal of the travel company was the consequence of their specific beliefs. Likewise, Maxham and Netemeyer (2002) found evidence of the importance of customers' perceptions of fairness as determinants of their judgment of the company as a whole.

Furthermore, according to the service recovery literature, customer behaviors are the salient consequences of their overall psychological evaluations of a firm's endeavor in remedying a service failure (Maxham and Netemeyer 2002). The main thrust of past research in examining organizational remedies has been to focus on how customers adjust their behavior in accordance with their overall judgments of firms after service recovery (e.g., Liao 2007, Maxham and Netemeyer 2002). In a study examining service recovery in restaurants and hotels, DeWitt et al. (2007) showed that customers' continued patronage depended on their post-recovery appraisal of the firm. Likewise, Kau and Loh (2006) revealed that mobile users' overall satisfaction after service recovery was an important driver of recommendation behavior.

In essence, the service recovery literature highlights the importance of customers' overall psychological evaluations in influencing their behavior after an online privacy breach incident; moreover, their overall psychological evaluations are the summary of customers' specific beliefs with regard to organizational remedies in response to the online privacy breach.

4.2.3 Justice Framework

A theoretical model for online privacy breach recovery needs to take into account factors that circumscribe the remedies undertaken by online firms. These factors are rooted in specific compensation, redress procedures, and explanations. The service recovery literature suggests that the justice framework may serve as a useful starting point for looking at customers' specific beliefs with regard to privacy breach remedies (Hoffman and Kelley 2000, Maxham and Netemeyer 2002, Smith and Bolton 2002). Justice (also often referred to as fairness) is indicative of how fairly an individual is treated by another individual or by an organization (Moorman 1991, Culnan 1995). It is viewed as a key principle in a variety of social exchange relationships such as organization-employee (Tekleab et al. 2005, Howard 1999, Lee et al. 1999), faculty-student (Schmidt et al. 2003), editor-author (Gilliland and Beckstein 1996), and firm-customer (Tax et al. 1998). Unsurprisingly, a growing number of researchers have been studying the concept of justice to explain individuals' behavior in the context of information privacy (Alge 2001, Zweig and Webster 2002, Ashworth and Free 2006, Son and Kim 2008, Poddar et al. 2009, Wirtz and Lwin 2009). A consistent finding of these justice-based privacy studies is that individuals' perceptions about the fairness of a particular privacy situation affect how these individuals actually react to the situation under investigation. In general, we believe that this justice perspective provides a valuable framework for examination of how people react to the recovery tactics online firms undertake after a privacy breach.

The justice framework identifies three types of justice, namely distributive, procedural, and interactional, all of which are particularly relevant in privacy breach recovery (Holloway et al. 2005). First, distributive justice refers to the perceived fairness of compensation that a customer receives from a vendor (Homans 1961, Martínez-Tur et al. 2006). Distributive justice is based on the notion of equity, which is the result of a mental comparison of inputs and outputs (Gilliland 1993). This concept is also consistent with the privacy calculus or a cost-benefit analysis that is widely established in privacy research (Laufer and Wolfe 1977, Culnan and Bies 2003, Dinev and Hart 2006). Second, procedural justice refers to the perceived fairness of the procedure used in handling a customer's question or feedback regarding a vendor's reaction to a breach (Thibaut and Walker 1975). Procedural justice differs from distributive justice because procedural justice is concerned with the fairness of the process in handling customer complaints, whereas distributive justice focuses mainly on outcomes (Greenberg 1990, Culnan and Armstrong 1999). Finally, interactional justice refers to the perceived fairness of the interpersonal treatment with which the procedures are implemented (Bies and Moag 1986, Gilliland and Beckstein 1996). Interactional justice is a concept that once was considered part of procedural justice but now is its own distinct category (Cropanzano et al. 2002). In particular, procedural justice focuses on formal procedures, but interactional justice deals with such subtleties as respect, care, and politeness (Bies and Moag 1986).

Prior research has drawn on the justice framework to study recovery tactics after service failure. For instance, Goles et al. (2009) examined

delivery delay in commercial transactions. They found that when a seller was helpful in resolving the issue, patrons perceived less violation of their expectations and experienced fewer negative emotions compared to when the seller was not helpful. Likewise, in a study on e-service recovery, Collier and Bienstock (2006) verified the importance of justice in recovering from damaged shipments and found that by ensuring distributive justice, procedural justice, and interactional justice, customers were more satisfied and happier with their online purchase experience. In a study examining delivery failure recovery by online retailers, Lin et al. (2011) operationalized the three types of justice in terms of compensatory discounts, redelivery time, and politeness in e-mails. Their results suggested that when the three attributes of service recovery were ensured, customers were more pleased and delighted with the online retailer. Overall, past studies show that the justice framework forms a relevant theoretical basis for identifying the key attributes of organizational remedies after a service failure.

4.2.4 Psychological Contract

The service recovery literature theorizes that customers' specific beliefs with regard to organizational remedies determine their overall psychological evaluations of firms (Hoffman and Kelley 2000, Maxham and Netemeyer 2002, Smith and Bolton 2002). Whereas the justice perspective sheds light on the development of specific beliefs associated with the organizational remedies, the notion of psychological responses helps understand customers' overall psychological evaluations of remedy strategies after a privacy breach. Specifically, the psychological contract perspective

posits that social exchange partners establish a contract, which can be developed explicitly or implicitly, to delineate obligations between partners in the exchange (Morrison and Robinson 1997, Robinson and Morrison 2000). For instance, in a study examining IT outsourcing projects, Koh et al. (2004) found that a psychological contract could manifest in customers' perceptions of the obligation of suppliers to deliver high quality services, demonstrate high professionalism, and establish clear authority structures. Likewise, Kingshott and Pecotich (2007) noted that the psychological contracts that distributors constructed centered mainly on the suppliers' responsibility to ensure fair dealing and good faith in a business exchange.

Violation of a psychological contract occurs when an exchange partner fails to uphold its obligations. To illustrate, in online shopping, customers generally expect a retailer to ship a functional product and fulfill the delivery within a stated period (Parasuraman et al. 2005). More important, customers typically expect their personal information, which is often required to complete online purchases, to be safeguarded by the retailer and used exclusively for the transaction (Culnan and Armstrong 1999). Consequently, when an online firm fails to recover from a privacy breach, customers are likely to think the firm has violated the psychological contact because it is not only incompetent in safeguarding customer information but also is unable to remedy the issue (Wang and Huff 2007).

According to the psychological contract perspective, when a contract is not honored, individuals react psychologically with cognitive and emotional responses (Morrison and Robinson 1997, Robinson and Morrison 2000). A

cognitive response occurs as a result of a deliberate calculation of whether the firm's treatment meets or falls short of the psychological contract (Pavlou and Gefen 2005). The service recovery literature suggests that a cognitive response is predominately shaped by compensation adequacy and procedural fairness. Although adequate compensation ensures equity in offsetting damages associated with the privacy breach, fair procedures assure a formal process that leads to an equitable outcome (Culnan and Bies 2003). In contrast, an emotional response transcends a mere cognitive appraisal of an event and relates instead to feelings of distress associated with the firm's lack of faithfulness and oversight (Schoefer and Ennew 2005). Past research that examined service recovery suggests that an emotional response can be especially sensitive to reparation and interpersonal treatment. Inadequate reparation not only contributes to customers' perceptions of a breach of the psychological contract but also triggers feelings of contract violation (Grégoire and Fisher 2008). Poor interpersonal treatment is experienced when customers undergo bad social interactions, such as personal slights, demeaning offenses, or disrespectful actions, which are known to arouse a sense of violation (Barclay et al. 2005). In the literature, these cognitive and emotional dimensions are represented, respectively, by perceived breach and feelings of violation (Morrison and Robinson 1997, Robinson and Morrison 2000). We define perceived breach as an overall cognitive judgment concerning a particular privacy-related incident as well as the measures taken by a company in addressing the incident (Pavlou and Gefen 2005).[15] Feelings of violation

[15] The concept of perceived breach does not represent one's perception about the extent of a privacy breach itself. Rather it indicates a deliberate judgment of whether the firm has fulfilled its responsibilities to recover from a breach incident.

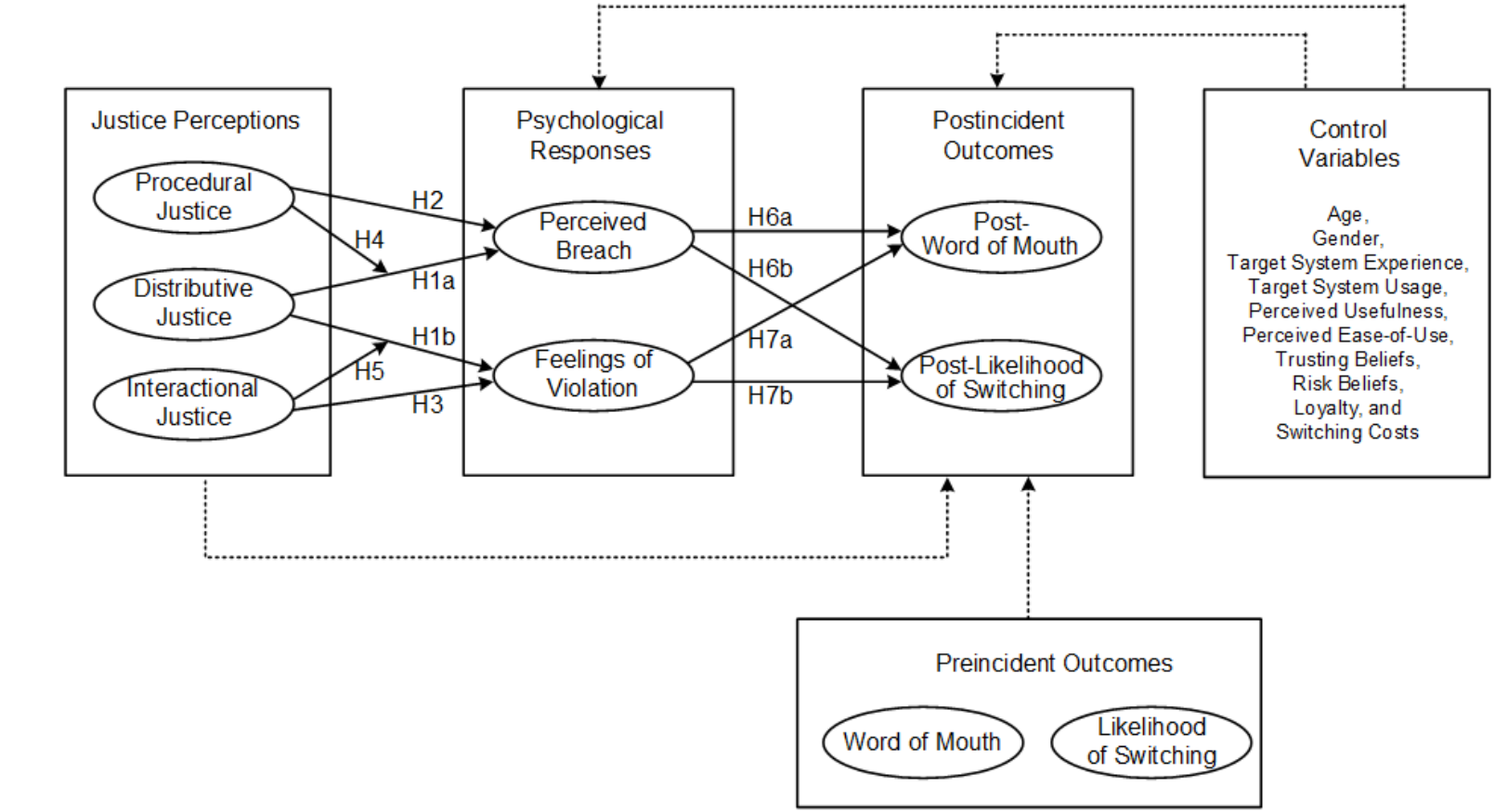
are defined as the emotional state of betrayal or distress that a customer feels toward a vendor after a privacy breach recovery (Morrison and Robinson 1997).

In sum, used as the overarching framework in this study, the service recovery literature postulates that customers' specific justice perceptions with regard to organizational remedies determine overall psychological evaluations, which are summarized into perceived breach and feelings of violation. Furthermore, the literature suggests that customers' overall psychological evaluations, in turn, regulate their behavior after service recovery.

4.3 RESEARCH MODEL AND HYPOTHESES

By drawing on the service recovery literature, we proposed our conceptual model, which is presented in Figure 4.1. In general, the model shows that customers' justice perceptions as specific beliefs determine psychological responses as overall evaluations, which in turn, influence postincident outcomes. We first developed research hypotheses concerning the relationships between justice perceptions and psychological responses (H1-H3). Subsequently, we offer theoretical explanations of the impact of the interaction between justice perceptions on psychological responses (H4-H5). Finally, we hypothesize the effects that psychological responses have on postincident outcomes (H6-H7).

Figure 4.1. Study III Research Model



Note: ⟶ Hypothesized Effects; ⇢ Controlled Effects.

4.3.1Justice Perceptions and Psychological Reactions

Distributive justice is especially important in reducing perceived breach of psychological contract in online privacy breach recovery. In the online environment, to complete commercial transactions, customers are typically required to provide personal information to online firms with which they often lack a history of interpersonal relations (Culnan and Armstrong 1999). As a result, customers in general assume that the online firm will safeguard their information (Bart et al. 2005). A privacy breach essentially challenges customers' cost assessment by exposing them to unforeseen damages such as identity theft and credit card fraud (Zeithaml et al. 2002). Although many are dissatisfied by the unexpected privacy loss, customers are likely to react less negatively when the online firm, despite the lack of interpersonal relationships, ensures distributive justice in privacy breach recovery (Holloway et al. 2005). Distributive justice is often maintained through the provision of monetary compensation, such as refunds, rebates, and future discounts. In online privacy breach recovery, an adequate monetary compensation is particularly important because it categorically restores the balance of personal information exchange (Li et al. 2011). Indeed, recent IS studies offer empirical evidence that monetary compensation is particularly important in shaping customers' cognitive response to privacy issues in the online environment. For instance, Xie et al. (2006) found that monetary compensation helped address the disutility of personal information disclosure in online transactions. Likewise, in a study on location-based services, Xu et al. (2009) revealed that distributive justice addressed users' negative perceptions associated with the exposure of locality information to online

companies. In essence, by compensating for the costs inflicted by a privacy breach, distributive justice restores equity in online transactions and hence alleviates customers' negative perceptions towards the breach of psychological contract. Thus, we hypothesize that perceived breach will decrease (increase) as distributive justice increases (decreases).

H1 (a): Distributive justice will be related negatively to perceived breach.

The appraisal-tendency framework posits that negative emotions arise from individuals' appraisal of responsibility for negative events (Lerner and Kelter 2000). Especially, when others are responsible for the negative events, individuals experience negative emotions, such as anger, dejection, and agitation. Similarly, customers often experience strong negative emotions in online privacy breaches. This is because when customers provide personal information in online transactions, they generally expect the online firms to be responsible in properly managing their information (Wang and Huff 2007). As a result, in recovery from an online privacy breach, customers' appraisal of a firm's responsibility for the privacy loss arouses negative emotions.

Distributive justice is especially important in addressing customers' feelings of violation in online privacy breach recovery. Given the lack of personal relationships in online commercial transactions, customers may be highly anxious about the firm's commitment to safeguarding their privacy. By ensuring distributive justice, customers could ascertain the online firm's faithfulness in upholding its responsibility in the recovery and hence reduce their feelings of displeasure or hostility (Clayton 1992; Markovsky 1988).

Furthermore, distributive justice helps ensure adequate reparation, which is a key remedy for customers' emotional feelings triggered by online privacy breaches. Evidence suggests that distributive justice is of particular importance to customers' emotional responses about online privacy issues. For instance, Hann et al. (2007) found that monetary compensations reduced customers' feelings of insecurity and vulnerability that stemmed from online privacy failures. Thus, we hypothesize that feelings of violation will decrease (increase) as distributive justice increases (decreases).

H1 (b): Distributive justice will be related negatively to feelings of violation.

Although compensation may not satisfy all victims of a privacy breach, these victims often want to ensure that procedural justice is maintained in service recovery, i.e., that the process in which they are compensated is consistent, fair, and reasonable (Rahim et al. 2000; Brockners et al. 1994). According to the psychological contract perspective, customers' cognitive response (i.e., perceived breach) is predominately determined by the outcome and the procedure that leads to the outcome (Morrison and Robinson 1997). In particular, the procedural justice literature argues that when customers perceive a high degree of fairness in the outcome allocation procedure, they believe outcome equity is ensued (Brockner and Wiesenfeld 1996). Because a fair procedure helps assure equity restoration, procedural justice is likely to have a prominent impact on cognitive response (Folger and Konovsky 1989). Indeed, past research suggests that procedural justice in online service recovery is especially important in evoking a cognitive response because

service representatives and customers usually do not physically meet each other (Holloway and Beatty 2003). Since customers are separated from the actual recovery process in the online environment, they often have limited access to the procedures this process entails. Consequently, customers may be forced to rely entirely on the firm's website to learn about the recovery policies. Difficulty in obtaining information through the firm's website leads customers to question the justice of service recovery procedures and intensifies their dissatisfaction with the firm (Cho et al. 2001).

Research has shown that procedural justice ranks among the most essential practices that online companies can use to placate customers whose privacy is at risk (e.g., Collier and Bienstock 2006). In online privacy breach recovery, procedural justice manifests in terms of organizational mechanisms through which customers can be informed about the recovery process, such as how the privacy breach was identified, what information was leaked, and what safeguards are in place to resolve the privacy failure (Stevens 2010). A high degree of procedural justice helps overcome the lack of physical interaction by increasing the transparency of privacy breach recovery procedures and assuring customers about the firm's fair practices in addressing privacy issues (Culnan and Bies 2003). As a result, when customers perceive a high degree of procedural justice in privacy breach recovery, they conclude that the online firm is taking steps to ensure equity in the recovery. Thus, in online privacy recovery, it is reasonable to expect that fair procedures (e.g., thorough descriptions of the decision-making processes) reduce customers' perceived breach of a psychological contract. Therefore,

H2: Procedural justice will be related negatively to perceived breach.

The psychological contract perspective posits that the personal interaction process individuals experience plays a prevailing role in shaping emotional responses (Morrison and Robinson 1997). According to this perspective, feelings of violation are particularly sensitive to negative social experience and hence do not require deliberate reflection (Rousseau 1989). Similarly, in the service recovery context, ample evidence suggests that interactional justice plays a key role in shaping customers' emotional reactions associated with service recovery. For example, Chebat and Slusarczyk (2005) surveyed bank customers on their service recovery experience and found that their negative emotions could be reduced when they received respectful and pleasant treatment from bank staffs. In addition, Moorman (1991) demonstrated, after controlling for distributive and procedural justice, that interactional justice has a positive impact on job satisfaction. Customers who feel they are not treated with respect are likely to regard a situation as unacceptable and also to have negative feelings toward the vendor.

The effects of interactional justice on emotions are particularly evident in recovery endeavor from an online privacy breach (Gu 2010). This is because an online privacy breach not only entails explicit damage, such as financial loss and wasted time, but also engenders immense negative emotions, such as anger, hurt, and frustration (Lewicki and Bunker 1996). Furthermore, given the lack of established interpersonal relationships, customers are especially likely to feel disregarded by the online firm and develop aversive feelings (Bart et al. 2005). Lack of apologies not only

worsens customers' distress, but also makes them doubt the online firm's sincerity in accepting responsibility (Holloway and Beatty 2003). In essence, when an online business does not handle privacy breach recovery with interactional justice, customers are likely to experience negative emotions. Therefore, we propose that interactional justice is negatively related to feelings of violation.

H3: Interactional justice will be related negatively to feelings of violation.

4.3.2 Interactions between Justice Perceptions

Referent cognitions theory (RCT) offers an explanation for the joint effect of distributive justice and procedural justice on subsequent cognitive reactions (Folger 1986). Specifically, this theory states that individuals tend to evaluate outcomes (i.e., distributive justice) based on whether fair procedures are followed (i.e., procedural justice). When people have a high opinion of the fairness of the procedures followed, they would be less sensitive to outcome equity in service recovery. However, if they perceive the procedures as unfair, they are more likely to focus on attaining an equitable outcome (Brockner et al. 1994). Thus, according to RCT, the question of whether fair procedures were faithfully followed moderates the way people cognitively evaluate outcome equity. In particular, RCT predicts that when procedural justice is ranked higher, the effect of distributive justice on cognitive response becomes weaker; in contrast, when procedural justice is ranked lower, its effect becomes stronger.

RCT is considered an informative perspective in explaining individual behavior in recovery from an online privacy breach. Whereas relationships in traditional business settings are predominately built through personal interaction, they are typically maintained online with little person-to-person contact. Indeed, customers often interact with an online firm through self-service technology. Thus, in the absence of direct contact, procedural justice is considered the actual reflection of the online firm's compliance with principles of fair information practice (FIP) (Culnan and Bies 2003). When procedural justice is high, customers can be assured that the online firm has followed the industry guidelines and privacy laws in providing equitable compensation, thereby reducing their sensitivity toward distributive justice (Tang et al. 2008). However, when procedural justice is amiss, equitable compensation for the firm's negligence cannot be guaranteed; hence, customers' sensitivity toward distributive justice is likely heightened. Taken together, in the domain of online privacy breach recovery, customers who are satisfied with organizational procedures tend to perceive the monetary reward as acceptable; therefore, procedural justice could complement distributive justice in affecting perceived breach. Thus,

H4: The relationship between distributive justice and perceived breach will decrease (increase) as procedural justice increases (decreases).

The cognitive appraisal model of emotion holds that the effect of outcome appraisal on emotions is moderated by the judgment of the outcome allocation experience (Montada 1994). According to the model, an individual's emotional response begins with an appraisal of an outcome as

either harmful or beneficial (Weiss and Cropanzano 1996). Essentially, when the outcome is undesirable, negative emotions emanate. This outcome appraisal is coupled with an experience appraisal, which involves an evaluation of the way individuals are treated in the course of receiving the outcome (Weiss et al. 1999). In service recovery, customers typically expect to be treated with respect and dignity; otherwise they would blame not only the service representative but also the firm for being irresponsible (Chebat and Slusarczyk 2005). Because the assignment of blame has a strong effect on negative emotions (Ortony et al. 1988), when customers experience poor interpersonal treatment, the effects of the outcome assessment on customers' emotional response will be emphasized. The earlier discussion leads us to expect that customers who are treated respectfully would more likely consider the monetary reward reasonable, and thereby, interactional justice could complement distributive justice in affecting feelings of violation.

In online privacy breach recovery, when interactional justice is high, customers would find the service representative sincere and helpful in addressing the privacy failure incident. As the service representative represents the online firm in privacy recovery, customers would be assured that the firm is accepting its responsibility, and hence their emotional response will be less aroused by distributive justice. By contrast, when interactional justice is low, customers would find the service representative disrespectful and lacking empathy. Consequently, they might become especially angry that the online firm is not accepting its responsibility. In such a case, they are

more likely to consider the firm irresponsible and thus increase the impact of distributive justice in arousing feelings of violation. Thus,

H5: The relationship between distributive justice and feelings of violation will decrease (increase) as interactional justice increases (decreases).

4.3.3 Determinants of Postincident Outcomes

Customer behavior takes on a myriad of forms such as repurchases, paying a premium, and interest in alternatives (Dick and Basu 1994, Bendapudi and Berry 1997, Kim and Son 2009). Nevertheless, two behavioral outcomes, namely, word of mouth and likelihood of switching, have been the focus of attention among researchers and practitioners (Zeithaml et al. 1996).

Word of mouth refers to the extent to which an individual intends to recommend, or say positive things about, a service to others (Srinivasan et al. 2002). Serving as a reference is risky because it involves the potential of tarnishing the social image or credibility of the person making the reference. Thus, a referral represents the ultimate form of a customer's dedication to a firm (Jones and Sasser 1995). In this regard, research shows that word of mouth — which represents a customer's willingness to recommend a firm's product or service to others — is a more powerful predictor of a firm's revenue growth than customer loyalty, customer satisfaction, or intent to repurchase (Reichheld 2003). Moreover, the significance of word of mouth is being amplified in the Internet age because opinions spread freely with few barriers of time, space, or socioeconomic status (Reichheld and Schefter 2000). A number of IS studies have been conducted to explain individuals' willingness to recommend within the context of online business (Gefen 2002,

Kim et al 2002, Mithas et al 2006, Kim and Son 2009). Furthermore, word of mouth has been the focus of much information privacy research designed to gauge the effect of privacy perceptions on customer behavior (Son and Kim 2008, Taylor et al. 2009). In particular, Culnan and Williams (2009) argued that service providers are essentially in "the reputation business," and thus it is important for them to cultivate "a culture of privacy" (p. 683). Therefore, it is important to examine the determinants of word of mouth for a better understanding of online customers' reactions to privacy breach recovery.

Likelihood of switching is defined as the extent to which a customer intends to leave his or her current vendor (Morgan and Hunt 1994). Acquiring a new customer is expensive because of such "one-time" activities as advertising, promotions, account setup, etc. (Reichheld and Sasser 1990). A firm loses the opportunity to maximize the return from the initial investment if the new customer defects without subsequent transactions. Thus, customer retention is said to be one of the most critical factors affecting the bottom line of a business (Reichheld and Schefter 2000). In fact, Reichheld and Sasser (1990) showed that a 5% decrease in defection rates leads to an increase in profits of 25% to 85%. Moreover, the one-time costs of acquiring an online customer are known to be considerably higher than the costs of acquiring a traditional customer (Reichheld and Schefter 2000). Accordingly, it is important for an online firm to understand the mechanism that keeps a customer from switching to an alternative vendor. An increasing number of IS researchers are trying to understand what facilitates or deters one's switching to an alternative online service (Chen and Hitt 2002, Kim and Son 2009, Ray

et al. 2011). Similarly, some studies of information privacy have paid attention to the causal link between privacy perceptions and switching behavior (Elson and LeClerc 2006, Son and Kim 2008). Thus, it is important to investigate how privacy breach recovery affects online customers' intention to switch to another vendor.

As shown in Figure 4.1, two types of postincident outcomes are examined in this study, namely, post-word of mouth and post-likelihood of switching.[16] Post-word of mouth refers to the level of word of mouth activity after a vendor fails to protect personal information. Similarly, post-likelihood of switching refers to the likelihood of switching after a vendor fails to protect personal information. Although preincident outcomes drive postincident outcomes, customer behavior may not stay the same as before after personal information is compromised. Specifically, our model posits that in the context of online privacy, customers' overall psychological evaluations of a firm's recovery practices, i.e., perceived breach and feelings of violation, affect behavioral outcomes, i.e., post-word of mouth and post-likelihood of switching. The service recovery literature suggests that in online service failures and recovery settings, customer behaviors are mainly a function of customers' overall psychological evaluations of recovery practices (Hoffman and Kelley 2000, Maxham and Netemeyer 2002). This is because in the online context, customers rarely have human contact with an online firm, and

[16] In IS literature, individuals' privacy-protective responses are classified into three categories: (1) information provision (e.g., refusal, misrepresentation), (2) private action (e.g., negative word of mouth, removal of personal information), and (3) public action (e.g., complaining) (Son and Kim 2008). The postincident outcomes examined in this study correspond to the second category, i.e., private action.

the lack of personal interaction makes it difficult for them to build a close relational bond. As a result, customers tend to base their behavioral decisions on their overall psychological evaluations, i.e., perceived breach and feelings of violation, instead of on other long-term relational considerations (e.g., trust and loyalty).

Subscribing to this rationale, we expect perceived breach to affect both post-word of mouth and post-likelihood of switching after a privacy breach recovery. Past research has clearly demonstrated the impact of perceived breach on customer behavior. For instance, in the context of online privacy, Poddar et al. (2009) found that because online exchanges lack physical contact, online customer behavior in the presence of a privacy threat is influenced more by what people think about the situation than by their prior relationship with the online vendor. This finding is consistent with Oliver's (1999) claim that when relational bonds are not strongly established, cognitive factors play a dominant role in regulating customer behavior (Forbes et al. 2005). Thus, we hypothesize that in a situation in which an online firm attempts to recover from a breach incident, perceived breach will affect customer behaviors such as post-word of mouth and post-likelihood of switching.

H6 (a): Perceived breach will be negatively related to post-word of mouth.

H6 (b): Perceived breach will be positively related to post-likelihood of switching.

The discussion mentioned previously indicates that emotional responses such as feelings of violation are more likely to be salient in online privacy settings than in other contexts as the determinants of customer behavior. Empirical evidence suggests the important role of feelings of violation on online customer behavior in the context of information privacy (Son and Kim 2008, Youn 2009). For example, Son and Kim (2008) showed that individuals' feelings toward information privacy drive information privacy-protective actions (e.g., refusal, negative word of mouth, complaints). Along the same line, Youn (2009) also found that affective components affect privacy protection behaviors (e.g., confrontation and avoidance). Taken together, it is reasonable to argue that emotional responses to privacy breach recovery affect whether online customer say positive things to others and whether they eventually switch to an alternative vendor.

H7 (a): Feelings of violation will be negatively related to post-word of mouth.

H7 (b): Feelings of violation will be positively related to post-likelihood of switching.

4.3.4 Controlled Effects

We included in the model a number of control variables that might affect online customer behavior. The literature on information privacy holds that older people worry more than younger people about their privacy (Culnan 1995, Malhotra et al. 2004). In addition, women have been shown to be more concerned than men about privacy (Milne and Rohm 2000). Thus, age and gender are included as control variables in the study. Meanwhile, to reflect

customer experience and usage of a website, we included experience and website usage. Experience refers to the time elapsed since a customer's first use of a website, whereas website usage reflects frequency. Several studies have shown that both of these variables influence customer behavior (Sun et al. 2006, Soderlund 2002, Humphrey et al. 2004). Besides individual characteristics, we incorporated in the model two types of beliefs, namely perceived usefulness and perceived ease of use. Perceived usefulness is defined by the utilitarian value that an individual receives from using an online vendor. Such benefits include thorough descriptions of products, variety of product offerings, price discounts, and personalized services (Mathwick et al. 2001). In contrast, perceived ease-of-use refers to the degree to which a customer finds that dealing with the online vendor is effortless (Davis et al. 1989). This encompasses the navigation of websites, the layout of Web pages, the convenience of finding information and ordering products, and similar activities. Much research shows that these types of beliefs, identified in the widely known technology acceptance model (TAM) (Davis et al. 1989), play an important role in determining online customer behavior (Koufaris 2002, Devaraj et al. 2002, Gefen et al. 2003).

Customers inevitably take a risk when they release their personal information to a vendor. In such a risky environment, trust in a vendor is known to play an important role in regulating customer behavior (Gefen et al. 2003, van der Heijden et al. 2003). In IS research, trusting beliefs and risk beliefs have often been chosen to represent the trust-risk notion. Trusting beliefs are defined as the degree to which a customer believes that a vendor

will behave in a trustworthy way. Specifically, trusting beliefs are assumed to reflect three dimensions, namely, benevolence, integrity, and competence (McKnight et al. 2002). Meanwhile, risk beliefs refer to the degree to which a customer foresees a high potential for loss associated with transactions with a vendor (Malhotra et al. 2004). In particular, risk beliefs in this study are thought to represent financial, performance, and psychological losses involved in transactions with an online store (Murray and Schlacter 1990). Trust and risk factors have been shown to exert significant effects on behavioral outcomes such as cooperation (Morgan and Hunt 1994), attitudes toward online purchasing (van der Heijden 2003), willingness to buy (Jarvenpaa and Tractinsky 1999), and intended use (Gefen et al. 2003).

In addition, loyalty and switching costs were chosen in this study as control variables because of their potential effect on online customer behavior. Whereas loyalty refers to a consumer's deeply held affective commitment toward a vendor (Beatty and Kahle 1988, Oliver 1999), switching costs refer to the time, money, and psychological and physical effort associated with the process of switching from one vendor to a new one (Burnham et al. 2003, Jones et al. 2002). Loyalty is shown to affect such variables as usage intention, word of mouth, and likelihood of switching (Taylor and Hunter 2002, Henning-Thurau et al. 2002, Kim and Son 2009). Research also shows that switching costs affect various outcomes such as the search for alternatives and willingness to pay a premium (Weiss and Heide 1993, Zauberman 2003, Kim and Son 2009). As shown in Figure 4.1, loyalty and switching costs as

well as other variables mentioned previously are controlled for to explain both psychological responses and postincident outcomes.

Meanwhile, much research suggests that prior decisions serve as the basis for the formation of subsequent decisions (Kim and Malhotra 2005, Kim 2009). Thus, postincident outcomes are likely to be determined, at least to some extent, by pre-word of mouth and pre-likelihood of switching that were made before the privacy-related incident. Consequently, the model includes pre-word of mouth and pre-likelihood of switching as control variables. In addition, we also controlled for the effects of justice perceptions on postincident outcomes to determine if there are spillover effects that go beyond the mediating effects of psychological responses.

4.4 RESEARCH METHODOLOGY

4.4.1 Research Setting

This research employed a scenario-based experiment that integrates the characteristics of field surveys and lab experiments (Malhotra 2004). In privacy research, a real-world environment is critical to data collection because one's sense of privacy is shaped, to a large extent, by the relational bond with the other party (Petronio 1991). Thus, we ensured that subjects had a realistic sense about doing business with an online vendor in order for them to respond meaningfully to our questionnaire. Meanwhile, although our study focuses on customers' reactions to privacy breaches, it is impractical to presume that all the subjects suffered a significant privacy problem with the vendor in question. Accordingly, we relied on the simulation of a privacy-related incident using a scenario-creation method that has been widely used in

privacy research (e.g., Nowak and Phelps 1992, Sheehan and Hoy 2000). In summary, we used a survey questionnaire to measure customers' perceptions about an actual store while manipulating their treatment through hypothetical scenarios.

In this study, subjects were given a Web-based survey questionnaire. In the questionnaire, the subjects were first asked to indicate the name of an online vendor they had used in the past year. In information privacy research, online vendors have often been used as partners with which individual customers interact for the social exchange of personal information (Malhotra et al. 2004, Dinev and Hart 2006, Son and Kim 2008). Following the tradition of this stream of research, we also chose online vendors as our study context. Consequently, if a subject had not used an online vendor in the past year, that person was excluded from further consideration. The questionnaire then asked the remaining subjects to express their perceptions about the online vendor. In particular, we measured research variables such as trusting beliefs, risk beliefs, loyalty, switching costs, pre-word of mouth and pre-likelihood of switching.

After measuring the subjects' perceptions of the online vendor, we randomly presented one of the eight scenarios to each of the subjects. The scenarios asked the subjects to imagine that they had just received an e-mail from the online vendor that they had named earlier. The message of the e-mail was that hackers had stolen their credit card information. The e-mail message contained a description of the specific remedial steps taken by the online vendor. These steps addressed three categories of justice, i.e., distributive, procedural, and interactional. For each category of justice, we

developed high and low conditions. Thus, the experimental design is a 2x2x2 fully crossed between-subjects arrangement. Once a scenario was presented, the subjects were instructed to answer the subsequent questions based on the given scenario. The research variables specific to the scenario were distributive justice, procedural justice, interactional justice, perceived breach, feelings of violation, post-word of mouth, and post-likelihood of switching.

4.4.2 Data Collection

An initial version of a Web-based survey questionnaire was developed to check the accuracy, suitability, and usability of the survey system. We created only two scenarios for a pilot test, and each questionnaire was associated with one of the two scenarios. In one scenario, the experimental conditions were all high on the three categories of justice. In contrast, in the other scenario, all three justice categories were manipulated to be low. This arrangement helped us evaluate the validity of justice manipulation as well as the quality of the questionnaire and its instructions by using only two scenarios instead of the eight that would have been required for a 2x2x2 standard factorial design. To recruit subjects for a pilot test, we used a market research firm that maintains a panel of U.S.-based Internet users. We collected responses from 45 subjects for the high condition and from 41 subjects for the low condition. Based on the subjects' responses and comments, we further clarified items, scenarios, and instructions in the questionnaire.

For the main study, we developed eight different survey questionnaires that contained experimental conditions that varied across the three categories

of justice (i.e., a 2x2x2 factorial design). We used the same market research firm to collect the data necessary for the main test. A sample frame of panel members between the ages of 30 and 59 was drawn up. The rationale behind the selection of this middle-aged group was that loss of personal information was expected to carry more realistic implications for this mature group than for the students often used in other studies.[17] An e-mail invitation — including a link to a Web-based survey questionnaire with one of the eight case scenarios — was sent to 6,539 U.S.-based members who had been randomly selected from the panel pool. Subjects were notified that participation was voluntary and that only aggregate data that contained no personally identifiable information would be used. A small cash reward deposited to PayPal or similar online accounts was offered for a completed response. The subjects were randomly assigned to one of the eight groups. The Web-based survey ran for two weeks, and we collected 1,036 responses, representing a complete response rate of 15.8%. However, 29 responses were not usable because they did not meet the age criterion. As a result, a total of 1,007 usable responses were considered for data analysis, which yielded an effective response rate of 15.4%. The response rate, although not high, was

[17] According to PEW (2009), the middle-aged group (30 to 59 years old) makes up about 58% of the Internet population in the U.S., while the younger group (younger than 29) and the elderly group (older than 60) represent about 31% and 11% of the Internet population. Furthermore, according to the Census Bureau (2008), the average income for the middle-aged group is about $46,908, whereas average incomes for the younger and elderly groups are, respectively, about $23,334 and $37,051. These statistics indicate that the segment from 30 to 59 years old makes up a majority of Internet users, and it is relatively well off. In fact, the Federal Trade Commission (2009) indicates that 71% of fraud complaints (i.e., credit card and government benefits fraud, and personal identity thefts) are reported by the middle-aged group, whereas the younger and elderly groups account, respectively, for 21% and 8% of the complaints. Hence, the middle-aged group is more sensitive to the security of personal financial data, and loss of privacy information, such as the breach of credit card information used in our scenario, is more relevant to this group.

quite typical of survey research. For example, other researchers have reported similar response rates when e-mail was used to recruit participants (e.g., Son et al. 2006, Hui et al. 2007, Pavlou and Gefen 2004). The sample was split into early and late respondents and t-tests found no difference in the means of any research variables. The average age of subjects was 48, and 55% were female. The range of average ages across the eight groups spanned from 47.92 to 48.79. Female were found to consist of 47% to 62% of the groups. No significant differences existed between the eight groups in terms of age and gender ($ps > 0.05$). We compared the profiles of both respondents and nonrespondents in terms of age and gender and found no statistically significant differences between the two groups ($ps > 0.05$).

4.4.3 Measures and Scenarios

To measure the research variables, we adapted existing scales whose psychometric properties are established in the literature (see Appendix G for measurement items and scenarios). These measures were grouped into three parts in the survey questionnaire, i.e., Parts A, B, and C. The first part measures individuals' perceptions about an online vendor. These measures were not specific to any scenarios. In Part B, one of the eight scenarios was presented, and then the subsequent measures were designed to be specific to the particular scenario. Finally, Part C included measures such as demographic characteristics and other general items that are not specific to a scenario.

Part A. We used three items adapted from Agarwal and Karahanna (2000) to measure perceived usefulness. Three perceived ease-of-use items

also were borrowed from Agarwal and Karahanna (2000). The trusting beliefs scale, which consists of four items, was adapted from the 11-item McKnight et al. (2002) scale. To capture risk beliefs, three items were adapted from Jarvenpaa and Tractinsky (1999). Three items were adapted from Kim and Son (2009) to capture loyalty. The three switching costs items were adapted from Kim and Son (2009). Pre-word of mouth was measured with three items adapted from Kim and Son (2009). To capture pre-likelihood of switching, three items were developed based on the measures of "alternative/switching experience" in Jones et al. (2002).

Part B. The scenarios in this study described various situations in which customers were informed via e-mail about a compromise of their credit card information.[18] In the distributive justice category, we manipulated the amount of a cash coupon offered by the vendor as part of an apology.[19] Specifically, subjects in the high distributive justice condition would receive a $100 cash coupon as an apology, whereas those in the low distributive justice condition would receive a $10 cash coupon. In the procedural justice category, ease or difficulty of finding contact information for customer service was manipulated. In particular, in the high procedural justice condition, subjects would be told that the contact information of the online store would be easily found on its homepage, but they would be required to spend some time to

[18] Disclosure of credit card information is classified as a type of privacy breach (Culnan and Williams 2009). In the case of such a security breach, companies must immediately report the incidence to customers in an e-mail or letter (Privacy Rights Clearing House 2013).

[19] We chose $100 versus $10 for the high versus low values for distributive justice. According to U.S. Law (FTC 1986), individuals' financial liability for an unauthorized credit card transaction is capped at $50. This evidence shows that $100 is considered adequate compensation for financial liability, whereas $10 is inadequate. In fact, TJX compensated its customers affected by privacy breaches with vouchers up to $60 (Schuman 2007). Thus, we believe that the levels of compensation supplied in the scenarios are realistic. The soundness of these experimental manipulations will be revisited in Section 4.2.

locate the information in the low procedural justice condition. Finally, in the interactional justice category, we varied the apologetic tone of a script of a voice message left on a customer's phone by a service representative of the vendor. Specifically, in the high interactional justice condition, subjects would receive a voice message that was apologetic and offered explanation about the incident, whereas they would a voice message with brief explanations in the low interactional justice condition. After a particular scenario, the measures specific to the particular scenario were followed. First of all, distributive justice was measured with three items adapted from Blodgett et al. (1997) and Price and Mueller (1986). The procedural justice scale consisted of three items adapted from Moorman (1991). We used four items adapted from Blodgett et al. (1997) and Moorman (1991) to measure interactional justice. The three perceived breach items were modified from a scale created by Pavlou and Gefen (2005). Feelings of violation were measured with three items, two of which were borrowed from the anger scale developed by Bonifield and Cole (2007), and the other was borrowed from the feelings of violation scale created by Robinson and Morrison (2000). Post-word of mouth and post-likelihood of switching were measured with the same scales of pre-word of mouth and pre-likelihood of switching, respectively.

Part C. We included a three-item fantasizing scale adapted from O'Guinn and Faber (1989) as a way to represent a marker variable. This marker variable was intended to help assess the extent of common method variance (CMV) (Lindell and Whitney 2001, Malhotra et al. 2006). Finally,

other variables such as age, gender, experience, and website usage were measured with single-item scales.

4.5 DATA ANALYSIS AND RESULTS

4.5.1 Measurement Model

We used six different fit indices to evaluate model fit: the comparative fit index (CFI), the nonnormed fit index (NNFI), the root mean square error of approximation (RMSEA), and the standardized root mean square residual (SRMR), the goodness-of-fit index (GFI), and the adjusted goodness of fit (AGFI). According to the literature, the fit indices criteria for an acceptable model are as follows: CFI $\geq$ 0.95, NNFI $\geq$ 0.95, RMSEA $\leq$ 0.06, SRMR $\leq$ 0.08; GFI $\geq$ 0.90, and AGFI $\geq$ 0.80 (Hu and Bentler 1999, Bearden et al. 1993, Gefen et al. 2000). Our measurement model included 15 multi-item factors with 47 corresponding indicators. In addition to the multi-item factors, the model included four one-item variables such as age, gender, experience, and website usage. The results of CFA showed that the measurement model was a highly satisfactory fit for the data: χ^2 (1057) = 2059.67, p <0.001, CFI = 0.99, NNFI = 0.99, RMSEA = 0.031, SRMR = 0.021, GFI = 0.93, AGFI = 0.91. Table 4.2 shows the means, standard deviations, composite reliability (CR), average variance extracted (AVE), and correlations of the measures based on the measurement model.

Besides model fit, we checked the convergent validity of the scales. Convergent validity is considered satisfactory if the factor loading of an indicator is 0.60 or higher (Chin et al. 1997). We inspected the output of LISREL 8 and found that among the indicators examined, the lowest loading

was 0.68. This result indicated an acceptable convergent validity for the measures. Subsequently, we examined the discriminant validity of the scales. Specifically, as a way to check if two scales were empirically differentiable, we performed a chi-square difference test for each pair of the factors (Bagozzi and Yi 1988). The results of the chi-square difference tests indicated that none of the pairs was considered statistically the same, which supported discriminant validity. In addition to convergent and discriminant validity, we also evaluated the reliability of the scales. The reliability of the scales was examined through two criteria, namely, CR and AVE. Reliability is said to be acceptable when CR $\geq$ 0.70 and AVE $\geq$ 0.50 (Bagozzi and Yi 1988, Fornell and Larcker 1981). As Table 4.2 shows, the minimum CR and AVE values, respectively, are 0.86 and 0.67, indicating acceptable reliability of the scales.

Table 4.2: Properties of Measurement Scales

					Correlation																
	ME	SD	CR	AVE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1. AGE	48.41	6.90	na	na	1																		
2. GEN	1.55	0.50	na	na	-0.07	1																	
3. EXP	5.63	3.71	na	na	0.02	-0.07	1																
4. WU	5.16	1.68	na	na	-0.07	-0.02	0.30	1															
5. PU	5.01	1.43	0.94	0.84	-0.09	-0.01	0.07	0.33	1														
6. PE	5.98	1.03	0.86	0.67	0.00	0.03	0.04	0.35	0.37	1													
7. TRUST	5.89	1.06	0.93	0.78	0.07	0.02	0.02	0.32	0.39	0.62	1												
8. RISK	2.47	1.45	0.94	0.84	-0.16	-0.01	-0.07	-0.12	-0.03	-0.29	-0.40	1											
9. LOY	4.87	1.57	0.95	0.86	-0.01	0.04	0.12	0.53	0.46	0.46	0.58	-0.18	1										
10. SC	2.96	1.62	0.92	0.79	-0.10	-0.02	0.04	0.17	0.22	-0.03	0.07	0.30	0.31	1									
11. WOM	5.98	1.16	0.96	0.88	0.01	0.06	0.08	0.41	0.37	0.60	0.79	-0.34	0.59	0.09	1								
12. LOS	2.85	1.47	0.92	0.79	-0.17	-0.10	-0.03	-0.19	-0.05	-0.24	-0.44	0.51	-0.35	0.02	-0.45	1							
13. DJ	2.93	1.76	0.95	0.86	-0.04	-0.06	0.02	0.13	0.15	0.02	0.11	0.09	0.17	0.14	0.06	0.09	1						
14. PJ	4.44	1.82	0.93	0.82	0.01	-0.07	0.00	0.12	0.16	0.22	0.26	-0.06	0.24	0.11	0.22	-0.08	0.41	1					
15. IJ	4.73	1.72	0.97	0.90	-0.01	-0.02	0.03	0.14	0.20	0.22	0.29	-0.08	0.22	0.11	0.24	-0.10	0.57	0.66	1				
16. PB	4.68	1.86	0.96	0.88	-0.02	-0.01	0.00	-0.07	-0.06	0.01	-0.09	0.14	-0.10	0.04	-0.08	0.13	-0.47	-0.29	-0.35	1			
17. FV	4.70	1.78	0.94	0.84	-0.04	0.04	-0.02	-0.02	0.03	-0.05	-0.09	0.25	-0.02	0.06	-0.08	0.17	-0.40	-0.29	-0.49	0.51	1		
18. PWOM	3.68	1.89	0.99	0.96	-0.02	-0.05	0.04	0.21	0.15	0.13	0.20	0.02	0.29	0.19	0.25	-0.06	0.65	0.56	0.62	-0.54	-0.47	1	
19. PLOS	4.67	1.80	0.97	0.91	-0.10	0.04	-0.04	-0.12	-0.04	-0.03	-0.12	0.12	-0.19	-0.12	-0.13	0.30	-0.46	-0.40	-0.45	0.61	0.54	-0.69	1

Notes

- n = 1,007.
- ME = mean; SD = standard deviation; CR = composite reliability; AVE = average variance extracted.
- AGE = age; GEN = gender; EXP = experience; WU = website usage; PU = perceived usefulness; PEOU = perceived ease of use; TRUST = trusting beliefs; RISK = risk beliefs; LOY = loyalty; SC = switching costs; WOM = pre-word of mouth; LOS = pre-likelihood of switching; DJ = distributive justice; PJ = procedural justice; IJ = interactional justice; PB = perceived breach; FV = feelings of violation; PWOM = post-word of mouth; PLOS = post-likelihood of switching.

Finally, we assessed the extent of CMV using the marker-variable technique (Lindell and Whitney 2001, Malhotra et al. 2006). As discussed earlier, our choice for the marker variable in this study was fantasizing. This marker variable was thought to be largely irrelevant in the context of information privacy (e.g., Son and Kim 2008), and thus its relationships with other variables are deemed to imply common method variance. According to Lindell and Whitney (2001), the smallest correlation (in absolute terms) between the marker variable and other variables is a conservative estimate of CMV. To calculate correlations, we again performed CFA while adding fantasizing to the original measurement model. The result showed that the smallest correlation with fantasizing was -0.01 (p = ns), indicating that CMV was not substantial in this particular study. Taken together with the desirable psychometric properties shown previously, our measures were considered appropriate for subsequent data analyses.[20]

4.5.2 Manipulation Checks

To check whether our experimental manipulation of justice items worked, we compared the means of justice perceptions (i.e., distributive, procedural, and interactional justice) across different experimental conditions. First, we compared the means of distributive justice between the high and low distributive justice groups. Whereas the mean value in the high group was 3.5, the mean value in the low group was 2.4. The mean difference between the groups was found to be statistically significant ($p < 0.001$). Second, we

[20] To further assess the validity of our measures, we performed exploratory factor analysis on the research factors shown in Figure 7. Appendix H reports the details of our analysis, including its results. The results provided additional support for the convergent and discriminant validity of our measures.

compared the means of procedural justice between the high and low procedural justice groups. The result indicated that subjects in the high treatment group provided significantly higher ratings (i.e., 5.2) than those in the low treatment group (i.e., 3.7) ($p < 0.001$). Finally, we tested mean differences in interactional justice between the high and low interactional justice groups. As expected, the means of interactional justice differed significantly between the high (i.e., 5.0) and low (i.e., 4.5) conditions ($p < 0.001$). Overall, these results indicate that all three manipulations worked as anticipated.

4.5.3 Test of Proposed and Alternative Models

To test the proposed model, we used a structural equation modeling (SEM) tool, LISREL 8 (Jöreskog and Sörbom 1996). In the structural model, justice perceptions and control variables were treated as exogenous variables, whereas psychological reactions and postincident outcomes were specified as endogenous variables. We estimated interaction effects using the means of latent variable scores (MLVS) technique (Jöreskog 1998) with the residual centering method (Lance 1988). It should be noted that the structural errors of the factors that belong to the same category were allowed to correlate. Thus, the errors of perceived breach and feelings of violation were specified to correlate. The same procedure was applied to the pairing of post-word of mouth and post-likelihood of switching. In addition to the proposed model, two alternative models were tested. The first alternative model was the same as the proposed model except that the effects of justice perceptions on psychological responses and postincident outcomes were excluded. The

second alternative model also mirrored the proposed model except that it excluded the effects of psychological responses on postincident outcomes. These alternative models were examined as a way to evaluate the relative importance of justice perceptions and psychological responses in determining postincident outcomes (Vandenberg and Grelle 2009).

Table 4.3 presents the results of the alternative and proposed models. The results of SEM showed that the proposed model was a reasonable representation of the phenomenon. In particular, the fit indexes were well within the acceptable ranges [χ^2 (1157) =2211.14, p <0.001, CFI = 0.99, NNFI = 0.99, RMSEA = 0.030, SRMR =0.022, GFI = 0.93, AGFI = 0.90]. In addition, we found that the proposed model explained a significant amount of the variation in the endogenous variables. Specifically, the model accounted on average for about half of the variance because SMCs range from 29% to 65% (see Table 4.3). Meanwhile, the first alternative model without the effects of justice perceptions fit the data poorly according to SRMR [χ^2 (1181) =2798.85, p <0.001, CFI = 0.99, NNFI = 0.98, RMSEA = 0.037, SRMR =0.111, GFI = 0.91, AGFI = 0.88]. Moreover, it accounted for less than 7% of the variance in perceived beach (4.0%) and feelings of violation (6.8%); this implies the importance of justice perceptions in understanding psychological responses. Meanwhile, this model explained about 50% of the variation on average in the behavioral outcomes. A chi-square test showed that the proposed model represents the data better than the first alternative model [$\Delta\chi^2$ (24) = 587.71, p <0.001]. The second alternative model without the effects of psychological responses generally fit the data better than the first alternative

model [χ^2 (1161) =2463.25, p <0.001, CFI = 0.99, NNFI = 0.99, RMSEA = 0.033, SRMR =0.111, GFI = 0.91, AGFI = 0.88]. Nevertheless, it did not perform better than the proposed model in terms of fit [$\Delta\chi^2$ (4) = 252.11, p <0.001]. As shown in Table 4.3, the proposed model accounts for 60% of the variance in behavioral outcomes on average, but the second alternative model explains only 51% of the variation in behavioral outcomes . These results imply that psychological responses play a significant role in regulating postincident outcomes. As a whole, our results suggest that the proposed model was superior to the partial models in terms of both fit and explained variance.

4.5.4 Test of Research Hypotheses

We took a conservative approach when testing research hypotheses because of a relatively large sample size (n = 1,007). Large samples tend to be sensitive to the statistical significance of even a small effect. Instead of using a standard 0.05 significance level, therefore, we adopted a more stringent level of significance of 0.01 (one-tailed) (Lang and Secic 2006). Despite such conservative testing, we found the data fully supported all of the hypotheses proposed in this study. Table 4.4 summarizes the results of the hypothesis tests.[21]

[21] In order to check the robustness of the results, we reran the proposed model by specifying the three types of justice perceptions as dummy variables. Appendix J shows the results of structural equation modeling analysis. As shown in Appendix J, these results with dummy variables are highly comparable to the original results.

Table 4.3: Results of Structural Equation Modeling Analysis

Antecedents		Alternative Model 1				Alternative Model 2				Proposed Model			
		PR		PI		PR		PI		PR		PI	
		PB	FV	PWOM	PLOS	PB	FV	PWOM	PLOS	PB	FV	PWOM	PLOS
Control variables	AGE	0.00	0.01	0.02	-0.07**	-0.01	0.00	0.01	-0.07*	-0.01	0.00	0.02	-0.07**
	GEN	-0.01	0.04	-0.05	0.05	-0.04	0.01	-0.02	0.03	-0.04	0.01	-0.02	0.03
	EXP	0.03	-0.01	-0.01	-0.02	0.04	0.01	-0.02	0.00	0.03	0.01	-0.01	-0.02
	WU	-0.05	-0.01	0.05	-0.01	-0.03	0.01	0.04	-0.01	-0.03	0.00	0.04	-0.01
	PU	-0.04	0.04	-0.04	0.02	-0.01	0.08*	-0.07**	0.04	-0.01	0.07*	-0.07**	0.04
	PEOU	0.15**	0.02	-0.00	0.02	0.11**	-0.01	-0.05	0.07	0.11**	-0.01	-0.02	0.03
	TRUST	-0.06	-0.03	0.03	0.05	0.04	0.08	-0.15***	0.18***	0.03	0.07	-0.11**	0.12*
	RISK	0.14***	0.26***	0.17***	-0.11***	0.19***	0.31***	0.02	0.04	0.18***	0.30***	0.09**	-0.07*
	LOY	-0.08	0.02	0.17***	-0.10**	-0.04	0.03	0.10**	-0.06	-0.03	0.04	0.11***	-0.07*
	SC	0.01	-0.03	0.09**	-0.09**	0.04	0.01	0.04	-0.05	0.04	0.01	0.05*	-0.07**
Preincident Outcomes	WOM			0.16***	0.02			0.22***	-0.03			0.20***	0.00
	LOS			0.11***	0.24***			-0.01	0.34***			0.03	0.28***
Justice perceptions	DJ					-0.41***	-0.29***	0.42***	-0.34***	-0.41***	-0.29***	0.28***	-0.11***
	PJ					-0.11**	0.00	0.23***	-0.16***	-0.11**	0.01	0.20***	-0.12***
	IJ					-0.05	-0.30***	0.22***	-0.17***	-0.06	-0.31***	0.17***	-0.09*
Interactions between justice perceptions	DJ x PJ					0.10*	0.04*	-0.01	0.03	0.10*	0.04	0.02	-0.01
	DJ x IJ					0.01	0.10**	-0.04	0.05	0.01	0.10**	-0.03	0.02
	PJ x IJ					-0.09*	0.01*	0.04	-0.04	-0.09*	0.01	0.02	-0.01
Psychological responses	PB			-0.38***	0.43***							-0.22***	0.36***
	FV			-0.32***	0.32***							-0.13***	0.23***
SMC (R^2)		0.04	0.07	0.48	0.51	0.30	0.35	0.60	0.42	0.29	0.34	0.65	0.55

Notes:

- n = 1,007.
- DJ = distributive justice; PJ = procedural justice; IJ = interactional justice; PB = perceived breach; FV = feelings of violation; PWOM = post-word of mouth; PLOS = post-likelihood of switching; AGE = age; GEN = gender; EXP = experience; WU = website usage; PU = perceived usefulness; PEOU = perceived ease of use; TRUST = trusting beliefs; RISK = risk beliefs; LOY = loyalty; SC = switching costs; WOM = pre-word of mouth; LOS = pre-likelihood of switching.
- Standard deviations within parenthesis
- * $p<0.05$, ** $p<0.01$, *** $p<0.001$ (two-tailed).

Effects of Justice Perceptions. We proposed earlier that three types of justice perceptions would influence perceived breach and feelings of violation (H1, H2, and H3). As shown in Table 4.4, distributive justice has significant effects on both perceived breach and feelings of violation (H1 supported). In addition, as expected, procedural justice exhibited a significant impact on perceived breach (H2 supported). Finally, consistent with our hypothesis, interactional justice was a significant antecedent of feelings of violation (H3 supported). Notably, procedural justice had little impact on feelings of violation, and interactional justice had no impact on perceived breach. These results support our claim that procedural justice relates to cognitive elements, whereas interactional justice reflects the emotional aspects of a psychological contract breach.

Interactions between Justice Perceptions. We predicted earlier that the effect of distributive justice on perceived breach would decrease with an increase in procedural justice. As expected, we found that procedural justice moderated the relationship between distributive justice and perceived breach (H4 supported). Moreover, in line with our expectations, we found that interactional justice indeed moderated the relationship between distributive justice and feelings of violation (H5 supported).

Table 4.4: Tests of Research Hypotheses

	Proposed paths	Path estimates	p-levels (one-tailed)	Hypothesis tests†
H1a	DJ → PB	-0.41	< 0.001	Supported
H1b	DJ → FV	-0.29	< 0.001	Supported
H2	PJ → PB	-0.11	< 0.01	Supported
H3	IJ → FV	-0.31	< 0.001	Supported
H4	DJ x PJ → PB	0.10	< 0.01	Supported
H5	DJ x IJ → FV	0.10	< 0.01	Supported
H6a	PB → PWOM	-0.22	< 0.001	Supported
H6b	PB → PLOS	0.36	< 0.001	Supported
H7a	FV → PWOM	-0.13	< 0.001	Supported
H7b	FV → PLOS	0.23	< 0.001	Supported

Notes:

- n = 1,007.
- †Hypothesis tests were performed based on a level of significance of 0.01.
- DJ = distributive justice; PJ = procedural justice; IJ = interactional justice; PB = perceived breach; FV = feelings of violation; PWOM = post-word of mouth; PLOS = post-likelihood of switching.

Our findings also show that the effect of procedural justice on perceived breach would increase with an increase in interactional justice (parameter estimate = -0.09, $p < 0.05$). It is important to note that the interaction between procedural justice and interactional justice was rarely observed in traditional settings in which relationships were based on face-to-face contacts (Tax et al. 1998, Skarlicki et al. 1999). A plausible explanation is that interactional justice is treated as a cue for the authenticity of procedural justice, especially in the context of online privacy breach recovery in which customers are separated from the actual recovery process. In particular, as service representatives represent the online firm in privacy recovery, customers' understanding of the complex recovery process can be supplemented by their interactions with the representatives. Whereas high

quality interactions provide a glimpse of the firm's policies to ensure fairness in the recovery, poor interaction experience may raise doubts of whether or not fair procedures are followed, and hence reduce customers' sensitivity to procedural justice. Appendix I shows three plots for the interaction effects found in this study. The figures clearly show that the interaction between procedural justice and interactional justice is distinctly different from that between distributive justice and procedural justice and also from that between distributive justice and interactional justice.

Effects of Psychological Responses. We proposed that post-word of mouth and post-likelihood of switching would be affected by perceived breach (H6) and feelings of violation (H7). As hypothesized, perceived breach influenced both post-word of mouth and post-likelihood of switching (H6 supported). Likewise, we found that feelings of violation had significant effects on postincident outcomes (H7 supported).

Controlled Effects. We found that pre-word of mouth had a significant effect on post-word of mouth (0.20, $p < 0.001$, two tailed) whereas pre-likelihood of switching exerted a significant effect on post-likelihood of switching (0.28, $p < 0.001$, two-tailed). Each of the justice perceptions had significant effects on both post-word of mouth and post-likelihood of switching. However, none of the interactions between justice perceptions had any significant impact on postincident outcomes, which implies the important role of psychological responses in a theoretical framework.

As indicated in Table 4.3, individual characteristics — i.e., age, gender, experience, and website usage — generally have little impact on

psychological responses and postincident outcomes. Only one of 16 paths proved significant, and this exception occurred between age and post-likelihood of switching (estimate = -0.07, $p < 0.01$, two-tailed). These results imply that older people are less likely to switch to alternatives at the postincident stage, but except for the age effect, individual characteristics generally do not have impact on online customer behavior. Unlike individual characteristics, however, customers' perceptions at the preincident stage such as perceived usefulness, perceived ease of use, trusting beliefs, risk beliefs, loyalty, and switching costs were significantly related with at least one of the endogenous variables. These results suggest that preincident perceptions largely mediate the impact of individual characteristics on online customer behavior.

4.6 DISCUSSION AND CONCLUSION

The main purpose of this study was to develop and empirically test a model that explains the role of an online firm's postincident recovery endeavor in mitigating the impact of a privacy breach on customer relationships. Drawing on the service recovery literature, we integrated the notions of justice perceptions and psychological responses into a theoretical framework describing how individuals react to an online firm's postincident actions. The proposed model was tested on data collected from 1,007 actual users of online vendors. The results of SEM analysis generally supported our model. As expected, three types of justice perceptions were sharply distinct from each other in their main and interaction effects on psychological responses. In addition, consistent with our hypotheses, psychological

responses were shown to play an important role in shaping postincident outcomes in the online context. Overall, our findings suggest that justice perceptions and psychological responses are the keys to a better understanding of online customer behavior after a privacy breach. This study provides researchers and practitioners with a conceptual tool for analyzing the effectiveness of organizational practices in mitigating the damaging effect of a privacy breach on customer relationships.

4.6.1 Theoretical Implications

4.6.1.1 Three Types of Justice Perceptions

The notion of justice and its related perceptions, i.e., distributive, procedural, and interactional justice, have been shown to be useful in explaining customers' privacy-related predispositions and behavioral consequences (Malhotra et al. 2004, Son and Kim 2008). However, most of these past studies treated justice perceptions only abstractly without reference to any specific firms or organizational practices. Our study is meaningful in that it is the first to examine individuals' justice perceptions that are specific to an online firm and to its remedies. Furthermore, past research lacks a systematic investigation into the subtle difference between three types of justice perceptions. This study contributes significantly to information privacy literature by showing how justice perceptions differ from each other in the context of an online privacy breach recovery. Specifically, this study demonstrates that distributive justice has positive effects on both cognitive and emotional evaluations. However, we found that procedural justice affects cognitive evaluations (i.e., perceived breach), whereas interactional justice

determines emotional evaluations (i.e., feelings of violation). Our findings bolster a common notion that compensation exerts profound effects on individuals' overall evaluations of a situation in question. More interesting, this study reveals a relatively unknown fact of justice perceptions that once compensation is taken into account, fair procedures affect only the cognitive side but not the emotional side, whereas respectful treatments affect the emotional side but not the cognitive side. We suspect that the emergence of this discernible pattern from this particular study results, at least partly, from its lean online context in which individuals' judgments about fairness are rarely intermixed with rich human relationships. In any case, more research is needed to explore the distinct nature of justice perceptions that may vary with respect to various privacy contexts. Overall, this study adds to the justice literature by showing theoretically as well as empirically the clearly discernible patterns behind justice perceptions, especially when these patterns are examined within the context of an online privacy breach recovery.

4.6.1.2 Interactions Between Justice Perceptions on Psychological Responses

Another contribution of this study to the information privacy literature is the interactions between justice perceptions that are unique to our context of an online firm's reactions to a privacy breach. As hypothesized, procedural justice somewhat complements distributive justice. Customers with an opportunity to be involved in the recovery process tend more than excluded customers to perceive the monetary reward as acceptable. Thus, a high level of procedural justice compensates, to some extent, for a low level of

distributive justice. Similarly, interactional justice complements distributive justice. High interactional justice implies that an online firm is committed to taking responsibility for a privacy incident (Ahmad 2002). In such a situation, customers are less likely to doubt the fairness of compensation than they are otherwise. Procedural justice and interactional justice are distinct in their interaction effects because procedural justice moderates the effect of distributive justice on perceived breach, but interactional justice moderates the effect of distributive justice on feelings of violation. As proposed by the psychological contract perspective, the cognitive-emotion taxonomy that differentiates procedural justice and interactional justice seems to hold well, even for explaining their interactions with distributive justice on psychological responses.

Although not hypothesized in this study, the interaction between procedural justice and interactional justice is shown to exist on perceived breach. In fact, this interaction between procedural justice and interactional justice was rarely observed in traditional settings in which relationships are based on face-to-face contact (Tax et al. 1998, Skarlicki et al. 1999). We reason that interactional justice is similar to procedural justice in that both are more concerned with means than with ends. For this reason, people often consider each of the "relationship-oriented" justice perceptions as a cue for the authenticity of the other dimension (Martínez-Tur et al. 2006). Especially in a domain in which relational bonds are unstable, people are known to evaluate the two types of justice perceptions together instead of independently (Luo 2007). Therefore, when interactional justice is lower, online customers are

less likely to be sensitive to the question of whether or not fair procedures are followed. This is because in the case of low interactional justice, their reactions are likely to be generally unenthusiastic regardless of the level of procedural justice. Meanwhile, when interactional justice is higher, online customers will be more sensitive to the level of procedural justice. Thus, in the online privacy domain, the effects of procedural justice on perceived breach will be stronger when interactional justice is higher. Consistent with this reasoning, procedural justice is shown to be largely synergistic with interactional justice; that is, the impact of procedural justice is not maximized when interactional justice is low. Our findings will add to the growing literature on justice perceptions and their complex effects on individuals' overall evaluations.

4.6.1.3 Perceived Breach and Feelings of Violation

To the best of our knowledge, this is the first study to formally examine psychological contract violation in an online privacy breach. The lack of attention to the psychological contract perspective is surprising when one considers that a privacy breach constitutes a severe breach of a psychological contract in online commercial transactions. Drawing on the taxonomy proposed by Morrison and Robinson (1997), we explicitly differentiated between perceived breach, which represents a cognitive response, and feelings of violation, which indicate an emotional response. Our findings show that feelings of violation are indeed distinct from perceived breach ($r = 0.51$). Moreover, the emotional factor (i.e., feelings of violation) is found to affect post-word of mouth (parameter estimate = -0.13, $p < 0.001$) as

well as post-likelihood of switching (parameter estimate = 0.23, $p < 0.001$) after controlling for its cognitive counterpart (i.e., perceived breach). We should note that Pavlou and Gefen (2005) earlier introduced the notion of a psychological response in their effort to examine the buyer-seller relationship in the context of online auctions. Their study, however, focused mainly on the cognitive aspects of a breach and paid less attention to its emotional factors. Our results indicate that the current theory needs to be expanded to include both cognitive and emotional responses. We believe that our dual approach to psychological responses is effective not only in examining privacy problems but also in understanding other social exchange relationships.

4.6.1.4 Extending Justice Theories by Including Psychological Responses

Although both justice perceptions and psychological responses are known to explain potential conflicts arising from social exchange relationships (Gilliland 1993, Pavlou and Gefen 2005), those concepts have rarely been integrated into a coherent, unified framework. To integrate these two views, the present study draws on the service recovery literature, which posits that customers' specific beliefs with regard to organizational remedies determine overall psychological evaluations, which in turn, regulate behavior (Hoffman and Kelly 2000, Maxham and Neyemeyer 2002). Specifically, our conceptual model postulates that customers' specific justice perceptions determine overall psychological evaluations, which are summarized into perceived breach and feelings of violation. Furthermore, these psychological evaluations play a key role in shaping customer behavior after an online privacy breach recovery.

An interesting result was that when perceived breach and feelings of violation were excluded from the model, no interactions were significant in determining postincident outcomes. This result implies that a conceptual model that emphasizes the justice perspective but excludes psychological responses is likely to yield a limited view of online customer behavior in a situation in which individuals react to an online firm's postincident recovery endeavor to recover customer relationships from a privacy breach. To the best of our knowledge, no prior studies have combined justice perceptions and psychological responses and then show the efficacy of this integrative approach in the special context of online customer behavior after a privacy breach.

4.6.1.5 The Specificity of the Online Privacy Breach Context

The issues surrounding an online privacy breach and disaster recovery differ substantially from those in traditional retailing (Holloway and Beatty 2003, Forbes et al. 2005). For example, security and privacy issues are considered particularly serious and critical in the online environment (Zeithaml et al. 2002, Malhotra et al. 2004). Moreover, although personal relationships are lacking in the online setting, they are vital to the offline service experience and equally important to online businesses in maintaining customer relationships in the postincident stage (Fan et al. 2010). Drawing on both the privacy and service recovery literature, we argue that these characteristics specific to online privacy breach and recovery setting make justice perceptions particularly relevant in our study context. In fact, we observed clearly discernible patterns among justice perceptions and their

interactions that are predicted by our integrated theoretical framework. We suspect that in the offline environment the effects of justice perceptions on psychological responses would be more complex than those found in this study. This is because in such a traditional setting justice perceptions and psychological responses are more likely to be affected by a history of interpersonal relations accumulated over the course of business interactions and failure recoveries.

Moreover, our model includes several hypotheses related to the interactions of justice perceptions that are tightly intertwined with the online privacy breach and recovery domain under study. Our findings suggest that in line with our predictions, procedural justice and interactional justice act more or less complementary to distributive justice. In contrast, we found that procedural justice is synergistic with interactional justice (see Appendix I). Note that these interesting interaction effects were seldom shown in other contexts. We argue that the online privacy breach context examined in this study causes participants to carefully evaluate each dimension of justice perceptions without being affected by ongoing face-to-face interactions common in organizational and traditional retail settings. Taken together, we extend the boundary of knowledge in the field of information privacy by developing nuanced accounts specific to the domain in question and basing them on a more generalized and integrative framework

4.6.2 Managerial Implications

Our findings provide practitioners with valuable insights into how to salvage customer relationships damaged by privacy-related incidents. First,

we advocate that privacy breach recovery should be carefully reengineered. Specifically, managers could consider creating privacy breach remedies that allow for recovery efforts directed at improving the psychological responses experienced by customers. They should have an array of tools and resources available to address the specific needs of customers. Recall that, in our study, perceived breach and feelings of violation were greatly affected by compensation. However, perceived breach became less sensitive to compensation when a fair procedure was in place, and feelings of violation were less affected by compensation when respectful interpersonal treatment was experienced. This result is an important reminder that redressing privacy breaches means more than enacting all three aspects of privacy breach recovery. Thus, online firms must carefully consider the specific psychological responses to improve customers' privacy situations.

It is also worth noting that interactional justice amplified the effect of procedural justice on perceived breach. This finding implies that when interactional justice is low, organizational efforts to boost procedural justice are likely to be wasted and have little impact on perceived breach. Procedural justice and interactional justice are similar in that both are concerned with "means" to ends. Because of this resemblance, interpersonal treatment might be considered as a testimonial for the firm's practices. Although conventional wisdom suggests the significance of procedural justice and interactional justice, their synergistic power is not yet widely known. Our study clearly shows that interactional justice is a necessary condition to maximize the return from a firm's adherence to fair procedures. The online environment facilitates

information dissemination, which is vital for notifying customers about the process of remedying a privacy breach. However, the lack of physical contacts could hinder customers' understanding of the complex recovery process. In light of this understanding, to maximize the return from adherence to fair procedures, online firms should consider enhancing interpersonal interactions in developing their privacy breach recovery capabilities.

4.6.3 Limitations and Further Research

We examined online customers' reactions to a particular firm with which the customers had had actual experience. This approach contrasts with the approach of past studies in which individuals' attitudes and behavior were examined without reference to any real business (Son and Kim 2008, Dinev and Hart 2006, Stewart and Segars 2002). As a result, our findings are generally expected to be more realistic and practical than those of prior studies. However, this study employed hypothetical scenarios to simulate privacy incidents; such simulation is unavoidable to some degree, but nevertheless impairs the study's realism. We believe, all things considered, that the research methodology adopted in this study is reasonable. However, the findings of this study need to be corroborated by other field studies in which actual breaches and organizational responses are examined in real-life settings.

Another limitation relates to the cross-sectional nature of the data. Our model primarily implies a longitudinal analysis that examines customers' behaviors separately before and after a privacy breach. Although the model does not necessarily preclude a cross-sectional analysis as performed in the

present study, more conclusive inferences from our findings require their evaluation against a future longitudinal study. On a related issue, we used a survey questionnaire to measure pre- and postincident outcomes; consequently, CMV was considered a potential threat to the validity of our findings. As noted earlier, we explicitly checked for CMV and found it was not particularly problematic. Nevertheless, the findings of this study should be viewed with this potential bias in mind.

Furthermore, our findings are not necessarily generalizable to other settings. For example, the present study dealt with a case in which a firm notifies online customers of a breach. However, in some cases, the media may report an incident before a firm contacts its customers. Our findings cannot be generalized to such a situation in which customers receive the news of a breach from sources other than the firm responsible for handling the incident. Caution should be exercised when the model is applied to settings other than the one analyzed here.

In order to accurately describe online customer behavior, we tried to incorporate as many relevant factors as possible (including control variables) into the model. Nevertheless, we cannot exclude the possibility that variables were omitted that could change the study's result. For example, this study did not take into account perceived value or service quality, which are known to be significant determinants of online customer behavior (Devaraj et al. 2002, Kim et al. 2005). In addition, privacy concern is considered one of those potentially important factors. Our decision to exclude privacy concern from the model was deliberate and based on a research finding that trusting and risk

beliefs fully mediate the impact of privacy concern on behavioral intention (Malhotra et al. 2004). Given that trusting and risk beliefs are already controlled for, we believe that the impact of privacy concern on postincident outcomes will be minimal, if any, in our study. Yet our findings should be interpreted carefully until the impact of privacy concern is known.

In this study, procedural justice is conceptualized as the fairness of decision-making procedures. This conceptualization of procedural justice can manifest itself in many ways, such as accessibility (e.g., ease of finding a representative), speed (e.g., time taken to perform a procedure), flexibility (e.g., adaptability of procedures to suit individual needs), process control (e.g., ability to express views freely), etc. (Tax et al. 1998). However, in our scenarios, the notion of procedural justice was operationalized with a focus on accessibility and speed while other facets — for example, flexibility and process control — were not taken into account. Thus, readers should be cautious when they attempt to generalize our findings beyond the specific aspects of procedural justice examined in this study.

It is also worth noting that the high interactional justice group (i.e., 5.0) and the low interactional justice group (i.e., 4.5) had the lowest mean difference. In this study, interactional justice was manipulated by the tone of the service representatives in phone calls, which were used as a supplement to the main message delivered through e-mails. This manipulation of interactional justice is not unrealistic because a significant portion of customers would want to call the company to ask for more information on the privacy breach. Nevertheless, although the two conditions of interactional

justice differed significantly ($p < 0.001$), the role of interactional justice could have been more evident, given better manipulation.

This study opens up a number of exciting avenues for further research. First, three types of justice perceptions were examined to capture different aspects of perceived fairness. However, the justice literature suggests still another dimension of justice, namely, informational justice (Greenberg 1990, Colquitt 2001). As a concept separate from interactional justice, informational justice is concerned with whether the factors involved in a decision are properly explained. This concept of emphasizing fair communication is thought to differ from other justice perceptions related to outcomes (i.e., distributive justice), procedures (i.e., procedural justice), and interpersonal treatment (i.e., interactional justice). Although informational justice has not been accepted as widely as other justice perceptions, it certainly has the potential to broaden our understanding of customer behavior in the context of information privacy.

Additionally, this study focuses on the ways the justice perceptions could be facilitated in an online privacy breach recovery. In particular, distributive justice was facilitated by the amount of cash coupon compensation. Procedural justice was administrated by the availability of contact information on the firm's website. Interactional justice was applied through apologies and explanations. While this study explored the typical ways in which justice perceptions could be facilitated, future research could explore other technological characteristics that could help ensure fairness in online privacy breach recovery.

Furthermore, this study shows the significance of emotion in privacy-related behavior. In the present study, one's emotion is represented by a single factor called "feelings of violation." Yet customers' emotional responses are likely to manifest more subtle and complex patterns than what is captured by a one-dimensional variable. In fact, research shows a variety of emotional responses — for example, happiness, pride, anger, and sadness — that are related to perceived fairness and thus deemed relevant in the context of information privacy (Ruth et al. 2002). We encourage researchers to identify emotional factors that may be important to privacy research and examine how such emotions differentially affect behavioral outcomes.

Finally, in this study, we only focused on a firm's "immediate" reactions to a breach. However, maintaining customer relationships requires "long-term" efforts (Reichheld 2003). Thus, it is important to examine the overall effectiveness of such ongoing efforts over time. Especially, the temporal sequence of organizational measures could matter in determining their effectiveness. For example, a tactic designed to boost word of mouth is likely to be effective only when a prior action to prevent customers from switching to an alternative provider works. If a firm's immediate reaction to a breach falls short of keeping current customers, subsequent measures are unlikely to succeed. Taken together, further research could examine whether, and if so how, customers' perceptions and behavior change over time in the context of online privacy breach recovery.

CHAPTER 5 CONCLUSION

This thesis focuses on privacy issues in the contexts of online social interactions and commercial transactions. The three studies provide insights on individuals' privacy trade-off, behavioral responses to embarrassing exposures as well as psychological responses to organizational remedies. Specifically, Study I draws on the hyperpersonal framework and the privacy calculus perspective to elucidate the roles of privacy concerns and social rewards in synchronous online social interactions. In particular, this study examines the causes and the behavioral strategies that individuals utilize to protect their privacy. 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.

Study II draws on the social exchange theory to explain the consequences of an embarrassing exposure in online social networks. Specifically, this study examines the effects of information dissemination and network mutuality on individuals' exchange assessment as well as how this assessment shapes their behavioral responses. Results suggest that information dissemination and network mutuality jointly determine individuals' perceptions of relationship bonding and privacy invasion. Additionally, whereas perceived relationship bonding impedes both transactional avoidance and interpersonal avoidance, it leads to approach behavior. Further, while perceived privacy invasion increases transactional avoidance, it reduces approach behavior.

Study III focuses on an online firm's postincident recovery endeavor in mitigating the impact of a privacy breach on customer relationships. Drawing on the service recovery literature, this study integrates the notions of justice perceptions and psychological responses into a theoretical framework that describes how individuals react to an online firm's postincident recovery endeavor. Results indicate that the three types of justice perceptions (i.e., distributive justice, procedural justice, and interactional justice) differently affect psychological responses (i.e., perceived breach and feelings of violation). Moreover, justice perceptions are found to interact to influence their psychological responses, which are shown to be important in shaping postincident outcomes such as post-word of mouth and post-likelihood of switching.

Overall, the three studies are believed to provide a solid understanding on individuals' privacy-related behavior across different contexts. It is worth to note that the three studies of this thesis closely resemble the theoretical underpinning of the APCO framework (Smith et al. 2011). According to this framework, individuals' privacy-related psychological responses (i.e., perceptions, emotions, and beliefs) can be influenced by a divergent collection of antecedents specific to different contexts. Furthermore, the APCO framework underscores the importance of examining behavioral outcomes, which are driven by individuals' privacy related psychological responses. More important, the authors have explicitly noted the essentiality of considering privacy issues in different contexts. In this thesis, the three studies provide a focused perspective on privacy issues across online social

interactions and commercial transactions contexts. Collectively, by considering antecedents and outcomes in online social interactions and online commercial transactions, this thesis provides a useful macro understanding that would be salient across multiple disciplines and contexts. In particular, Study I identifies 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 tradeoffs 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. 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. Additionally, this study also presents new insights to prior privacy-related studies by extending the privacy calculus lens to the context of synchronous online social interactions. Essentially, in the absence of monetary or tangible rewards, social rewards are found to be just as attractive in balancing privacy concerns and governing individuals' behavior.

Furthermore, as discussed in Study II, this thesis enriches IS research on social interactions by providing a taxonomy of behavioral responses to embarrassing exposure in online social networks. Drawing on the dichotomy of passive and active behavior, Study II classifies behavioral responses into

four different types, namely inaction, transactional avoidance, interpersonal avoidance, and approach. The proposed taxonomy is expected to be helpful in analyzing a variety of behavior commonly performed in response to embarrassing exposures and thus serve as a useful tool for further examination of individuals' response behavior in online social networks.

Study II also makes important implications for application designers. In particular, by facilitating the traceability of the target's profile, posting with tagging has come under heavy criticism. Given the influence of network mutuality on target's interpretation of an embarrassing exposure, application designers may contemplate how they can use information on network mutuality to their advantage. For example, in cases where embarrassing content is disseminated, a target's perception of privacy invasion can be mitigated if posting with tagging is discouraged for a disseminator who has low network mutuality with the target. On the other hand, if the disseminator has high network mutuality with the target, the disseminator should be promptly notified regarding the option of tagging the target to induce the perception of relationship bonding.

Finally, Study III extends justice theories by including psychological responses to better explain potential conflicts arising from social exchange relationships. Specifically, this study draws on the service recovery literature, which posits that customers' specific beliefs with regard to organizational remedies determine overall psychological evaluations, which in turn, regulate behavior. Furthermore, Study III enriches existing understanding on online privacy breach recovery by formally examining psychological contract

violation in an online privacy breach incident. Overall, the inclusion of both cognitive and emotional responses is expected to be effective not only in examining privacy problems but also in understanding other social exchange relationships.

The findings in Study III also imply that online firms must carefully consider the specific psychological responses to improve customers' privacy situations. In particular, this study clearly shows that interactional justice is a necessary condition to maximize the return from a firm's adherence to fair procedures. The online environment facilitates information dissemination, which is vital for notifying customers about the process of remedying a privacy breach. However, the lack of physical contacts could hinder customers' understanding of the complex recovery process. In light of this understanding, to maximize the return from adherence to fair procedures, online firms should consider enhancing interpersonal interactions in developing their privacy breach recovery capabilities.

The findings of this thesis should be viewed with some limitations in mind. First, this research assumes that individuals' behavior in online social interactions is not essentially driven by malicious motivations, such as cyberbullying and Internet predation. Malevolent individuals could exhibit vastly different behavior due to their insidious motives. Despite this inadequacy, this research strives to be applicable to the general population.

The contributions of this thesis may also be limited by using a mock-up online social networking website in Study II. While the general layout and technical features of the mock-up website resembled those of a real online

social networking platform, the mock-up website may not reflect the actual online social networking environment entirely. However, in the actual environment, we could neither manipulate the experimental conditions (i.e., controlling the number of mutual friends the subjects and the friend share) nor capture subjects' actual behavioral responses (i.e., intercepting the private messages the subjects sent to his or her friends). Therefore, despite the limitation, the employment of this mock-up website is necessary. Future research will be necessary to verify the impact of embarrassing exposures on relationship bonding and privacy invasion in a more natural setting.

Another limitation is that Study III examined online customers' reactions to a particular firm with which the customers had had actual experience. This approach contrasts with the approach of past studies in which individuals' attitudes and behavior were examined without reference to any real business (Son and Kim 2008, Dinev and Hart 2006, Stewart and Segars 2002). As a result, findings of Study III are generally expected to be more realistic and practical than those of prior studies. However, this study employed hypothetical scenarios to simulate privacy incidents; such simulation is unavoidable to some degree, but nevertheless impairs the study's realism. Therefore, the findings of this study need to be corroborated by other field studies in which actual breaches and organizational responses are examined in real-life settings.

This thesis opens several interesting research opportunities. First, there is value in investigating "objective" measures of behavior in online social interactions, as opposed to our current reflective self reported

measurements in Study I. It is possible that individuals' recall may not completely reflect their actual behavior due to 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, Study II of this thesis has focused on behavioral responses facilitated by online social networking websites. In a real setting, the target might engage in behavior beyond the online environment. For instance, in response to the embarrassing exposure, the target might actively avoid transaction by complaining to the disseminator in physical encounters. Likewise, interpersonal avoidance might not be limited to breaking up connectivity within online social networks but could also escalate to relationship termination in the offline environment. Approach behavior might manifest in the target's active involvement during face-to-face interactions. Hence, future research could investigate how an embarrassing exposure that occurs within online social networks influences individuals' behavior in the offline environment.

Finally, Study III only focused on a firm's "immediate" reactions to a breach. However, maintaining customer relationships requires "long-term" efforts (Reichheld 2003). Thus, it is important to examine the overall effectiveness of such ongoing efforts over time. Especially, the temporal sequence of organizational measures could matter in determining their effectiveness. For example, a tactic designed to boost word of mouth is likely

to be effective only when a prior action to prevent customers from switching to an alternative provider works. If a firm's immediate reaction to a breach falls short of keeping current customers, subsequent measures are unlikely to succeed. Taken together, further research could examine whether, and if so how, customers' perceptions and behavior change over time in the context of online privacy breach recovery.

BIBLIOGRAPHY

Abril, P. S. 2007. "A (My)Space of One's Own: On Privacy and Online Social Networks," Northwestern Journal of Technology and Intellectual Property (6:1), pp 74-88.

Acohido, B., and J. Swartz (2007), "TJX Discloses Largest Data Theft : 45.7M Customers," *USA Today*, March 30. Retrieved from http://www.usatoday.com/money/industries/retail/2007-03-29-tjx-id-theft_n.htm

Acquisti, A., and Gross, R. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," Lecture Notes in Computer Science:4258), pp 36-58.

Agarwal, R., and E. Karahanna (2000), "Time Flies When You're Having Fun: Cognitive Absorption and Beliefs about Information Technology Usage," *MIS Quarterly*, 24, 4, pp. 665-694.

Agnew, C. R., Van Lange, P. A. M., Rusbult, C. E., and Langston, C. A. 1998. "Cognitive Interdependence: Commitment and the Mental Representation of Close Relationships," Journal of Personality and Social Psychology (74:4), pp 939-954.

Ahmad, S. (2002), "Service Failures and Customer Defection: A Closer Look at Online Shopping Experiences," *Managing Service Quality*, 12, 1, pp. 19-29.

Albert, J.K. (1992) "An Inferential/Strategic Explanation for the Social Organization of Teases," Journal of Language and Social Psychology, 11, pp. 153-177.

Alberts, J. K. 1992. "A Strategic/Inferential Explanation for the Social Organization of Teasing," Journal of Language and Social Psychology (11:3), pp 153-177.

Alberts, J. K., Kellar-Guenther, Y., and Corman, S. R. 1996. "That's Not Funny: Understanding Recipients' Responses to Teasing," Western Journal of Communication (60:4), pp 337-357.

Alge, B. J. 2001. "Effects of Computer Surveillance on Perceptions of Privacy and Procedural Justice," Journal of Applied Psychology (86:4), pp 797–804.

Altman, I., and Taylor, D. 1973. Social Penetration: The Development of Interpersonal Relationships, (Holt, Rinehart & Winston: Oxford, England.

Anderson, C.L., and R. Agarwal (2011), "The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information," Information Systems Research, 22, 3, pp. 469-490.

Archer, R. L., and Berg, J. H. 1978. "Disclosure Reciprocity and Its Limits: A Reactance Analysis," Journal of Experimental Social Psychology (14:6), pp 527-540.

Argo, J.J., K. White, and D.W. Dahl (2006), "Social Comparison Theory and Deception in the Interpersonal Exchange of Consumption Information," Journal of Consumer Research, 33, 1, pp. 99-108.

Aron, A., Aron, E. N., and Smollan, D. 1992. "Inclusion of Other in the Self Scale and the Structure of Interpersonal Closeness," Journal of Personality and Social Psychology (63:4), pp 596-612.

Ashworth, L., and C. Free (2006), "Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns," *Journal of Business Ethics*, 67, pp. 107-123.

Awad, N. F., and Krishnan, M. S. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization," MIS Quarterly (30:1), pp 13-28.

Bagozzi, R.P., and Y. Yi (1988), "On the Evaluation of Structural Equation Models," *Journal of the Academy of Marketing Science*, 16, 1, pp. 74-94.

Barclay, D., C. Higgins, and R. Thompson (1995), "The Partial Least Squares Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration," Technology Studies, 2, 2, pp. 285-324.

Baron, R.M., and D.A. Kenny (1986), "The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations," Journal of Personality and Social Psychology, 51, 6, pp. 1173-1182.

Barclay, L. J., D.P. Skarlicki, and S.D. Pugh (2005), "Exploring the Role of Emotions in Injustice Perceptions and Retaliation," *Journal of Applied Psychology*, 90, 4, pp. 629-643.

Bart, Y., V. Shankar, F. Sultan, and G.L. Urban (2005), "Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study," *Journal of Marketing*, 69, 4, pp. 133-152.

Bearden, W.O., R.G. Netemeyer, and M.F. Mobley (1993), *Handbook of Marketing Scales: Multi-item Measures for Marketing and Consumer Behavior Research*, Newbury Park, CA: Sage Publications.

Beatty, S.E., and L.R. Kahle (1988), "Alternative Hierarchies of the Attitude-Behavior Relationship: The Impact of Brand Commitment and Habit," *Journal of the Academy of Marketing Science*, 16, 2, pp. 1-10.

Beatty, S. E., and Lee, J. 1996. "Customer-Sales Associate Retail Relationships," Journal of Retailing (72:3), pp 223–247.

Beck, L., and I. Ajzen (1991), "Predicting Dishonest Actions: Using the Theory of Planned Behavior," Journal of Research in Personality, 25, 3, pp. 285-301.

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," MIS Quarterly (35:4), pp 1017-1041.

Bendapudi, N., and L.L. Berry (1997), "Customers' Motivations for Maintaining Relationships With Service Providers," *Journal of Retailing*, 73, 1, pp. 15-37.

Ben-Ze'ev, A. (2003), "Privacy, Emotional Closeness, and Openness in Cyberspace," Computers in Human Behavior, 19, 4, pp. 451-467.

Bies, R.J., and J.S. Moag (1986), "Interactional Justice: Communication Criteria of Fairness," In *Research on Negotiation in Organizations*, R. J. Lewicki, B. H. Sheppard, and B. H. Bazerman (Eds.), Vol. 1, Greenwich, CT: JAI Press, pp. 43-55.

Bitner, M. J., B. H. Booms, and M.S. Tetreault (1990), "The Service Encounter: Diagnosing Favorable and Unfavorable Incidents," *Journal of Marketing*, 54, 1, pp. 71-84.

Blau, P. 1964. Exchange and Power in Social Life, (Wiley: New York.

Blau, P. M. 1986. Exchange and Power in Social Life, (New Brunswick, NJ: Transaction Books.

Blodgett, J.G., D.J. Hill, and S.S. Tax (1997), "The Effects of Distributive, Procedural, and Interactional Justice on Postcomplaint Behavior," *Journal of Retailing*, 73, 2, pp. 185-210.

Bonifield, C., and C. Cole (2007), "Affective Responses to Service Failure: Anger, Regret, and Retaliatory Versus Conciliatory Responses," *Marketing Letters*, 18, 1-2, pp. 85-99.

Boxer, D., and Cortés-Conde, F. 1997. "From Bonding to Biting: Conversational Joking and Identity Display," Journal of Pragmatics (27:3), pp 275-294.

Brass, D. J., and Burkhardt, M. E. 1993. "Potential Power and Power Use: An Investigation of Structure and Behavior," Academy of Management Journal (36:3), pp 441-470.

Brockner, J., Konovsky, M., Cooper-Schneider, R., Folger, R., Martin, C., and Bies, R. J. (1994), "Interactive Effects of Procedural Justice and Outcome Negativity on Victims and Survivors of Job Loss," *Academy of Management Journal*, 37, 2, pp. 397-409.

Brockner, J., and Wiesenfeld, B. M. (1996), "An Integrative Framework for Explaining Reactions to Decisions: Interactive Effects of Outcomes and Procedures," *Psychological Bulletin*, 120, 2, pp. 189-208.

Bumgarner, B. A. 2007. "You Have Been Poked: Exploring the Uses and Gratifications of Facebook among Emerging Adults," First Monday (12:11).

Burgoon, J.K., R. Parott, B.A. Le Poire, D.L. Kelley, J.B. Walther, and D. Perry (1989), "Maintaining and Restoring Privacy through Communication in Different Types of Relationships," Journal of Social and Personal Relationships, 6, 2, pp. 131-158.

Burnham, T.A., J.K. Frels, and V. Mahajan (2003), "Consumer Switching Costs: A Typology, Antecedents, and Consequences," *Journal of the Academy of Marketing Science*, 31, 2, pp. 109-126.

Campell, A.J. (1997), "Relationship Marketing in Consumer Markets: A Comparison of Managerial and Consumer Attitudes about Information Privacy," Journal of Direct Marketing, 11, 3, pp. 44-57.

Campos, B., Keltner, D., Beck, J. M., Gonzaga, G. C., and John, O. P. 2007. "Culture and Teasing: The Relational Benefits of Reduced Desire for

Positive Self-Differentiation," Personality and Social Psychology Bulletin (33:1), pp 3-16.

Canessa, E., and R.L. Riolo (2003), "The Effect of Organizational Communication Media on Organizational Culture and Performance An Agent-Based Simulation Model," Computational and Mathematical Organization Theory, 9, 2, pp. 147-176.

Caplan, S.E., and J.S. Turner (2007), "Bringing Theory to Research on Computer-Mediated Comforting Communication," Computers in Human Behavior, 23, 2, pp. 985-998.

Carlson, J.R., and R.W. Zmud (1999), "Channel Expansion Theory and the Experiential Nature of Media Richness Perceptions," The Academy of Management Journal, 42, 2, pp. 153-170.

Carlson, P.J., and G.B. Davis (1998), "An Investigation of Media Selection Among Directors and Managers: From "Self" to "Other" Orientation," Management Information Systems Quarterly, 22, 3, pp. 335-362.

Carpenter, C. J., & Spottswood, E. L. (2013). Exploring romantic relationships on social networking sites using the self-expansion model. Computers in Human Behavior, 29(4), 1531-1537.

Census Bureau (2008), "Annual Social and Economic (ASEC) Supplement," Retrieved from http://www.census.gov/hhes/www/cpstables/032009/perinc/new01_001.htm

Chebat, J. C., and Slusarczyk, W. (2005), "How Emotions Mediate the Effects of Perceived Justice on Loyalty in Service Recovery Situations: An Empirical Study," *Journal of Business Research*, 58, 5, pp. 664-673.

Cheek, J.M., and Buss, A.H. (1981), "Shyness and Sociability," *Journal of Personality and Social Psychology*, 41, 2, pp. 330-339.

Chen, P.Y. and L.M. Hitt (2002), "Measuring Switching Costs and the Determinants of Customer Retention in Internet-Enabled Businesses: A Study of the Online Brokerage Industry," *Information Systems Research*, 13, 3, pp. 255-274.

Chin, W.W. (1998), "The Partial Least Squares Approach to Structural Equation Modeling," In: Modern Methods for Business Research, G.A. Marcoulides (Ed.),Mahway, NJ, Lawrence Erlbaum Associates Inc, pp. 295-336.

Chin, W.W., A. Gopal, and W.D. Salisbury (1997), "Advancing the Theory of Adaptive Structuration: The Development of a Scale to Measure Faithfulness of Appropriation," *Information Systems Research*, 8, 4, pp. 342-367.

Chuang, S. C., Y.H. Cheng, C.J. Chang, & S.W. Yang (2012), "The Effect of Service Failure Types and Service Recovery on Customer Satisfaction: A Mental Accounting Perspective," *The Service Industries Journal*, 32, 2, pp. 257-271.

Cho, Y., I. Im, R. Hiltz, and J. Fjermestad (2001), "The Effects of Post-Purchase Evaluation Factors on Online vs. Offline Customer Complaining Behavior: Implications for Customer Loyalty," *Advances in Consumer Research*, 29, 1, pp. 318-326.

Claburn, T. (2008), "This Year's Data Breaches Surpass 2007 Totals," *Information Week*, August 25, Retrieved from http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=210200622.

Clayton, S.D. (1992), "The Experience of Injustice: Some Characteristics and Correlates," *Social Justice Research*, 5, 1, pp. 71-91.

Cohen, J. (1992), "A Power Primer," Psychological Bulletin, 112, 1, pp. 155-159.

Collier, J.E., and C.C. Bienstock (2006), "Measuring Service Quality in E-Retailing," Journal of Service Research, 8, 3, pp. 260-275.

Collins, N. L., and Miller, L. C. 1994. "Self-Disclosure and Liking: A Meta-Analytic Review," Psychological bulletin (116:3), pp 457-475.

Colquitt, J.A. (2001), "On the Dimensionality of Organizational Justice: A Construct Validation of a Measure," Journal of Applied Psychology, 86, 3, pp. 386-400.

Cook, K. S., and Rice, E. 2003. "Social Exchange Theory," in Handbook of Social Psychology, J. Delamater (ed.): New York: Kluwer.

Cook, K. S., and Rice, E. 2006. "Social Exchange Theory," in The Handbook of Soical Psychology, J. D. DeLamater (ed.): New York: Kluwer, pp. 53-76.

Cook, K. S., and Whitmeyer, J. M. 1992. "Two Approaches to Social Structure: Exchange Theory and Network Analysis," Annual Review of Sociology (18:1), pp 109-127.

Cropanzano, R., Prehar, C. A., and Chen, P. Y. (2002), "Using Social Exchange Theory to Distinguish Procedural from Interactional Justice," *Group & Organization Management,* 27, 3, pp. 324-351.

Culnan, M.J., and P.K. Armstrong (1999), "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science*, 10, pp. 104-115.

Culnan, M.J., and R.J. Bies (2003), "Consumer Privacy: Balancing Economic and Justice Considerations," Journal of Social Issues, 59, 2, pp. 323-342.

Culnan, M. J., and Williams, C. C. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches," MIS Quarterly (4:6), pp 673-687.

Culnan, M.J. (1995), "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing," *Journal of Direct Marketing*, 9, 2, pp. 10–19.

Daft, R.L., and R.H. Lengel (1986), "Organizational Information Requirements, Media Richness and Structural Design," Management Science, 32, 5, pp. 554-571.

Daft, R.L., R.H. Lengel, and L.K. Trevino (1987), "Message Equivocality, Media Selection, and Manager Performance: Implications for Information Systems," MIS Quarterly, 11, 3, pp. 355-366.

Dahl, D. W., Manchanda, R. V., and Argo, J. J. 2001. "Embarrassment in Consumer Purchase: The Roles of Social Presence and Purchase Familiarity," Journal of Consumer Research (28:3), pp 473-481.

Davis, F.D., R.P. Bagozzi, and P.R. Warshaw (1989), “User Acceptance of Computer Technology: A Comparison of Two Theoretical Models,” *Management Science*, 35, 8, pp. 982-1003.

Debatin, B., J.P. Lovejoy, A.-K. Horn, and B.N. Hughes (2009), "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," Journal of Computer-Mediated Communication, 15, 1, pp. 83-108.

DeMaris, A. 1991. "A Framework for the Interpretation of First-Order Interaction in Logit Modeling," Psychological BUlletin (110:3), pp 557-570.

Dennis, A.R., and S.T. Kinney (1998), "Testing Media Richness Theory in the New Media: The Effects of Cues, Feedback, and Task Equivocality," Information Systems Research, 9, 3, pp. 256-274.

Dennis, A.R., S.T. Kinney, and Y.-T.C. Hung (1999), "Gender Differences in the Effects of Media Richness," Small Group Research, 30, 4, pp. 405-437.

DeWitt, T., D.T. Nguyen, & R. Marshall (2008), “Exploring Customer Loyalty Following Service Recovery The Mediating Effects of Trust and Emotions,” *Journal of Service Research*, 10, 3, pp. 269-281.

Devaraj, S., F. Ming, and R. Kohli (2002), “Antecedents of B2C Channel Satisfaction and Preference: Validating e-Commerce Metrics,” *Information Systems Research*, 13, 3, pp. 316-333.

Dick, A.S., and K. Basu (1994), “Customer Loyalty: Toward an Integrated Conceptual Framework,” *Journal of the Academy of Marketing Science*, 22, 2, pp. 99-113.

Dinev, T., and P. Hart (2006), "An Extended Privacy Calculus Model for E-Commerce Transactions," Information Systems Research, 1, 17, pp. 61-80.

Drew, P. 1987. "Po-faced Receipts of Teases," Linguistics (25), pp 219-253.

Duckworth, A. L., Peterson, C., Matthews, M. D., and Kelly, D. R. 2007. "Grift: Perseverance and Passion for Long-Term Goals," Journal of Personality and Social Psychology (92:6), pp 1087-1101.

Eisenberger, R., P.M. Fasolo, and V. Davis-LaMastro (1990), "Perceived Organizational Support and Employee Diligence, Commitment, and Innovation," Journal of Applied Psychology, 75, 1, pp. 51-59.

Eisenberger, R., Armeli, S., Rexwinkel, B., Lynch, P. D., and Rhoades, L. 2001. "Reciprocation of Perceived Organizational Support," Journal of Applied Psychology (86:1), pp 42-51.

Ellison, N. B., Steinfield, C., and Lampe, C. 2007. "The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites," Journal of Computer Mediated Communication (12:4), pp 1143-1168.

Eldon, E. 2010. "Facebook Tests New "Subscribe To" Option for Friends and Pages."

Ellison, N. B., Steinfield, C., and Lampe, C. 2011. "Connection Strategies: Social Captial Implications of Facebook-Enabled Communication Practices," New Media & Society (13:6), pp 873-892.

Ellison, N. B., Steinfield, C., and Lampe, C. 2011. "Connection Strategies: Social Captial Implications of Facebook-Enabled Communication Practices," New Media & Society (13:6), pp 873-892.

Ellison, N.B., J.T. Hancock, and C.L. Toma (2011), "Profile as Promise: A Framework for Conceptualizing Veracity in Online ating Self-Presentations," New Media and Society, 13, 6, pp. 1-18.

Elson, R.J. and R. LeClerc (2006), "Customer Information: Protecting the Organization's Most Critical Asset from Misappropriation and Identity Theft," *Journal of Information Privacy & Security*, 2, 1, pp. 3-15.

Emerson, R. M. 1972a. "Exchange Theory, Part I: A Psychological Basis for Social Exchange," in Sociological Theories in Progress, J. Berger, M. Z. Jr. and B. Anderson (eds.): Boston: Houghton Mifflin, pp. 38-57.

Emerson, R. M. 1972b. "Exchange Theory, Part II: Exchange Relations and Network Structures," in Sociological Theories in Progress, J. Berger, M. Z. Jr. and B. Anderson (eds.): Boston: Houghton Mifflin, pp. 58-87.

Fan, Y., C Wu, and W. Wu (2010), "The Impacts of Online Retailing Service Recovery and Perceived Justice on Consumer Loyalty," *International Journal of Electronic Business Management*, 8, 3, pp. 239-249.

Federal Trade Commission (1986), "Truth in Lending Act, Amendments: Fair Credit Billing Act," Retrieved from http://www.ftc.gov/os/statutes/fcb/fcb.pdf

Federal Trade Commission (2006), "ChoicePoint Settles Data Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress," Retrieved from http://www.ftc.gov/opa/2006/01/choicepoint.shtm

Finn, J. (2004), "A Survey of Online Harassment of a University Campus," Journal of Interpersonal Violence, 19, 4, pp. 468-483.

Firestone, I. J. 1977. "Reconciling Verbal and Nonverbal Models of Dyadic Communication," Journal of Nonverbal Behavior (2:1), pp 30-44.

Floyd, J. and Parks, M.R. (1995), "Manifesting Closeness in the Interactions of Peers: A Look at Siblings and Friends," Communication Reports, 8, 2, pp. 69-76.

Folger, R. (1986), "Rethinking Equity Theory: A Referent Cognitions Model," In *Justice in Social Relations*, H.W. Bierhoff, R.L. Cohen, and J. Greenberg (Eds.), New York, NY: Plenum, pp. 145–162.

Folger, R., and Konovsky, M. A. (1989), "Effects of Procedural and Distributive Justice on Reactions to Pay Raise Decisions," *Academy of Management Journal*, 32, 1, pp. 115-130.

Forbes, L.P, S.W. Kelly, and K.D. Hoffman (2005), "Typologies of E-Commerce Retail Failures and Recovery Strategies," *Journal of Service Marketing*, 19, 5, pp. 280-292.

Fornell, C. and D.F. Larcker (1981), "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*, 18, 1, pp. 39-50.

Foster, E. K. 2004. "Research on Gossip: Taxonomy, Methods, and Future Directions," Review of General Psychology (8:2), pp 78-99.

Fox, J., Warber, K. M., and Makstaller, D. C. (forthcoming). The role of Facebook in romantic relationship development: An exploration of Knapp's relational stage model. Journal of Social and Personal Relationships.

Fusilier, M. R., and Hoyer, W. D. 1980. "Variables Affecting Perceptions of Invasion of Privacy in a Personnel Selection Situation," Journal of Applied Psychology (65:5), pp 623-626.

Gal-Or, E., and Ghose, A. (2005), "The Economic Incentives for Sharing Security Information," *Information Systems Research*, 16, 2, pp. 186-208.

Gefen, D. (2002). "Customer Loyalty in E-Commerce," *Journal of the Association for Information Systems*, 3, pp. 27-51.

Gefen, D., E. Karahanna, and D.W. Straub (2003), "Trust and TAM in Online Shopping: An Integrated Model," *MIS Quarterly*, 27, 1, pp. 51-90.

Gefen, D., and Ridings, C. M. 2002. "Implementation Team Responsivenss and User Evaluation of Cusomter Relationship Management: A Quasi-Experimental Design Study of Social Exchange Theory," Journal of Management Information Systems (19:1), pp 47-69.

Gefen, D., D. Straub, and M. Boudreau (2000), "Structural Equation Modeling and Regression: Guidelines for Research Practice," Communications of the Association for Information Systems, 4, 7, pp. 1-77.

Gibbs, J.L., N.B. Ellison, and R.D. Heino (2006), "Self-Presentation in Online Personals," Communication Research, 33, 2, pp. 152-177.

Gilbert, S.J., and D. Horenstein (1975), "The Communication of Self-Disclosure: Level Versus Valence," Human Communication Research, 1, 4, pp. 316-322.

Gilliland, S.W. (1993), "The Perceived Fairness of Selection Systems: An Organizational Justice Perspective," *Academy of Management Review*, 18, 4, pp. 694-734.

Gilliland, S.W., and B.A. Beckstein (1996), "Procedural and Distributive Justice in the Editorial Review Process," *Personnel Psychology*, 49, 3, pp. 669-691.

Gibbons, D., and Olk, P. M. 2003. "Individual and Structural Origins of Friendship and Social Position Among Professionals," Journal of Personality and Social Psychology (84:2), pp 340-351.

Goles, T., Lee, S., Rao, S. V., and Warren, J. (2009), "Trust Violation in Electronic Commerce: Customer Concerns and Reactions," *Journal of Computer Information Systems*, 49, 1, pp. 1-9.

Goodwin, C., and I. Ross (1992), "Consumer Responses to Service Failures: Influence of Procedural and Interactional Fairness Perceptions," *Journal of Business Research*, 25, 2, pp. 149-163.

Grace, D. 2009. "An Examination of Consumer Embarrassment and Repatronage Intentions in the Context of Emotional Service Encounters," Journal of Retailing and Consumer Services (16:1), pp 1-9.

Granovetter, M. 1973. "The Strength of Weak Ties," American Journal of Sociology (78:6), pp 1360-1380.

Greenberg, J. (1990), “Organizational Justice: Yesterday, Today, and Tomorrow,” *Journal of Management*, 16, 2, pp. 399-432.

Greenberg, J., and Eskew, D. E. 1993. "THe Role of Role Playing in Organizational Research," Journal of Management (19:2), pp 221-241.

Greenberg, C. I., and Firestone, I. J. 1977. "Compensatory Responses to Crowding: Effects of Personal Space Intrusion and Privacy Reduction," Journal of Personality and Social Psychology (35:9), pp 637-644.

Greenhow, C. and Robelia, B. (2009) “Old Communication, New Literacies: Social Network Sites as Social Learning Resources,” Journal of Computer-Mediated Communication, 14, 4, pp. 1130-1161.

Grégoire, Y., & Fisher, R. J. (2008), “Customer Betrayal and Retaliation: When Your Best Customers Become Your Worst Enemies,” *Journal of the Academy of Marketing Science*, 36, 2, pp. 247-261.

Grewal, D., A.L. Roggeveen, and M. Tsiros (2008), “The Effect of Compensation on Repurchase Intentions in Service Recovery,” *Journal of Retailing*, 84, 4, pp. 424-434.

Grosser, T. J., Lopez-Kidwell, V., & Labianca, G. (2010). A social network analysis of positive and negative gossip in organizational life. Group & Organization Management, 35(2), 177-212.

Gu,B. (2010), “The Impact of Online Service Recovery on Customer Satisfaction: Empirical Evidences from Service Operations,” *Americas Conference on Information Systems*, Lima, Peru, August 12-15.

Hancock, J.T., and P.J. Dunham (2001), "Impression Formation in Computer-Mediated Communication Revisited: An Analysis of the Breadth and Intensity of Impressions," Communication Research, 28, 3, pp. 325-347.

Hann, I.R., K.L. Hui, S.Y. Lee, and P.L. Png (2007), "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," Journal of Management Information Systems, 24, 2, pp. 13-42.

Harris, N. N., and Sutton, R. I. 1983. "Task Procrastination in Organizations: A Framework for Research," Human Relations (36:11), pp 987-995.

van der Heijden, H., T. Verhagen, and M. Creemers (2003), “Understanding Online Purchase Intentions: Contributions from Technology and Trust Perspectives,” *European Journal of Information Systems*, 12, 1, pp. 41-48.

Hemetsberger, A. (2002), "Fostering Cooperation on the Internet: Social Exchange Processes in Innovative Virtual Consumer Communities," Advances in Consumer Research, 29, 1, pp. 354-356.

Henning-Thurau, T., K.P. Gwinner, and D.D. Gremler (2002), “Understanding Relationship Marketing Outcomes: An Integration of Relational Benefits and Relationship Quality,” *Journal of Service Research*, 4, 3, pp. 230-247.

Higgins, E. T. 1998. "Promotion and Prevention: Regulatory Focus as a Motivational Principle," in Advances in Experimental Social Psychology, M. P. Zanna (ed.): San Diego, CA: Academic Press, pp. 1-46.

Hines, M. (2007), "TJX Stolen Data Used in Florida Crime Spree: Police Arrest Group Accused of Using Credit Card Info Stolen from TJX Customers; Losses Total More Than $8 Million," *InfoWorld*, March 21, Retrieved from http://www.infoworld.com/d/security-central/tjx-stolen-data-used-in-florida-crime-spree-118

Hoadley, C. M., Xu, H., Lee, J. J., and Rosson, M. B. 2010. "Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry," Electronic Commerce Research and Applications (9:1), pp 50-60.

Hoffman, K. D., and S.W. Kelley (2000), "Perceived Justice Needs and Recovery Evaluation: A Contingency Approach," *European Journal of Marketing*, 34, 34, pp. 418-433.

Holden, R.R. (1994), "Social Desirability," In: Encyclopedia of Psychology, R.J. Corsini (Ed.),New York: John Wiley, 429-430.

Holloway, B.B and S.E. Beatty (2003), "Service Failure in Online Retailing: A Recovery Opportunity," *Journal of Service Research*, 6, 1, pp. 92-105.

Holloway, B.B., S. Wang, and J.T. Parish (2005), "The Role of Cumulative Online Purchasing Experience in Service Recovery Management," *Journal of Interactive Marketing*, 19, 3, pp. 54-66.

Homans, G. C. (1964). Bringing men back in. American Sociological Review, 809-818.

Homans, C. G. 1961. Social Behavior: Its Elementary Forms, (New York: Harcourt, Brace & World.

Homans, G. C. 1958. "Social Behavior as Exchange," The American Journal of Sociology (63:6), pp 597-606.

Howard, L.W. (1999), "Validity Evidence for Measures of Procedural/Distributive Justice and Pay/Benefit Satisfaction," *Journal of Business and Psychology*, 14, 1, pp. 135-147.

Hu, L.-T., and P.M. Bentler (1999), "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives," Structural Equation Modeling, 6, 1, pp. 1-55.

Hui, K.L., H.H. Teo, and L.S.Y. T (2007), "The Value of Privacy Assurance: An Exploratory Field Experiment," MIS Quarterly, 31 1, pp. 19-33.

Humphrey, S.E., A.P.J. Ellis, D.E. Conlon, and C.H. Tinsley (2004) "Understanding Customer Reactions to Brokered Ultimatums: Applying Negotiation and Justice Theory," *Journal of Applied Psychology*, 89, 3, pp. 466-482

IDA (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

IDA (2012) "Infocomm Usage – Households and Individuals." Retrieved from http://www.ida.gov.sg/Infocomm-Landscape/Facts-and-Figures/Infocomm-Usage-Households-and-Individuals#4

Identity Theft Resource Center (2009) "Data Breach," Retrieved from http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml

Jarvenpaa, S.L., and N. Tractinsky (1999), "Consumer Trust in an Internet Store: A Cross-Cultural Validation," *Journal of Computer-Mediated Communication* [Online Serial], 5, 2, Retrieved from http://www.ascusc.org/jcmc/vol5/issue2/jarvenpaa.html

Jewell, M. (2007), "TJX, Visa Reach $40.9M Settlement for Data Breach," Retrieved from http://www.usatoday.com/money/industries/retail/2007-11-30-tjx-visa-breach-settlement_N.htm

Ji, P., and P.S. Lieber (2010), "Am I Safe? Exploring Relationships between Primary Territories and Online Privacy " Journal of Internet Commerce, 9, 1, pp. 3-22.

Jiang, L.C., N.N. Bazarova, and J.T. Hancock (2010), "The Disclosure-Intimacy Link in Computer-Mediated Communication: An Attributional Extension of the Hyperpersonal Model," Human Communication Research, 37, 1, pp. 58-77.

Joinson, A.N., A. Woodley, and U.-R. Reips (2007), "Personalization, Authentication and Self-Disclosure in Self-Administered Internet Surveys," Computers in Human Behavior, 23, 1, pp. 275-285.

Joinson, N.A. (2001), "Self-Disclosure in Computer-Mediated Communication: The Role of Self-Awareness and Visual Anonymity," European Journal of Social Psychology, 31, 2, pp. 177-192.

Jones, M.A., D.L. Mothersbaugh, and S.E. Beatty (2002), "Why Customers Stay: Measuring the Underlying Dimensions of Services Switching Costs and Managing Their Differential Strategic Outcomes," *Journal of Business Research*, 55, pp. 441-450.

Jones, D. C., Newman, J. B., and Bautista, S. 2005. "A Three-factor Model of Teasing: The Influence of Friendship, Gender, and Topic on Expected Emotional Reactions to Teasing during Early Adolescence," Social Development (14:3), pp 421-439.

Jones, T.O., and W.E. Sasser, Jr. (1995), "Why Satisfied Customers Defect," *Harvard Business Review*, November-December, pp. 88-99.

Jöreskog, K. (1998), "Interaction and Nonlinear Modeling: Issues and Approaches," in *Interaction and Nonlinear Effects in Structural Equation Modeling*, R.E. Schumacker and G.A. Marcoulides (eds.), Mahwah, NJ: Lawrence Erlbaum Associates, Inc., pp. 239-250.

Jöreskog, K., and D. Sörbom (1996), *LISREL8: User's Reference Guide*, Chicago, IL: Scientific Software International.

Kamis, A., M. Koufaris, & T. Stern (2008), "Using an Attribute-based Decision Support System for User-customized Products Online: An Experimental Investigation," *MIS Quarterly*, 32, 1, pp. 159-177.

Kau, A. K., & E.W.Y. Loh (2006), "The Effects of Service Recovery on Consumer Satisfaction: A Comparison between Complainants and Non-complainants," *Journal of Services Marketing*, 20, 2, pp. 101-111.

Keltner, D., Capps, L., Kring, A. M., Young, R. C., and Heerey, E. A. 2001. "Just Teasing: A Conceptual Analysis and Empirical Review," Psychological Bulletin (127:2), pp 229-248.

Keltner, D., Young, R. C., Heerey, E. A., Oemig, C., and Monarch, N. D. 1998. "Teasing in Hierarchical and Intimate Relations," Journal of Personality and Social Psychology (75:5), pp 1231-1247.

Kerber, R. (2007), "Cost of Data Breach at TJX Soars to $256M Suits, Computer Fix Add to Expenses," *The Boston Globe*, Aug. 15. Retrieved from http://www.boston.com/business/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/

Kim, S.S. (2009), "The Integrative Framework of Technology Use: An Extension and Test," *MIS Quarterly*, 33, 3, pp. 513-537.

Kim, J. K., Y. H. Cho, W. J. Kim, J. R. Kim, and J. Y. Suh (2002), "A Personalized Recommendation Procedure for Internet Shopping Support," *Electronic Commerce Research and Applications*, 1, 3, pp. 301-313.

Kim, S.S., and N.K. Malhotra (2005), "A Longitudinal Model of Continued IS Use: An Integrative View of Four Mechanisms Underlying Postadoption Phenomena," *Management Science,* 51, 5, pp. 741-755.

Kim, S.S., N.K. Malhotra, and S. Narasimhan (2005), "Two Competing Perspectives on Automatic Use: A Theoretical and Empirical Comparison," *Information Systems Research*, 16, 4, pp. 418-432.

Kim, S.S., and J. Son. (2009), "Out of Dedication or Constraint? A Dual Model of Post-adoption Phenomena and Its Empirical Test in the Context of Online Services," *MIS Quarterly*, 33, 1, pp. 49-70.

Kim, K.-H., and H. Yun (2007), "Crying for Me, Crying for Us: Relational Dialectics in A Korean Social Network Site," Journal of Computer-Mediated Communication, 13, 1, pp. 298-318.

Kingshott, R. P., and Pecotich, A. (2007), "The Impact of Psychological Contracts on Trust and Commitment in Supplier-Distributor Relationships," *European Journal of Marketing*, 41, 9/10, pp. 1053-1072.

Kjaerland, M. (2006), "A Taxonomy and Comparison of Computer Security Incidents from the Commercial and Government Sectors," *Computers & Security*, 25, 7, pp. 522-538.

Koh, C., Ang, S., and Straub, D. W. (2004), "IT Outsourcing Success: A Psychological Contract Perspective," *Information Systems Research*, 15, 4, pp. 356-373.

Kotthoff, H. 2003. "Responding to Irony in Different Contexts: on Cognition in Conversation," Journal of Pragmatics (35:9), pp 1387-1411.

Koufaris, M. (2002), "Applying the Technology Acceptance Model and Flow Theory to Online Consumer Behavior," *Information Systems Research*, 13, 2, pp. 205-223.

Kruger, J., Gordon, C. L., and Kuban, J. 2006. "Intentions in Teasing: When "Just Kidding" Just Isn't Good Enough," Journal of Personality and Social Psychology (90:3), pp 412-425.

Kuhl, J. 1981. "Motivational and Functional Helplessness: The Moderating Effect of State versus Action Orientation " Journal of Personality and Social Psychology (40:1), pp 155-170.

Lampert, M. D., and Ervin-Tripp, S. M. 2006. "Risky Laughter: Teasing and Self-Directed Joking Among Male and Female Friends," Journal of Pragmatics (38:1), pp 51-72.

Lance, C.E. (1988), "Residual Centering, Exploratory and Confirmatory Moderator Analysis, and Decomposition of Effects in Path Models Containing Interactions," *Applied Psychological Measurement*, 12, 2, pp. 163-175.

Lange, P. G. 2007. "Publicly Private and Privately Public: Social Networking on YouTube," Journal of Computer Mediated Communication (13:1), pp 361-380.

Lang, T.A., and M. Secic (2006), *How to Report Statistics in Medicine*, 2nd ed. Philadelphia, PA: American College of Physicians.

Laufer, R.S., and M. Wolfe (1977) "Privacy as a Concept and a Social Issue: A Multidimensional Development Theory," *Journal of Social Issues*, 33, 3, pp. 22-42.

Lawler, E.J., and S.R. Thye (1999), "Bringing Emotions into Social Exchange Theory," Annual Review of Sociology, 25, pp. 217-244.

Le Poire, B.A., J.K. Burgoon, and R. Parrott (1992), "Status and Privacy Restoring Communication in the Workplace," Journal of Applied Communication Research, 20, 4, pp. 419-436.

Lee, C., K.S. Law, and P. Bobko (1999), "The Importance of Justice Perceptions on Pay Effectiveness: A Two-Year Study of a Skill-Based Pay Plan," *Journal of Management*, 25, 6, pp. 851-873.

Lea, M., R. Spears, and D. Groot (2001), "Knowing Me, Knowing You: Anonymity Effects on Social Identity Processes within Groups," Personality and Social Psychology Bulletin, 27, 5, pp. 526-537.

Lenhart, A., and Madden, M. 2007. "Teens, Privacy & Online Social Networks."

Lerner, J. S., and Keltner, D. (2000), "Beyond Valence: Toward a Model of Emotion-Specific Influences on Judgment and Choice," *Cognition & Emotion,* 14, 4, pp. 473-493.

Lewicki, R.J., and B.B. Bunker (1996), "Developing and Maintaining Trust in Work Relationships," in *Trust in Organizations: Frontiers of Theory and Research*, R.M. Kramer and T.R. Tyler (eds), Thousand Oaks, CA: SAGE, pp. 114-139.

Lewis, K., Kaufman, J., and Christakis, N. 2008. "The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network," Journal of Computer-Mediated Communication (14:1), pp 79-100.

Li, H., R. Sarathy, and H. Xu (2011), "The Role of Affect and Cognition on Online Consumers' Decision to Disclose Personal Information to Unfamiliar Online Vendors," *Decision Support Systems*, 51, 3, pp. 434-445.

Liao, H. (2007), "Do It Right This Time: The Role of Employee Service Recovery Performance in Customer-perceived Justice and Customer

Loyalty After Service Failures," *Journal of Applied Psychology*, 92, 2, pp. 475-489.

Lin, H. H., Wang, Y. S., & Chang, L. K. (2011), "Consumer Responses to Online Retailer's Service Recovery After a Service Failure: A Perspective of Justice Theory," *Managing Service Quality*, 21, 5, pp. 511-534.

Lindell, M.K., and D.J. Whitney (2001), "Accounting for Common Method Variance in Cross-Sectional Research Designs," *Journal of Applied Psychology*, 86, 1, pp. 114-121.

Lipkus, I. M., and Bissonnette, V. L. 1996. "Relationships among Belief in a Just World, Willingness to Accommodate, and Martial Well-Being," Personality and Social Psychology Bulletin (22:10), pp 1043-1056.

Long, J. S. 2000. Regression Models for Categorical and Limited Dependent Variables, (Thousand Oaks, CA, US: Sage Publications, Inc.

Luo, Y. (2007), "The Independent and Interactive Roles of Procedural, Distributive and Interactional Justice in Strategic Alliances," *Academy of Management Journal*, 50, 3, pp. 644-664.

Madden, M., S. Fox, A. Smith, and J. Vitak (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

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

Madden, M., and Zickuhr, K. 2011. "65% of Online Adults Use Social Networking Sites."

Malhotra, N.K. (2004), *Marketing Research: An Applied Orientation*, 4th ed. Upper Saddle River, NJ: Prentice Hall.

Malhotra, N.K., S.S. Kim, and A. Patil (2006), "Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research," *Management Science*, 52, 12, pp. 1865-1883.

Malhotra, N.K., S.S. Kim, and J. Agarwal (2004), "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and A Causal Model," Information System Research, 15, 4, pp. 336-355.

Markovsky, B. (1988), "Injustice and Arousal," *Social Justice Research*, 2, pp. 223-233.

Marsh, A. A., Ambady, N., and Kleck, R. E. 2005. "The Effects of Fear and Anger Facial Expression on Approach- and Avoidance-Related Behaviors," Emotion (5:1), pp 119-124.

Martínez-Tur, V., J.M. Peiró, J. Ramos., and C. Moliner (2006), "Justice Perceptions as Predictors of Customer Satisfaction: The Impact of Distributive, Procedural and Interactional Justice," *Journal of Applied Social Psychology*; 36, 1, pp. 100-119.

Maslach, C., Stapp, J., and Santee, R. T. 1985. "Individuation: Conceptual Analysis and Assessment," Journal of Personality and Social Psychology (49:3), pp 729-738.

Mathwick, C., N.K. Malhotra, and E. Rigdon (2001), "Experiential Value: Conceptualization, Measurement and Application in the Catalog and Internet Shopping Environment," *Journal of Retailing*, 77, 1, pp. 39-56.

Mavridis, N., Kazmi, W., and Toulis, P. 2010. Friends with Faces: How Social Networks Can Enhance Face Recognition and Vice Versa, (Springer: London.

Maxham III, J. G. (2001), "Service Recovery's Influence on Consumer Satisfaction, Positive Word-of-mouth, and Purchase Intentions," *Journal of Business Research*, 54, 1, pp. 11-24.

Maxham III, J. G., and Netemeyer, R. G. (2002), "Modeling Customer Perceptions of Complaint Handling Over Time: The Effects of Perceived Justice on Satisfaction and Intent," *Journal of Retailing*, 78, 4, pp. 239-252.

McLeod, P. (2011), "Effects of Anonymity and Social Comparison of Rewards on Computer Mediated Group Brainstorming Small Group Research, 42, pp. 475-503.

McGrath, J.E., and A.B. Hollingshead (1993), "Putting the "Group" Back in Group Support Systems: Some Theoretical Issues about Dynamic Processes in Groups with Technological Enhancements," In: Group Support Systems: New Perspectives, L.M. Jessup and J.S. Valacich (Eds.),New York, NY: Macmillan, pp. 78-96.

McKnight, D.H., V. Choudhury, and C. Kacmar (2002), "Developing and Validating Trust Measures for E-Commerce: An Integrative Topology," *Information Systems Research*, 13, 3, pp. 334-359.

McLaughlin, C., and Vitak, J. 2011. "Norm Evolution and Violation on Facebook," New Media & Society) September 26, 2011.

Meuter, M.L., A.L. Ostrom, R.L. Roundtree, and M.J. Bitner (2000), "Self-Service Technologies: Understanding Customer Satisfaction with Technology-based Service Encounters," *Journal of Marketing*, 64, 3, pp. 50-65.

Milne, G.R., and M.E. Gordon (1993), "Direct Mail Privacy-Efficiency Trade-offs Within an Implied Social Contract Framework," Journal of Public Policy and Marketing, 12, 2, pp. 206-215.

Molm, L. D. 1990. "Structure, Action, and Outcomes: The Dynamics of Power in Social Exchange," American Sociological Review (55:3), pp 427-447.

Molm, L.D., Peterson, G. and Takahashi, N. (2003) "In the Eye of the Beholder: Procedural Justice in Social Exchange," American Sociological Review, 68, 1, pp. 128-152.

Milne, G.R. and A.J. Rohm (2000), "Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives," *Journal of Public Policy & Marketing*, 19, 2, pp. 238-249.

Mithas, S., D. Almirall, and M.S. Krishnan (2006), "Do CRM Systems Cause One-to-one Marketing Effectiveness?" *Statistical Science*, 21, 2, pp. 223-233.

Molm, L. D., Takahashi, N., and Peterson, G. 2000. "Risk and Trust in Social Exchange: An Experimental Test of a Classical Proposition," American Journal of Sociology (105:5), pp 1396-1427.

Montada, L. (1994), "Injustice in Harm and Loss," *Social Justice Research*, 7, pp. 5-28.

Moorman, R.H. (1991), "Relationship between Organizational Justice and Organizational Citizenship Behaviors: Do Fairness Perceptions Influence Employee Citizenship?" *Journal of Applied Psychology*, 76, 6, pp. 845-855.

Moral-Toranzo, F., J. Canto-Ortiz, and L. Gómez-Jacinto (2007), "Anonymity Effects in Computer-Mediated Communication in the Case of Minority Influence," Computers in Human Behavior, 23, 3, pp. 1660-1674.

Morgan, R.M., and S.D. Hunt (1994), "The Commitment-Trust Theory of Relationship Marketing," *Journal of Marketing*, 58, 3, pp. 20-38.

Murray, S. L., Holmes, J. G., and Griffin, D. W. 1996. "The Self-Fulfilling Nature of Positive Illusions in Romantic Relationships: Love is Not Blind, but Prescient," Journal of Personality and Social Psychology (71:6), pp 1155-1180.

Morrison, E.W. and S.L. Robinson (1997), "When Employees Feel Betrayed: A Model of How Psychological Contract Violation Develops," *Academy of Management Review*, 22, 1, pp. 226-256.

Murray, K.B., and J.L. Schlacter (1990), "The Impact of Services Versus Goods on Consumers' Assessment of Perceived Risk and Variability," *Journal of the Academy of Marketing Science*, 18, 1, pp. 51-65.

Nichols, D.S., and R.L. Greene (1997), "Dimensions of Deception in Personality Assessment: The Example of MMPI-2," Journal of Personality Assessment, 68, 2, pp. 251-266.

Nowak, G.J., and J. Phelps (1992), "Understanding Privacy Concerns: An Assessment of Consumers' Information-Related Knowledge and Beliefs," *Journal of Direct Marketing*, 6, 4, pp. 28-39.

Ofcom (2011), "Ofcom Technology Tracker," Retrieved from http://www.ofcom.org.uk/static/marketdataresearch/statistics/main_set.pdf

Office of the Privacy Commissioner of Canada (2007) "Key Steps for Organizations in Responding to Privacy Breaches," Retrieved from http://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.pdf

O'Guinn, T.C., and R.J. Faber (1989), "Compulsive Buying: A Phenomenological Exploration," *Journal of Consumer Research*, 16, 2, pp. 147-157.

Oliver, R.L. (1999), "Whence Consumer Loyalty?" *Journal of Marketing*, 63, Special Issue, pp. 33-44.

Ortony, A., G.L. Clore, & A. Collins (1988), "The Cognitive Structure of Emotions," New York: Cambridge University Press.

Parasuraman, A., V.A. Zeithaml, and A. Malhotra (2005), "E-S-QUAL: A Multiple-item Scale for Assessing Electronic Service Quality," *Journal of Service Research*, 7, 3, pp. 213-233.

Parzefall, M.-R., and Salin, D. M. 2010. "Perceptions of and reactions to Workplace Bullying: A Social Exchange Perspective," Human Relations (63:6), pp 761-780.

Pavlou, P. A. 2011. "State of the Information Privacy Literature: Where Are We Now and Where Should We Go?," MIS Quarterly (35:4), pp 977-988.

Pavlou, P.A., and D. Gefen (2004), "Building Effective Online Marketplaces with Institution-Based Trust," Information Systems Research, 15, 1, pp. 37-59.

Pavlou, P.A., and D. Gefen (2005), "Psychological Contract Violation in Online Marketplaces: Antecedents, Consequences, and Moderating Role," *Information Systems Research*, 16, 4, pp. 272-299.

Peng, C.-Y. J., Lee, K. L., and Ingersoll, G. M. 2002. "An Introduction to Logistic Regression Analysis and Reporting," Journal of Educational Research (96:1), pp 3-14.

Peng, C.-Y. K., and So, T.-K. H. 2002. "Logistic Regression Analysis and Reporting: A Primer," Understanding Statistics (1:1), pp 31-70.

Peris, R., M.A. Gimeno, D. Pinazo, G. Ortet, V. Carrero, M. Sanchiz, and I. Ibanez (2002), "Online Chat Rooms: Virtual Spaces of Interaction for Socially Oriented People," CyberPsychology & Behavior, 5, 1, pp. 43-51.

Perreault, S., and R.Y. Bourhi (1999), "Ethnocentrism, Social Identification, and Discrimination," Personality and Social Psychology Bulletin, 25, 1, pp. 92-103.

Petronio, S. (1991), "Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples," Communication Theory, 1, 4, pp. 311-335.

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

Petronio, S., Olson, C., and Dollar, N. 1989. "Privacy Issues in Relational Embarrassment: Impact on Relational Quality and Communication Satisfaction " Communication Research Reports (6:1), pp 21-27.

PEW Internet & American Life Project (2009) "Generations Online in 2009," Retrieved from http://www.pewinternet.org/Reports/2009/Generations-Online-in-2009.aspx

PEW Internet & American Life Project (2013) "Internet User Demographics," Retrieved from http://www.pewinternet.org/data-trend/internet-use/latest-stats/

Pinsonneault, A., and N. Heppel (1997), "Anonymity in Group Support Systems Research: A New Conceptualization, Measure, and Contingency Framework," Journal of Management Information Systems, 14, 3, pp. 89-108.

Poddar, A., J. Mosteller, and P.S. Ellen. (2009), "Consumers' Rules of Engagement in Online Information Exchanges," *Journal of Consumer Affairs*, 43, 3, pp. 419-448.

Podsakoff, P., S. MacKenzie, J. Lee, and N. Podsakoff (2003), "Common Method Biases in Behavioral Research: A Critical review of the Literature and Recommended Remedies," Journal of Applied Psychology, 88, 5, pp. 879-903.

Ponemon (2009) "Fourth Annual US Cost of Data Breach Study," Retrieved from http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf

Postmes, T., and R. Spears (1998), "Deindividuation and Antinormative Behavior : A Meta-Analysis," Psychological Bulletin 123, 3, pp. 238-259.

Preston, J. (2004), "Judge Strikes Down Section of Patriot Act Allowing Secret Subpoenas of Internet Data," *New York Times*, September 30.

Price, J.L., and C.W. Mueller (1986), *Handbook of Organizational Measurement*, Marshfield, MA: Pittman.

Privacy Rights Clearing House (2013),, "Face Sheet 17b: How to Deal with a Security Breach," Retrieved from https://www.privacyrights.org/fs/fs17b-SecurityBreach.htm#FigureOutWhat

Rahim, M.A., N.R. Magner, and D.L. Shapiro (2000), "Do Justice Perceptions Influence Styles of Handling Conflict with Supervisors? What Justice Perceptions, Precisely?" *International Journal of Conflict Management*, 11, 1, pp. 9-31.

Ratan, R.A., J.E. Chung, C. Shen, D. Williams, and M.S. Poole (2010), "Schmoozing and Smiting: Trust, Social Institutions, and Communication Patterns in an MMOG," Journal of Computer-Mediated Communication, 16, 1, pp. 93-114.

Ray, S., S.S. Kim, and J.G. Morris (2011), "Online Users' Switching Costs: Their Nature and Formation," *Information Systems Research*, forthcoming.

Raynes-Goldie, K. 2010. "Aliases, Creeping, and Wall Cleaning: Understanding Privacy in the Age of Facebook," First Monday (15:1).

Reichheld, F.F. (2003), "The One Number You Need to Grow," *Harvard Business Review*, December, pp. 46-54.

Reichheld, F.F., and P. Schefter (2000), "E-Loyalty: Your Secret Weapon on the Web," *Harvard Business Review*, July-August, pp. 105-113.

Reichheld, F.F., and W. E. Sasser (1990), "**Zero Defections: Quality Comes to Services," *Harvard Business Review*, 68, 5, pp. 105-111.**

Rempel, J. K., Holmes, J. G., and Zanna, M. P. 1985. "Trust in Close Relationships," Journal of Personality and Social Psychology (49:1), pp 95-112.

Rindfleisch, T. C. 1997, "Privacy, Information Technology, and Health Care," *Communications of the ACM*, 40, 8, pp. 92-100.

Roberson, Q. M., and Colquitt, J. A. 2005. "Shared and Configural Justice: A Social Network Model of Justice in Teams," Academy of Management Review (30:3), pp 595-607.

Robinson, S.L., and E.W. Morrison (2000), "The Development of Psychological Contract Breach and Violation: a Longitudinal Study," *Journal of Organizational Behavior*, 21, pp. 525-546.

Rousseau, D.M. (1989), "Psychological and Implied Contracts in Organizations," *Employee Responsibilities and Rights Journal*, 2, 2, pp. 121-139.

Rusbult, C. E., and Buunk, B. P. 1993. "Commitment Processes in Close Relationships: An Interdependence Analysis," Journal of Social and Personal Relationships (10:2), pp 175-204.

Rusbult, C. E., Farrell, D., Rogers, G., and Mainous Iii, A. G. 1988. "Impact of Exchange Variables on Exit, Voice, Loyalty, and Neglect: An Integrative Model of Responses to Delining Job Satisfaction," Academy of Management Journal (31:3), pp 599-627.

Rusbult, C. E., and Martz, J. M. 1995. "Remaining in an Abusive Relationship: An Investment Model Analysis of Nonvoluntary Dependence," Personality and Social Psychology Bulletin (21:6), pp 558-571.

Ruth, J.A., F.F. Brunel, and C.C. Otnes (2002), "Linking Thoughts to Feelings: Investigating Cognitive Appraisals and Consumption Emotions in a Mixed-Emotions Context," *Academy of Marketing Science*, 30, 1, pp. 44-58.

Sabini, J., Garvey, B., and Hall, A. L. 2001. "Shame and Embarrassment Revisited," Personality and Social Psychology Bulletin (27:1), pp 104-117.

Schimel, J., J. Arndt, T. Pyszczynski, and J. Greenberg (2001), "Being Accepted for Who We are: Evidence That Social Validation of The Intrinsic Self Reduces General Defensiveness," Journal of Personality and Social Psychology, 80, 1, pp. 35-52.

Schmidt, T.A., M.B. Houston, L.A. Bettencourt, and P.D. Boughton (2003), "The Impact of Voice and Justification on Students' Perceptions of Professors' Fairness," *Journal of Marketing Education*, 25, 2, pp. 177-186.

Schoefer, K., and C. Ennew (2005), "The Impact of Perceived Justice on Consumers' Emotional Responses to Service Complaint Experiences," *The Journal of Service Marketing*, 19, 5, pp. 261-270.

Schoenbachler, D.D., and G.L. Gordon (2002), "Multi-Channel Shopping: Understanding What Drives Channel Choice," Journal of Consumer Marketing, 19, 1, pp. 42-53.

Schuman, E. (2007), "TJX Settles Lawsuits, Offers Discount Days," Retrieved from http://www.eweek.com/c/a/Security/TJX-Settles-Lawsuits-Offers-Discount-Days/

Sheehan, K. B., and Hoy, M. G. 2000. "Dimensions of Privacy Concern Among Online Consumers," Journal of Public Policy & Marketing (19:1).

Sheer, V.C. (2011), "Teenagers' Use of MSN Features, Discussion Topics, and Online Friendship Development: The Impact of Media Richness and Communication Control," Communication Quarterly, 59, 1, pp. 82-103.

Sias, P. M., and Perry, T. 2004. "Disengaging from Workplace Relationships," Human Communication Research (30:4), pp 589-602.

Skarlicki, D.P., R, Folger, and P. Tesluk (1999), "Personality as a Moderator in the Relationship between Fairness and Retaliation," *Academy of Management Journal*, 42, 1, pp. 100-108.

Smith, A. K., and R. N. Bolton (2002), "The Effect of Customers' Emotional Responses to Service Failures on their Recovery Effort Evaluations and Satisfaction Judgments," *Journal of the Academy of Marketing Science*, 30, 1, pp. 5-23.

Smith, A. K., R.N. Bolton, and J. Wagner (1999), "A Model of Customer Satisfaction with Service Encounters Involving Failure and Recovery," *Journal of Marketing Research*, 36, 3, pp. 356-372.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," MIS Quarterly (35:4), pp 989-1015.

Smith, H.J., S.J. Milberg, and S.J. Burke (1996), "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," MIS Quarterly 20, 2, pp. 167-196.

Sobel, M.E. (1982), "Asymptotic confidence intervals for indirect effects in structrual equations models," In: Sociological Methodology, S. Leinhart (Ed.),San Franciso, CA, Jossey-Bass, pp. 290-312.

Soderlund, M. (2002) "Customer Familiarity and Its Effects on Satisfaction and Behavioral Intentions," *Psychology and Marketing*, 19, 10, pp. 861-880

Soh, D. (2014) "Coping with Information in Social Media: The Effects of Network Structure and Knowledge on Perception of Information Value", Computers in Human Behavior.

Solove, D. J. 2006. "A Taxonomy of Privacy," University of Pennsylvania Law Review (154:3), pp 477-564.

Son, J.-Y., and S.S. Kim (2008), "Internet Users' Information Privacy-Protective Responses: A Taxonomy and A Nomological Model," MIS Quarterly, 32, 3, pp. 503-529.

Son, J., S. S. Kim, and F. Riggins (2006), "Consumer Adoption of Net-Enabled Infomediaries: Theoretical Explanations and an Empirical Test," *Journal of the Association for Information Systems*, 7, 7, pp. 473-508.

Srinivasan, S.S., R. Anderson, and K. Ponnavolu (2002), "Customer Loyalty in E-Commerce: An Exploration of Its Antecedents and Consequences," *Journal of Retailing*, 78, pp. 41-50.

Stewart, K.A., and A.H. Segars (2002), "An Empirical Examination of the Concern for Information Privacy Instrument," Information Systems Research, 13, 1, pp. 36-49.

Stevens, G. (2010) Federal Information Security and Data Breach Notification Laws, Library of Congress Washington DC, Congressional Research Service. Retrieved from http://www.fas.org/sgp/crs/secrecy/RL34120.pdf

Sun, T., S. Youn, G. Wu, M. Kuntaraporn (2006), "Online Word-of-Mouth (or Mouse): An Exploration of Its Antecedents and Consequences," *Journal of Computer-Mediated Communication*, 11, 4, Retrieved from http://jcmc.indiana.edu/vol11/issue4/sun.html

Tang, Z., Y. Hu, and M.D. Smith (2008), "Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor," *Journal of Management Information Systems*, 24, 4, pp. 153-174.

Tax, S.S., S.W. Brown, and M. Chandrashekaran (1998), "Customer Evaluations of Service Complaint Experiences: Implications for Relationship Marketing," *Journal of Marketing*, 62, 2, pp. 60-76.

Taylor, D.G., D.F. Davis, and R. Jillapalli (2009), "Privacy Concern and Online Personalization: The Moderating Effects of Information Control and Compensation," *Electronic Commerce Research*, 9, 3, pp. 203-223.

Taylor, S.A. and G.L. Hunter (2002), "The Impact of Loyalty with eCRM Software and eServices," *The International Journal of Service Industry Management Special Issue - Research on eService*, 13, 5, pp. 452-472.

Tedeschi, J. T. 2001. "Social Power and Aggression," in Social Influence: Direct and Indirect Processes, J. P. Forgas and K. D. Williams (eds.): New York: Psychology, pp. 109-126.

Tekleab, A.G., R. Takeuchi, and M.S. Taylor (2005), "Extending the Chain of Relationships among Organizational Justice, Social Exchange, and Employee Reactions: The Role of Contract Violations," *Academy of Management Journal*, 48, 1, pp. 146-157.

Terrion, J. L., and Ashforth, B. E. 2002. "From `I' to `We': The Role of Putdown Humor and Identity in the Development of a Temporary Group," Human Relations (55:1), pp 55-88.

Thibaut, J., and L. Walker (1975), *Procedural Justice: A Psychological Analysis*, Hillsdale, NJ: Erlbaum.

Tidwell, L. C., and 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), pp 317-348.

Ting-Toomey, S., and Oetzel, J. G. 2001. Managing Intercultural Conflict Effectively, (Thousand Oaks, CA: Sage.

Tolchinsky, P. D., McCuddy, M. K., Adams, J., Ganster, D. C., Woodman, R. W., and Fromkin, H. L. 1981. "Employee Perceptions of Invasion of Privacy: A Field Simulation Experiment," Journal of Applied Psychology (66:3), pp 308-313.

Toma, C.L., and J.T. Hancock (2010), "Looks and Lies: The Role of Physical Attractiveness in Online Dating Self-Presentation and Deception," Communication Research, 37, 3, pp. 335-351.

Tragesser, S. L., and Lippman, L. G. 2005. "Teasing: For Superiority or Solidarity?," Journal of General PSychology (132:2), pp 255-266.

Tucker, L.R., and C. Lewis (1973), "Reliability Coefficient for Maximum Likelihood Factor Analysis," Psychometrika, 38, 1, pp. 1-10.

Turner, M. M., Mazur, M. A., Wendel, N., and Winslow, R. 2003. "Relaitonal Ruin or Social Glue? The Joint Effect of Relationship and Gossip Valence on Liking, Trust, and Expertise," Communication Monographs (70:2), pp 129-141.

Vandebosch, H., and K. Van Cleemput (2009), "Cyberbullying Among Youngsters: Profiles of Bullies and Victims," New Media & Society, 11, 8, pp. 1349-1371.

Vandenberg, R. J., and Grelle, D. M. (2009), "Alternative Model Specifications in Structural Equation Modeling," *Statistical and Methodological Myths and Urban Legends,* pp. 165-191.

van der Heijden, H. (2003), "Factors Influencing the Usage of Websites: The Case of a Generic Portal in the Netherlands," *Information and Management,* 40, 6, pp. 541-549.

Verhoef, P.C. (2003), "Understanding the Effect of Customer Relationship Management Efforts on Customer Retention and Customer Share Development," Journal of Marketing, 67, 4, pp. 30-45.

Viégas, F.B. (2005), "Bloggers' Expectations of Privacy and Accountability: An Initial Survey," Journal of Computer-Mediated Communication, 10, 3.

Walther, J.B. (1996), "Computer-Mediated Communication: Impersonal, Interprsonal, and Hyperpersonal Interaction," Communication Research, 23, 1, pp. 3-43.

Walther, J.B. (2007), "Selective Self-Presentation in Computer-Mediated Communication: Hyperpersonal Dimensions of Technology, Language, and Cognition," Computers in Human Behavior, 23, 5, pp. 2538-2557.

Wang, S. and L. Huff (2007), "Explaining a Buyer's Response to a Seller's Violation of Trust," *European Journal of Marketing*, 41, 9-10, pp. 1033-1052.

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., and Cranor, L. F. 2011. ""I regretted the minute I pressed share": a qualitative study of regrets on Facebook," in Proceedings of the Seventh Symposium on Usable Privacy and Security, ACM: Pittsburgh, Pennsylvania.

Weiss, A.M. and J.B. Heide (1993), "The Nature of Organizational Search in High Technology Markets," *Journal of Marketing Research*, 30, 2, pp. 220-233.

Weiss, H. M., and Cropanzano, R. (1996), "An Affective Events Approach to Job Satisfaction," In B. M. Staw and L. L. Cummings (Eds.), *Research in Organizational Behavior*, 18, pp. 1-74. Greenwich, CT: JAI Press.

Weiss, H. M., K. Suckow, and R. Cropanzano (1999), "Effects of Justice Conditions on Discrete Emotions," *Journal of Applied Psychology*, 8, pp. 786-794.

Wellman, B., and Wortley, S. 1990. "Different Strokes from Different Folks: Community Ties and Social Support," American Journal of Sociology (96:3), pp 558-588.

Wheeless, L.R., and J. Grotz (1976), "Self-Disclosure and Interpersonal Solidarity: Measurement, Validation, and Relationships," Human Communication Research, 3, 1, pp. 47-61.

Whitman, M. E., and H. J. Mattord (2009), "Principles of Information Security," 3rd ed., Florence, KY: Course Technology.

Wilson, D. T. 1995. "An integrated model of buyer-seller relationships," Journal of the Academy of Marketing Science (23:4), pp 335-345.

Wirtz, J., and M.O. Lwin (2009), "Regulatory Focus Theory, Trust, and Privacy Concern," *Journal of Service Research*, 12, 2, pp. 190-207.

Wolak, J.J.D., K.J. Mitchell, and D. Finkelhor (2007), "Does Online Harassment Constitute Bullying? An Exploration of Online Harassment by Known Peers and Online-Only Contacts," Journal of Adolescent Health, 41, 6, pp. 51-58.

Xie, E., H.-H. Teo, and W. Wan (2006), "Volunteering Personal Information on the Internet: Effects of Reputation, Privacy Notices, and Rewards on Online Consumer Behavior," *Marketing Letters*, 17, 1, pp. 61-74.

Xu, H., X. Luo, J.M. Carroll, and M.B. Rosson (2011), "The Personalization Privacy Paradox: An Exploratory Study of Decision Making Process for Location-Aware Marketing," Decision Support Systems, 51, 1, pp. 42-52.

Xu, H., H.H. Teo, B.C.-Y. Tan, and R. Agarwal (2009), "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," Journal of Management Information Systems, 26, 3, pp. 135-174.

Yao, M.Z., and A.J. Flanagin (2006), "A Self-Awareness Approach to Computer-Mediated Communication," Computers in Human Behavior, 22, 3, pp. 518--544.

Youn, S. 2005. "Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach " Journal of Broadcasting & Electronic Media (49:1), pp 86-110.

Youn, S. (2009), "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents," *Journal of Consumer Affairs*, 43, 3, pp. 389-418.

Yue, W. T., and Cakanyildirim, M. (2007), "Intrusion Prevention in Information Systems: Reactive and Proactive Responses," *Journal of Management Information Systems*, 24, 1, pp. 329-353.

Zauberman, G. (2003), "The Intertemporal Dynamics of Consumer Lock-In," *Journal of Consumer Research*, 30, 3, pp. 405-419.

Zeithaml, V.A., A. Parasuraman, and A. Malhotra (2002), "Service Quality Delivery Through Web Sites: A Critical Review of Extant Knowledge," *Journal of the Academy of Marketing Science*, 30, 4, pp. 362-375.

Zeithaml, V.A., L.L. Berry, and A. Parasuraman (1996), "The Behavioral Consequences of Service Quality," *Journal of Marketing*, 60, 2, pp. 31-46.

Zetter, K. (2009), "Heartland Breach Cost Company $12.6 Million So Far," Retrieved from http://www.wired.com/threatlevel/2009/05/heartland-breach-cost-company-126-million-so-far/

Zohar, D. and Tenne-Gazit, O. (2008) "Transformational Leadership and Group Interaction as Climate Antecedents: A Social Network Analysis," Journal of Applied Psychology.

Zweig, D., and J. Webster (2002), "Where is the Line between Benign and Invasive? An Examination of Psychological Barriers to the Acceptance of Awareness Monitoring Systems," *Journal of Organizational Behavior*, 23, 5, pp. 605-633.

Zwick, D., and N. Dholakia (2004), "Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing," Journal of Macromarketing, 24, 1, pp. 31-43.

Zywica, J., & Danowski, J. (2008). The Faces of Facebookers: Investigating Social Enhancement and Social Compensation Hypotheses; Predicting Facebook™ and Offline Popularity from Sociability and Self-Esteem, and Mapping the Meanings of Popularity with Semantic Networks. Journal of Computer-Mediated Communication, 14(1), 1-34.

APPENDIX A: STUDY I 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 which directed interested users to a questionnaire hosted on a well-known online survey website.[22] Although such a sampling method could utilize chatroom 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.

In order 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 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 due to the lack of recency. Hence, the responses gathered did not accurately reflect their perceptions over a particular interaction, but several possibly unrelated privacy episodes which 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 chatroom 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 chatrooms, 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.

[22] www.surveyconsole.com

APPENDIX B: STUDY I 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 chatroom I was using allowed me and the other party to communicate through a variety of different cues (such as emotional tone, attitude or formality) in our messages.
(2) I believe that the online chatroom I was using allowed me and the other party to use rich and varied language (such as numeric data, pictures, or non-word expressions that have meanings) in our interaction.
(3) I believe that the online chatroom 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 chatroom 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 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 chatroom 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): developed 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: STUDY I 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: STUDY I SOBEL TEST RESULTS

		Self Disclosure		Misrepresentation	
		Sobel Z	Mediation	Sobel Z	Mediation
PAS	Privacy Concerns	-2.32*	Yes	2.48*	Yes
	Social Rewards[1]	-	-	-	-
PAO	Privacy Concerns	-2.10*	Yes	2.41*	Yes
	Social Rewards	-2.53*	Yes	2.45*	Yes
PMR	Privacy Concerns[2]	-	-	-	-
	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
* $p < 0.05$, ** $p < 0.01$
[1] No hypothesized relationship between perceived anonymity of self and social rewards
[2] No hypothesized relationship between perceived media richness and privacy concerns

APPENDIX E: STUDY II MEASUREMENT ITEMS

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

Information Dissemination (ID) (True/False)
(1) I am tagged in the note published by X.
(2) X has tagged me to the note.
(3) The note published by X has become a "Notes about me" because it is tagged to my profile.

Network Mutuality (NM)
(1) My online social network overlaps considerably with that of X.
(2) X and I have many common friends in the online social network.
(3) My online social network is highly similar to that of X.
(4) Many of my friends are also friends of X in the online social network.

Perceived Relationship (PRB): adapted from Wheeless and Grotz (1976) and Murray et al. (1996)
(1) After reading the note I feel very close to X.
(2) After reading the note, I am willing to disclose a great deal of positive and negative things about myself, honestly and fully, to X.
(3) After reading the note I am extremely happy with my relationship with X.
(4) After reading the note I think my relationship with X is very strong.
(5) After reading the note, I do not feel that my relationship with X is successful. (r)

Perceived Privacy Invasion (PPI): adapted from Fusilier and Hoyer (1980) and Alge (2001)
(1) I feel comfortable with the note about me being made public in this way. (r)
(2) I feel X needs to exercise greater controls to limit this kind of note publication.
(3) I feel that the note is none of anybody's business but my own.
(4) I feel my exposure in the note was an invasion of my privacy.

Control Variables

Sociability (SO): Adapted from Cheek and Buss (1981)
(1) I like to be with people
(2) I welcome the opportunity to mix socially with people.
(3) I prefer working with others rather than alone.

Shyness (SH): Adapted from Cheek and Buss (1981)
(1) I am socially somewhat awkward.
(2) I don't find it hard to talk to strangers.
(3) I feel tense when I'm with people I don't know well.

Perceived Network Closeness (PNC): Adapted from Floyd and Parks (1995)

(1) I frequently contact my friends in Facebook.
(2) I frequently share confidences with my friends in Facebook.
(3) I frequently get help from my friends in Facebook.

- Age: (Years old)
- Gender: (1 = male; 2 = female)
- Internet Experience: "How long have you been using the Internet?" (Years)
- Facebook Usage Experience: "How long have you been using Facebook?" (Years)

Notes:

(r) reverse items.

APPENDIX F: STUDY II THRESHOLD ESTIMATES

In model B, the first threshold estimate (TA = 0) is 1.11, which indicates that the predicted probability of score of 0 on transactional avoidance is higher than that of scores of 1 and 2 when both perceived relationship bonding and perceived privacy invasion are zero. The second threshold estimate (TA = 1) is 3.38, which indicates that the predicted probability of score of 0 and 1 is higher than that of score of 2 when both independent variables are zero.

In model C, the first threshold estimate (IA = 0) is 2.23, which indicates that the predicted probability of score of 0 on interpersonal avoidance is higher than that of scores of 1 and 2 when both perceived relationship bonding and perceived privacy invasion are zero. The second threshold estimate (IA = 1) is 3.94, which indicates that the predicted probability of score of 0 and 1 is higher than that of score of 2 when both independent variables are zero.

In model D, the first threshold estimate (AP = 0) is 3.12, which indicates that the predicted probability of score of 0 on approach is higher than that of scores of 1 and 2 when both perceived relationship bonding and perceived privacy invasion are zero. The second threshold estimate (AP = 1) is 6.38, which indicates that the predicted probability of score of 0 and 1 is higher than that of score of 2 when both independent variables are zero.

APPENDIX G: STUDY III MEASURES AND SCENARIOS*

[Part A]

Perceived Usefulness (PU)

- Using this online store enhances my effectiveness.
- Using this online store enhances my productivity.
- Using this online store improves my performance.

Perceived Ease-of-Use (PEOU)

- Interacting with this online store does not require a lot of mental effort.
- I find it easy to get the online store to do what I want it to do.
- I find the online store easy to use.

Trusting Beliefs (TRUST)

- This online store is trustworthy.
- I believe that this online store keeps its promises and commitments.
- I trust this store to keep customers' best interests in mind.
- This online store has sufficient expertise and resources to do business on the Internet.

Risk Beliefs (RISK)

- There is a high potential for loss involved in transactions with the online store.
- There is too much uncertainty associated with transactions with the online store.
- Transactions with the online store would involve many unexpected problems.

Loyalty (LOY)

- I consider myself to be highly loyal to the online store.
- I feel loyal towards the online store.
- It means a lot to me to continue to use the online store.

Switching Costs (SC)

- Switching to a new online store would involve some hassle.
- Some problems may occur when I switch to another online store.
- It would be complicated for me to change to another online store.

Pre-word of Mouth (WOM)

- I will say positive things about this online store to other people.
- I will recommend this online store to anyone who seeks my opinion.
- I will encourage friends to use this online store.

Pre-likelihood of Switching (LOS)

- I will look for an alternative online store for better service.
- I will think about switching to an alternative online store.
- I will consider another online store as my major service provider.

[Part B]

Scenarios

Imagine you have just received an e-mail from the online store that you indicated earlier (e.g. Amazon.com, eBay.com, Yahoo!Shopping, Overstock.com, DealsDirect.com, etc). In the email, the online store says that your credit card information has been stolen out by some hackers.

- Distributive Justice
  High: The e-mail clearly states that the online store is offering you a $100 cash coupon as an apology.

  Low: The e-mail clearly states that the online store is offering you a $10 cash coupon as an apology.

- Procedural Justice
  High: You feel like contacting the online store for further clarification. You find it very easy to obtain its contact information from the online store's homepage.

  Low: You feel like contacting the online store for further clarification. After navigating through the online store's website for some time, you finally obtain its contact information.

- Interactional Justice
  High: When you return home, you find a voice message left on your phone by a service representative of the online store. The service representative sincerely apologizes to you for the incident and explains the details of how the incident occurred.

  Low: When you return home, you find a voice message left on your phone by a service representative of the online store. The service representative explains briefly how the incident occurred.

Distributive Justice (DJ)

- I am being fairly rewarded for the risk to my personal information.
- Taking everything into consideration, the online store's offer is quite fair.
- Given the circumstances, I feel that the online store offers adequate compensation.

Procedural Justice (PJ)

- It is easy to figure out who to talk to in this online store regarding the problem.
- There are opportunities to request clarification or additional information.
- The online store allows me to provide feedback regarding the problem.

Interactional Justice (IJ)

- I am treated with courtesy and respect.
- The online store seems to care about the customer.
- The online store treats me with kindness and consideration.
- The online store shows concern for my rights as a customer.

Perceived Breach (PB)

- The online store has failed to meet its obligation to me.
- The online store has done a poor job of meeting its obligations to me.
- The online store has neglected the most important obligations to me.

Feelings of Violation (FV)

- I feel extremely frustrated by how I was treated by this service provider.
- The more I think about it, the more hostile I feel towards the website.
- I feel a great deal of anger toward this website

Post-Word of Mouth (PWOM)

The same as the WOM scale.

Post-likelihood of Switching (PLOS)

The same as the LOS scale.

[Part C]

Fantasizing (FAN)

- I daydream a lot.
- When I go to the movies I find it easy to lose myself in the film.
- I often think of what might have been.

Control Variables

- Age: (Years old)
- Gender: (1 = male; 2 = female)
- Experience: "How long have you been using the online store?" (Years)
- Website Usage: "I am a frequent customer of this online store." (Seven-point scale anchored with "strongly disagree" and "strongly agree")

Note: * Unless otherwise indicated, the anchors for all items were 1 = strongly disagree to 7 = strongly agree.

APPENDIX H: STUDY III EXPLORATORY FACTOR ANALYSIS

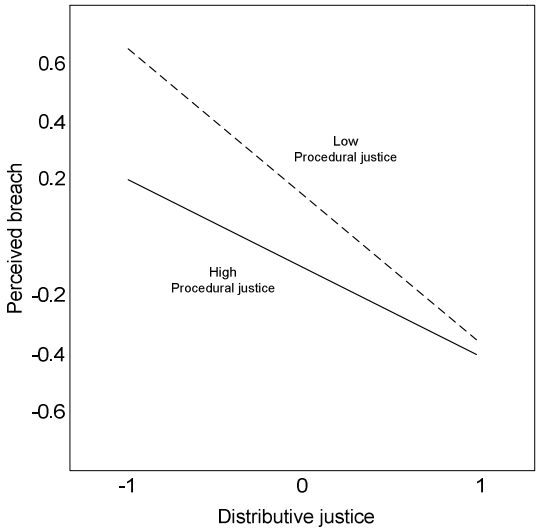
We performed exploratory factor analysis on the research factors shown in Figure 4.1. Table H1 shows the factor loadings and cross-loadings. The results indicated that the nine-factor solution explained a total of 91.39% of variance. The convergent and discriminant validity is established because factor loadings exceed 0.7 and cross-loadings are lower than 0.4 (Malhotra 2004). Thus, more confidence can be placed on the validity of our scales.

Table H1: Results of Exploratory Factor Analysis

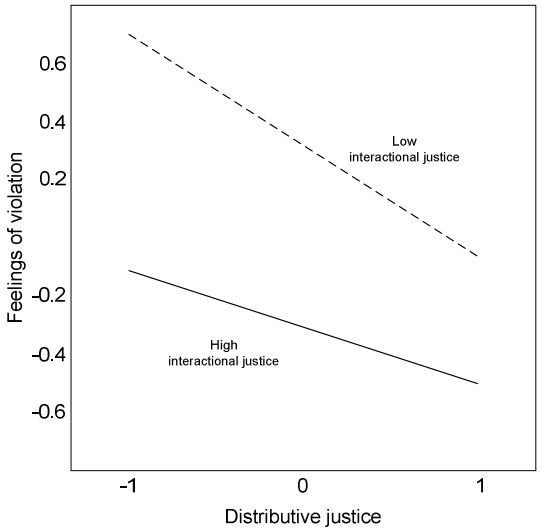
	Factor								
	1	2	3	4	5	6	7	8	9
DJ1	.751	.170	.131	-.131	-.145	.235	-.125	-.013	.095
DJ2	.848	.210	.144	-.158	-.183	.232	-.150	.026	.077
DJ3	.849	.213	.140	-.134	-.196	.235	-.149	.006	.067
IJ1	.214	.785	.317	-.192	-.095	.188	-.128	.104	-.059
IJ2	.246	.815	.277	-.194	-.097	.215	-.139	.117	-.021
IJ3	.219	.819	.313	-.177	-.099	.219	-.148	.098	-.034
IJ4	.234	.770	.303	-.183	-.105	.239	-.146	.105	-.015
PJ1	.146	.215	.754	-.067	-.095	.204	-.144	.066	-.020
PJ2	.118	.263	.881	-.104	-.065	.170	-.100	.086	-.025
PJ3	.132	.267	.803	-.065	-.089	.191	-.131	.113	-.019
FV1	-.150	-.188	-.111	.768	.184	-.102	.170	-.020	.040
FV2	-.105	-.144	-.069	.895	.178	-.148	.175	-.012	.090
FV3	-.136	-.114	-.053	.851	.224	-.155	.207	-.002	.078
PB1	-.198	-.086	-.066	.191	.847	-.153	.210	-.023	.059
PB2	-.149	-.075	-.102	.200	.868	-.180	.220	-.003	.044
PB3	-.148	-.066	-.077	.217	.823	-.182	.243	-.028	.062
PWOM1	.294	.216	.247	-.175	-.220	.739	-.308	.139	.029
PWOM2	.280	.210	.236	-.172	-.211	.784	-.314	.137	.012
PWOM3	.296	.205	.234	-.150	-.212	.763	-.317	.130	.024
PLOS1	-.148	-.134	-.139	.227	.263	-.295	.774	-.024	.189
PLOS2	-.138	-.109	-.135	.207	.272	-.267	.813	-.021	.174
PLOS3	-.152	-.113	-.134	.221	.246	-.257	.806	-.009	.164
WOM1	-.004	.081	.080	-.032	-.022	.085	-.030	.903	-.213
WOM2	.003	.090	.086	-.021	-.015	.062	-.008	.922	-.219
WOM3	.028	.055	.057	.023	-.007	.100	-.016	.876	-.202
LOS1	.062	-.043	-.013	.091	.034	.003	.082	-.219	.839
LOS2	.069	-.018	-.025	.050	.045	.009	.105	-.214	.895
LOS3	.048	.003	-.008	.030	.052	.006	.143	-.180	.832

APPENDIX I: STUDY III INTERACTION PLOTS

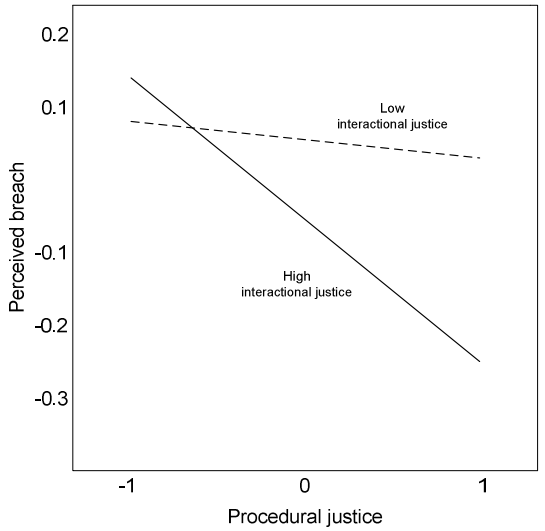
Figure I1. Interactions between Justice Perceptions on Psychological Responses



A. Moderating effect of procedural justice on the relationship between distributive justice and perceived breach



B. Moderating effect of interactional justice on the relationship between distributive justice and feelings of violation



C. Moderating effect of interactional justice on the relationship between procedural justice and perceived breach

APPENDIX J: STUDY III ROBUSTNESS CHECK

In order to check the robustness of the results, we reran the proposed model by specifying the three types of justice perceptions as dummy variables. The results of CFA showed that the model fit the data satisfactorily: χ^2 (817) = 1645.35, p <0.001, CFI = 0.99, NNFI = 0.99, RMSEA = 0.032, SRMR = 0.020, GFI = 0.94, AGFI = 0.91. However, the model with dummy variables was found to explain less variation in psychological responses and postincident outcomes than the model with continuous variables. In particular, the dummy-variable model accounted for 9% of perceived breach, 13% of feelings of violation, 49% of post-word of mouth, and 51% of likelihood of switching. These values were considerably lower than those reported at the column of the proposed model in Table 4.3. Nevertheless, the results of research hypotheses based on the dummy-variable model were generally comparable to those based on the continuous-variable model. Table J1 shows the new results of research hypotheses based on the dummy-variable model. As shown in Table J1, all of the hypotheses are supported by the data except one (H1b). Thus, it seems reasonable to conclude that our findings are almost equivalent regardless of the operationalization of justice perceptions.

Table J1: Tests of Research Hypotheses (Justice Perceptions as Dummy Variables)

Proposed paths		Path estimates	p-levels (one-tailed)	Hypothesis tests†
H1a	DJ → PB	-0.08	< 0.01	Supported
H1b	DJ → FV	-0.07	ns	Not supported
H2	PJ → PB	-0.15	< 0.001	Supported
H3	IJ → FV	-0.07	< 0.01	Supported
H4	DJ x PJ → PB	0.16	< 0.001	Supported
H5	DJ x IJ → FV	0.12	< 0.01	Supported
H6a	PB → PWOM	-0.37	< 0.001	Supported
H6b	PB → PLOS	0.43	< 0.001	Supported
H7a	FV → PWOM	-0.31	< 0.001	Supported
H7b	FV → PLOS	0.32	< 0.001	Supported

Notes:

- n = 1,007.
- † Hypothesis tests were performed based on a level of significance of 0.01.
- DJ = distributive justice; PJ = procedural justice; IJ = interactional justice; PB = perceived breach; FV = feelings of violation; PWOM = post-word of mouth; PLOS = post-likelihood of switching.